United States Government Accountability Office

Report to Congressional Committees

September 2026

IT SYSTEMS ANNUAL ASSESSMENT

DOD Should Improve IT Fraud Risk Management Practices

GAO-26-108596

GAO Highlights

IT SYSTEMS ANNUAL ASSESSMENT

DOD Should Improve IT Fraud Risk Management Practices

GAO-26-108596 September 2026

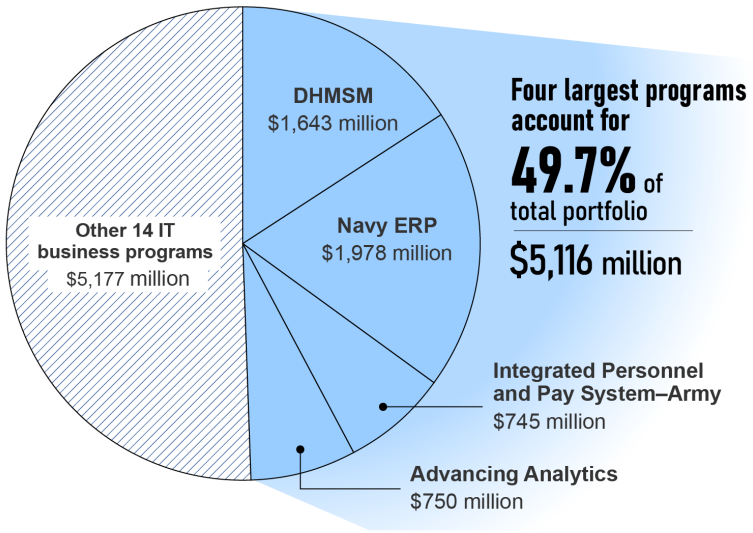
A report to congressional committees.

For more information, contact: Vijay D'Souza at dsouzav@gao.gov.

What GAO Found

To meet its mission to protect the security of our nation and provide warfighters the assets they need, the Department of Defense (DOD) relies heavily on the use of information technology (IT). According to DOD's Office of the Chief Information Officer (OCIO), the department planned to spend $10.3 billion on the 18 major IT business programs from fiscal years (FY) 2024 through 2026. The four largest programs account for 50 percent of the planned spending (see figure).

The Department of Defense's (DOD) Planned Costs for the Four Largest Information Technology (IT) Business Programs Compared to the Remaining 14 Selected Programs from Fiscal Year (FY) 2024 through FY 2026



DHMSM = Department of Defense (DOD) Healthcare Management System Modernization, Navy ERP = Navy Enterprise Resource Planning, IT = information technology

Source: GAO analysis of Department of Defense Office of the Chief Information Officer data, as of February 2026. | GAO-26-108596

To help determine whether operational programs are meeting their business or mission purpose, programs are required by the General Services Administration to identify and track a minimum of five performance metrics across the categories of customer satisfaction, strategic and business results, financial performance, and innovation. Of the 18 programs, 17 were operational. Of these, 15 identified the minimum required number of performance metrics in each category. However, the remaining two did not. Accordingly, the extent to which these two programs were improving customer satisfaction, increasing financial performance, and delivering innovative approaches is unknown. GAO has previously reported on DOD IT business programs not fully reporting

Why GAO Did This Study

IT is critical to the success of DOD's major business functions. These functions include such areas as health care, human capital, financial management, logistics, and contracting.

The National Defense Authorization Act for FY 2019, as amended, includes a provision for GAO to conduct assessments of selected DOD IT programs annually through March 2029. GAO's objectives for this seventh review were to (1) examine what progress selected DOD IT business programs have made on cost, schedule, and performance; (2) assess the extent to which DOD has implemented key fraud risk management, software development, and cybersecurity practices for selected programs; and (3) describe actions DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, GAO selected the 18 IT business programs listed as DOD's major IT investments in its FY 2026 submission to the Federal IT Dashboard. GAO analyzed data from DOD's OCIO to examine DOD's planned expenditures for these programs from FY 2024 through FY 2026. GAO also administered a questionnaire to the 18 program offices to obtain and analyze information about cost and schedule changes that the programs reported experiencing since January 2024. Further, GAO compared programs' performance metrics data provided by DOD's OCIO to guidance from the Office of Management and Budget.

To address the second objective, the questionnaire also sought information about the selected programs' practices in fraud risk management, software development, and cybersecurity. GAO compared the responses and documentation against relevant

What GAO Found (continued)

performance metric data and made recommendations to the department to do so (see GAO-22-105330 and GAO-25-107649). Regarding achieving performance goals, of the 17 programs that identified metrics, six programs met all performance targets, 10 programs met more than one target but not all, and one program met no targets.

The IT programs demonstrated mixed progress in implementing key practices for fraud risk awareness, software development, and key cybersecurity initiatives. Developing fraud risk awareness—particularly in staff who manage key IT programs—is an important step toward maturing DOD in fraud risk management. Of the 18 programs, seven programs reported via GAO's questionnaire that program staff were either unaware of or did not receive training to recognize and report signs of fraud or tampering in IT systems (see table). In response, DOD officials indicated that the department does not currently require training to recognize and report signs of fraud in IT systems, rather that personnel receive mandatory, general fraud awareness training. While these broad efforts are important, programs' reported lack of awareness of training to manage or report fraud can increase the risk of software development- and cybersecurity-related fraud within IT programs, making them vulnerable to exploitation.

Department of Defense (DOD) Major Information Technology (IT) Business Programs Reporting Fraud Risk Awareness

Fraud risk awareness practice	Number of programs that reported practice
Receiving training or knowing about available training over the past two years to recognize and report signs of fraud in IT systems	11 of 18
Assessing fraud risks facing the program	10 of 18

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

Further, 10 of the 18 DOD IT business programs reported actively developing software using recommended Agile and iterative software development approaches and practices. However, in areas related to tracking customer satisfaction and progress of software development, eight of the 10 programs did not report or demonstrate using required metrics and management tools. GAO previously recommended that DOD address this issue. Additionally, six of the 18 programs had not developed plans to implement zero trust in their cybersecurity frameworks by DOD's 2027 deadline (see table). In addition, while five programs reported using artificial intelligence (AI) tools to secure their systems, three programs did not have an approved cybersecurity strategy. GAO has previously recommended that all programs develop one (see GAO-22-105330).

Department of Defense (DOD) Major Information Technology (IT) Business Programs That Reported Having an Approved Cybersecurity Strategy or Implementing Zero Trust Architecture

Development approach or practice	Number of programs that reported using each approach or practice
Having a DOD approved cybersecurity strategy	15 of 18
Implementing zero trust architecture as part of the security framework	12 of 18

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

DOD continues to make efforts to improve its management of IT investments as a result of legislative and policy changes. These efforts include revising its business systems investment management guidance, modernizing its business enterprise architecture, adopting a zero trust cybersecurity strategy, developing AI acquisition guidance, updating its agency strategic plan, and implementing cost efficiency initiatives. GAO will continue to monitor DOD's efforts to improve how the department manages its IT investments.

Why GAO Did This Study (continued)

guidance and leading practices to identify gaps and risks. For programs that did not demonstrate having documentation or strategies, GAO followed up with DOD officials for clarification.

For the third objective, GAO reviewed and summarized (1) policy, plans, and guidance associated with the department's efforts to implement changes to its defense business systems investment management guidance and business enterprise architecture and (2) efforts to adopt zero trust cybersecurity principles, develop AI acquisition guidance, update its strategic plan, and implement cost efficiency initiatives. GAO also met with DOD OCIO officials to discuss their efforts in these areas.

What GAO Recommends

GAO reiterates that DOD should address the six recommendations previously made that have not yet been implemented from prior annual assessment reviews. GAO is also making one new recommendation to DOD to ensure that major IT business programs promote and sustain an antifraud tone that permeates programs' organizational culture through training focused on increasing awareness of fraud and fraud risk, recognition of fraud risks in relevant functional settings, and awareness of fraud risk assessment activities.

DOD partially agreed with GAO's recommendation and described actions it was taking to address the recommendation. While the response stated that the DOD Comptroller is the dedicated entity to oversee fraud risk management, GAO maintains that the OCIO must coordinate with that office to ensure that the staff of major IT business systems receive fraud risk training.

Contents

Tables

Figures

Abbreviations

ADVANA	Advancing Analytics
AI	artificial intelligence
ATP	authority to proceed
BEA	business enterprise architecture
CDAO	Chief Digital and Artificial Intelligence Office
CIO	Chief Information Officer
DBS	Defense Business Systems
DevOps	Development and Operations
DevSecOps	Development, Security, and Operations
DHMSM	Department of Defense Healthcare Management System Modernization
DME	development, modernization, and enhancement
DOD	Department of Defense
DOGE	Department of Government Efficiency
DSS	Distribution Standard System
EBS-C	Enterprise Business Systems—Convergence
FY	fiscal year
GSA	General Services Administration
IT	Information Technology
Navy ERP	Navy Enterprise Resource Planning
NDAA	National Defense Authorization Act
NIPRNET	Non-classified Internet Protocol Router Network
N-MRO	Naval—Maintenance, Repair, and Overhaul
O&S	operations and sustainment
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIO	Performance Improvement Officer
SMP	Strategic Management Plan

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

September 28, 2026

Congressional Committees

The Department of Defense (DOD) is one of the largest and most complex organizations in the world. To meet its mission to protect the security of our nation and provide warfighters the assets they need, DOD relies heavily on the use of information technology (IT). In support of its military operations, the department manages many IT investments encompassing communications, command and control, and business systems that support the department's operations (e.g., human capital, health care, contracting, logistics, and financial management). For fiscal year (FY) 2026, the department requested approximately $66.1 billion for its IT and cyberspace activities.[1] These investments include DOD's major IT business programs, which are intended to help the department sustain its key operations.[2] These are the focus of this report.

The John S. McCain National Defense Authorization Act (NDAA) for FY 2019 includes a provision as amended for GAO to conduct annual assessments of selected DOD IT programs through March 2029.[3] This report presents the results of our seventh annual assessment. Our specific objectives for this assessment were to (1) examine the current status of cost, schedule, and performance of selected DOD IT business programs, (2) determine the extent to which DOD has implemented key fraud risk management, software development, and cybersecurity practices for selected programs, and (3) describe actions DOD has taken

[1]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: President's Budget (PB) 2026 Budget Request* (August 2025).

[2]These unclassified IT investments also include non-major programs and supporting infrastructure (cloud, general IT, and cyber-specific capabilities).

[3]Pub. L. No 115-232, § 833, 132 Stat. 1636, 1858 (Aug. 13, 2018), adding a new section 2229b, Comptroller General assessment of acquisition programs and initiatives, to Title 10 of the U.S. Code, since renumbered § 3072. Under this provision, we are to report on these assessments no later than March 30 of each year. The provision has been amended several times, most recently extending GAO's reviews until 2029. Pub. L. No. 118-159, § 813(a)(3), 138 Stat. 1773, 1980 (Dec. 23, 2024). Our assessment of the performance of DOD's weapon programs is included in a separate report, which we also prepared in response to section 833 of the NDAA for FY 2019. See GAO, *Weapon Systems Annual Assessment: Requiring Mature Technologies Could Enable Shift to Rapid Delivery*, GAO-26-108457 (Washington, D.C.: July 2, 2026).

to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, we selected the 18 major IT business programs from the 31 programs that DOD listed as major IT investments in its FY 2026 Federal IT Dashboard (Dashboard) data, as of July 2025.[4] We based our selection on newly identified programs for FY 2026 and programs with over $250 million in FY 2024-2025 funding.[5] We analyzed data provided by DOD's Office of the Chief Information Officer (OCIO) to examine DOD's planned expenditures on these programs from FY 2024 through FY 2026. Additionally, we analyzed supporting documentation, including key program documents pertaining to each program's life cycle cost, schedule estimates, and baselines. We also analyzed responses to a questionnaire we administered to all 18 program offices in September 2025. The questionnaire focused on programs' cost and schedule, software development practices, cybersecurity, software risks and challenges, and fraud risk management. Further, for the 18 programs, we analyzed DOD's performance data provided by the DOD OCIO and compared the data to Office of Management and Budget (OMB) guidance on reporting on IT investments.[6]

For the second objective, we analyzed information from our questionnaire on fraud risk management, software development, and cybersecurity practices used by the 18 programs, including 10 programs that we identified as actively developing software.[7] We compared the information to relevant best practices and guidance (e.g., Defense Science Board and

[4]DOD classifies these programs as defense business systems. The Dashboard is a public, government website operated by the General Services Administration (GSA) at https://www.itdashboard.gov/. It includes streamlined data on IT investments to enable agencies and Congress to better understand and manage federal IT portfolios.

[5]We used $250 million because it was a natural break in the funding amount of potential investments to select for this review.

[6]FY 2026 reporting requirements for IT investments are contained in Section 55 of OMB's Circular No. A-11 guidance and in GSA's supporting guidance for complying with OMB's submission requirements. Office of Management and Budget, *Preparation, Submission, and Execution of the Budget,* Circular No. A-11, (Washington, D.C.: Aug. 2025); General Services Administration, *BY 2026 IT Collect-Submission Overview* (Washington, D.C.: Dec. 2024).

[7]For the purposes of this assessment, we considered programs to be actively developing software if officials reported that they were actively developing new software functionality. Officials for the other eight programs reported either that their software development efforts were to sustain existing functionality, involved minor enhancements, or that they were not actively developing software.

Defense Innovation Board reports, DOD instructions, DOD's zero trust framework,[8] and OMB guidance) to identify any gaps.[9] Also, we analyzed questionnaire responses on DOD's fraud risk management practices and compared the responses against GAO's Fraud Risk Management Framework to identify any gaps and risks.[10] In addition, we reviewed programs' reported use of Agile metrics and management tools as part of DOD's software development efforts. Further, we analyzed supporting documents about programs' reported cybersecurity practices including the implementation of artificial intelligence (AI) and plans for and implementation of zero trust cybersecurity. Lastly, we assessed information about key challenges related to software development and cybersecurity reported by program officials and the actions that programs and DOD officials reported taking to address the challenges.

To address the third objective, we summarized actions DOD has taken to 1) implement previously identified legislative and policy changes that could affect its IT acquisitions[11] and 2) efforts to adopt zero trust cybersecurity, develop AI acquisition guidance, update its agency strategic plan, and implement cost efficiency initiatives. To do so, we reviewed policies, plans, and guidance provided by DOD. We also coordinated with the GAO team conducting a companion assessment for FY 2026 examining major defense acquisition programs.[12] Appendix I provides a detailed discussion of our objectives, scope, and methodology.

[8]Zero trust is a set of cybersecurity principles that are founded on the concept that no actor, system, network, or service operating outside of or within an organization's security perimeter should be trusted.

[9]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 (Washington, D.C.: Feb. 2, 2017, incorporating Change 2, Jan. 24, 2020); Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense*, Test and Evaluation*, Instruction 5000.89 (Nov. 19, 2020); OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[10]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

[11]The previously identified legislative and policy changes are discussed in GAO*, IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Cybersecurity Planning*, GAO-25-107649 (Washington, D.C.: June 12, 2025).

[12]GAO-26-108457.

We conducted this performance audit from June 2025 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In support of its military operations, DOD manages many IT investments encompassing communications, command and control, and business systems. For FY 2026, the department requested approximately $66.1 billion for its IT and cyberspace activities.[13] These investments include DOD's major IT business programs, which are intended to help the department sustain its key mission support operations (e.g., human capital, health care, contracting, logistics, and financial management).[14]

DOD's Policy and Framework for Managing Major IT Acquisitions

In January 2020, DOD updated its acquisition policy to create a framework to enable flexible and responsive acquisitions. The reissued DOD Instruction 5000.02 established the new adaptive acquisition framework, provided high-level policy for the framework, and assigned roles and responsibilities to acquisition officials.[15] In addition, DOD Instruction 5000.02 was updated in June 2022, with a subsequent update made in April 2026, that streamlined the management of acquisition programs.

Under the adaptive acquisition framework, program managers are to tailor their acquisition strategy by using one or more pathways: (1) urgent capability acquisition, (2) middle tier of acquisition, (3) major capability acquisition, (4) business systems acquisition, (5) software acquisition, and (6) defense acquisition of services. Additionally, the framework calls for program managers to establish a risk management program and continuously address cybersecurity throughout the program life cycle.

While the instruction established overarching policy for acquisition programs, separate instructions specify the roles, responsibilities, and

[13]Department Of Defense, *Information Technology and Cyberspace Activities Budget Overview.*

[14]These unclassified IT investments also include non-major programs and supporting infrastructure.

[15]Department of Defense, *Operation of the Adaptive Acquisition Framework,* Instruction 5000.02 (Washington, D.C.: Jan. 23, 2020; updated June 2022 and April 2026).

procedures for each pathway. Of the six pathways, two deal primarily with the acquisition of IT business systems and software.

Business Systems Acquisition Pathway

According to DOD Instruction 5000.02, the purpose of the business systems pathway is to acquire information systems that support DOD's business operations. The pathway can also be used to acquire non-developmental, software-intensive programs that are not business systems. Under this pathway, DOD is to assess the business environment and identify existing commercial or government solutions that could be adopted to satisfy the department's needs.

In January 2020, DOD updated the instruction for the business systems acquisition pathway to align business system acquisitions with the adaptive acquisition framework. Instruction 5000.75 establishes policy for using the five-phase business capability acquisition cycle for business system requirements and acquisitions.[16] While maintaining the general structure of the defense business systems pathway, the 2020 update removed certain oversight requirements and encouraged a tailored approach to each program. The 2020 update also enabled and encouraged acquisition officials to delegate decision-making down to the "lowest practical level."

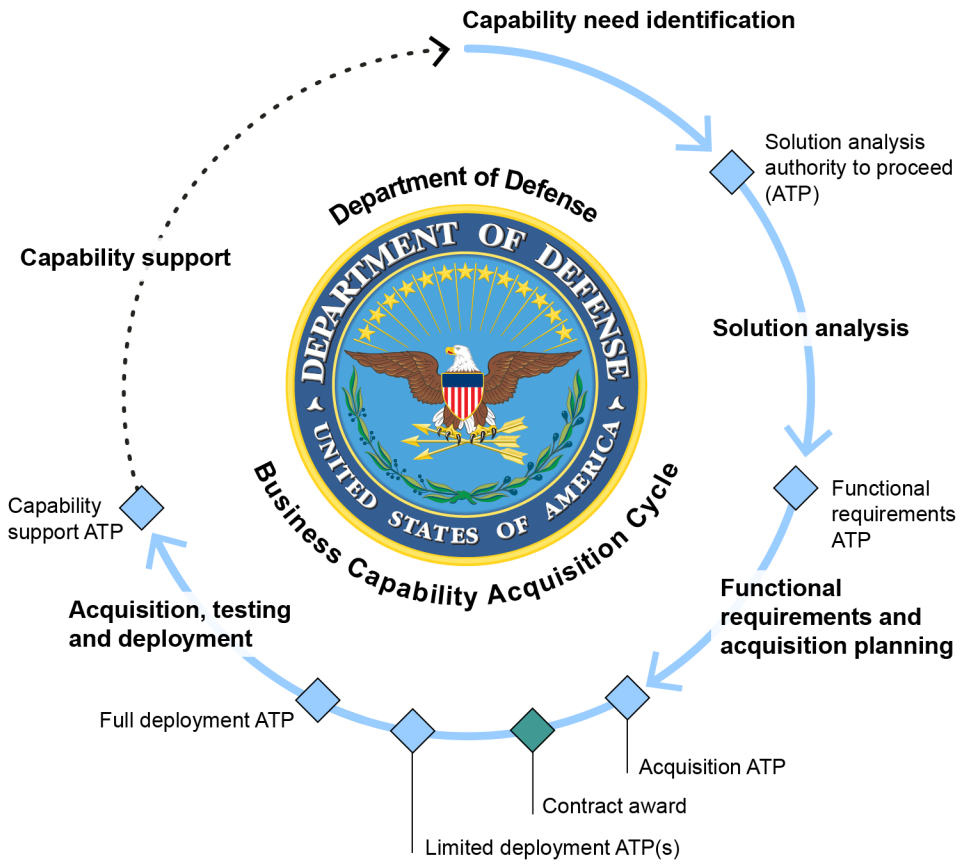
Under the pathway, business system acquisition program officials are to

- align the program with commercial best practices;
- minimize the need for customization of commercial products to the greatest extent possible;
- conduct thorough industry analysis and market research of both process and IT solutions using commercial off-the-shelf and government off-the-shelf software;
- tailor and delegate authority to proceed decision points, as necessary, to contribute to the successful delivery of business capabilities;
- automate testing; and
- use Agile software development (Agile) or incremental software development processes to the greatest extent practical.

[16]Department of Defense, Instruction 5000.75.

Figure 1 shows DOD's business capability acquisition cycle under the business system pathway

Figure 1: The Department of Defense's (DOD) Business Capability Acquisition Cycle



Sources: GAO presentation of DOD information; DOD (logo). | GAO-26-108596

Milestones are the critical acquisition decision points for authorization to proceed or concurrence with contractual commitments. The milestones fall under the two higher-level phases of the system life cycle, referred to as development and sustainment. Additionally, investment expenditures in DOD's annual budget submissions are broken down into two categories of cost representing these two phases: (1) development,

modernization, and enhancement (DME) and (2) operations and sustainment (O&S).[17]

For the business capability acquisition cycle, development is associated with the activities and milestones starting at the beginning of the system lifecycle, at the capability need identification stage, and includes the development and delivery of new functionality or enhancements through full and limited deployments. A limited deployment is any deployment before the full deployment authority to proceed (ATP) that provides a set of functionalities to a set of users of the business system. Limited deployments are approved at a limited deployment ATP, a decision point where the milestone decision authority considers the results of testing and approves the deployment of the release to limited portions of the end user community.[18] Full deployment is the delivery of full functionality to all planned users of the business system in accordance with the full deployment ATP. This is a decision point where the milestone decision authority considers the results of limited deployment(s) and operational testing and approves deployment to the entire user community.

Sustainment is associated with the activities and milestones starting at the beginning of the capability support stage, once the business system has been fully deployed, and includes supporting the capability and maintaining the system (e.g., continued cybersecurity readiness and appropriate upgrades). More specifically, capability support is a phase where the functional sponsor manages and governs the business capability and the program manager oversees the technical implementation and configuration of the system in accordance with the capability support ATP (i.e., a decision point where the milestone decision authority accepts full deployment of the system and approves the transition to capability support).

Software Acquisition Pathway

Section 800 of the NDAA for FY 2020 mandated that DOD develop the software acquisition pathway.[19] In October 2020, the department issued DOD Instruction 5000.87 *Operation of the Software Acquisition*

[17]*Operations and sustainment* is a term used by DOD to describe a stage of the program life cycle equivalent to operations and maintenance.

[18]The milestone decision authority determines the entry points of an acquisition program in the acquisition process and is the approval authority for a number of other program documents, strategies, and goals.

[19]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 800, 133 Stat 1198, 1478 (Dec. 20, 2019).

Pathway.[20] According to this guidance, the pathway is to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software.

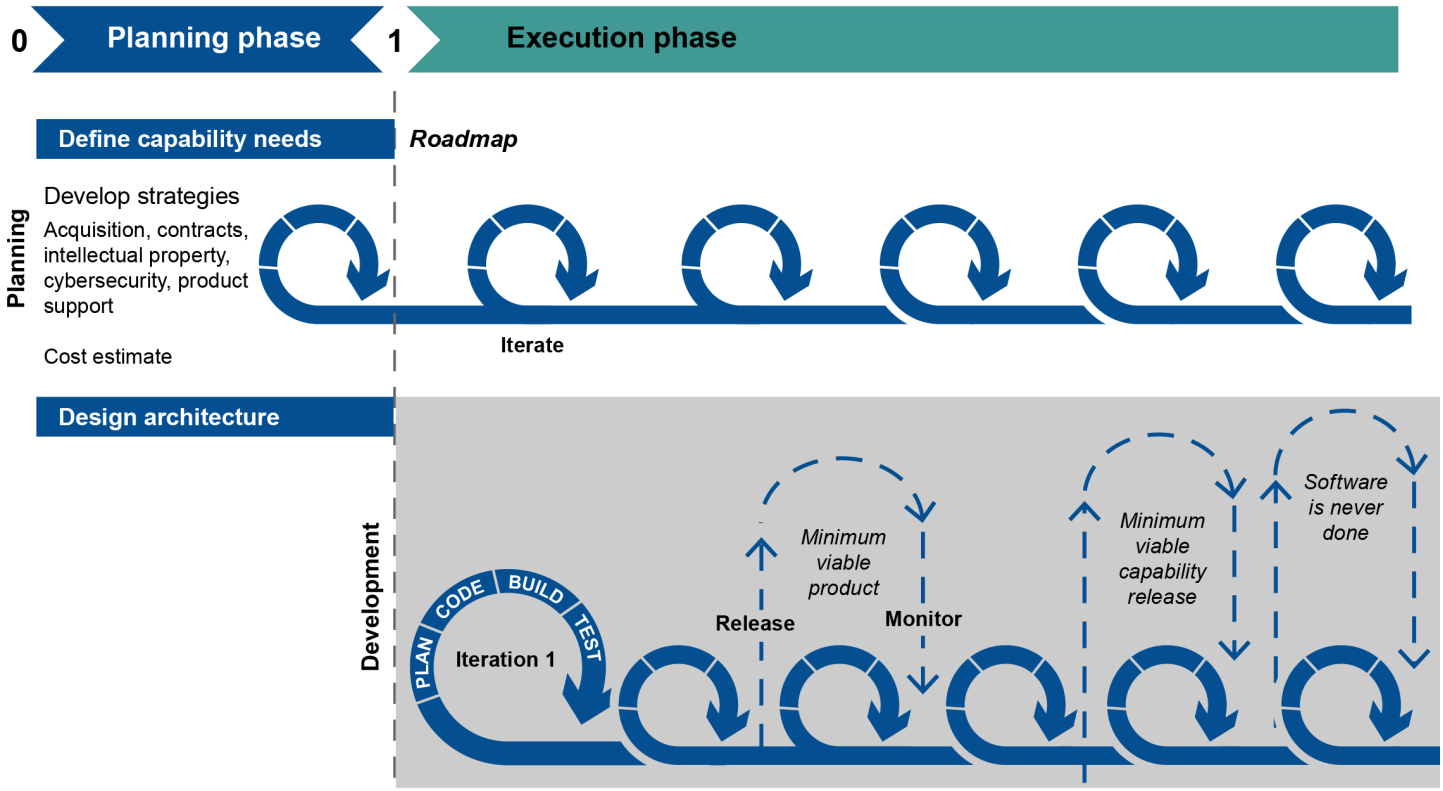
According to DOD Instruction 5000.02, the software acquisition pathway is intended to integrate modern software development practices such as Agile; Development, Security, and Operations (DevSecOps); and lean practices.[21] Under this pathway, small cross-functional teams that include users, testers, software developers, and cybersecurity experts use enterprise services to deliver software rapidly and iteratively to meet users' needs.

Under DOD Instruction 5000.87, the software acquisition pathway contains a planning phase and an execution phase. Figure 2 shows the pathway's two phases.

[20]Department of Defense, *Operation of the Software Acquisition Pathway,* Instruction 5000.87 (Washington, D.C.: Oct. 2, 2020). Prior to the publication of Instruction 5000.87, the department had an interim policy in effect. Department of Defense, *Software Acquisition Pathway Interim Policy and Procedures* (Washington, D.C.: Jan. 3, 2020).

[21]Throughout this report, we refer to steps DOD has taken to implement Agile software development. DOD has also developed resources for iterative development methodologies that are consistent with Agile, such as DevSecOps, and that are not mutually exclusive. In this report, we discuss these under the category of Agile software development because they also support Agile development.

Figure 2: The Department of Defense's Software Acquisition Pathway



Source: GAO presentation of Department of Defense information. | GAO-26-108596

Designed for software-intensive systems, the pathway contains two sub-paths: one for applications deploying software that runs on commercial hardware and cloud platforms and the other for upgrades and improvements to software embedded in military systems. The guidance in DOD Instruction 5000.87 applies to both of these sub-paths. The guidance also encourages program officials to delegate decisions to the lowest practical level, frequently engage with users, automate as much as possible, and reach key program milestones at least annually.

DOD's Implementation of Agile Software Development

Agile is an iterative development approach in which software is delivered in increments throughout the project and is built iteratively by refining or discarding portions as required based on user feedback. This includes delivering a minimum viable product that is an early version of the software to deliver or field basic capabilities to users to evaluate. Iterative development can allow program staff to catch errors quickly and

continuously, integrate new code with ease, and obtain user feedback throughout the process. Consistent with studies recommending DOD's transition toward Agile software development, and to implement statutory mandates to help enable its transition, the department has begun implementing Agile as part of its software modernization initiatives.[22]

As previously mentioned, updates to the business systems pathway and the creation of the software acquisition pathway were designed, in part, to enable Agile software development. Both pathways contain provisions that support this type of development. For example, a limited deployment in the business systems pathway can be similar to a minimum viable product in an Agile development methodology, and the program team is expected to iteratively release functionality. In addition, the software acquisition pathway requires the use of iterative and Agile practices.

In February 2022, DOD also issued a software modernization strategy, in part to advance its implementation of Agile development.[23] The strategy is intended to support DOD's efforts to improve software delivery through modern infrastructure and platforms and to enable these improvements by transforming processes and developing personnel. The strategy has three goals:

- accelerate development of the DOD enterprise cloud environment,
- establish a department-wide software factory environment, and
- transform processes to enable resilience and speed.

To further support implementation of the modernization strategy, the department established a Software Modernization Senior Steering Group in February 2022. The group includes membership from offices across the department, including the offices of the DOD Chief Information Officer

[22]Defense Science Board, *Design and Acquisition of Software;* Defense Innovation Board, *Software is Never Done*. Section 873 and 874 of the NDAA for FY 2018 established two Agile pilot programs, National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, §§ 873-874, 131 Stat. 1283, 1498-1503 (Dec. 12, 2017). Section 800 of the NDAA for FY 2020 established a software acquisition pathway that, according to DOD Instruction 5000.02, is to include support for Agile practices. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 800, 133 Stat. 1198, 1478 (Dec. 20, 2019). We reported on the implementation status of the section 873 and 874 pilots in GAO, *Weapons Systems Annual Assessment: Challenges to Fielding Capabilities Faster Persist,* GAO-22-105230 (Washington, D.C.: June 8, 2022).

[23]Department of Defense, *Department of Defense Software Modernization* (Washington, D.C.: Feb. 1, 2022).

(CIO); Under Secretary of Defense for Acquisition and Sustainment; Under Secretary of Defense for Research and Engineering; Under Secretary of Defense for Intelligence and Security; Director, Operational Test and Evaluation; and Director, Cost Assessment and Program Evaluation, as well as the military departments and services, Joint Chiefs of Staff, and the Defense Information Systems Agency.

DOD's Cybersecurity Guidance

DOD Instruction 8500.01 describes cybersecurity requirements for all DOD acquisition programs containing IT.[24] Broadly, it requires the department to implement a cybersecurity risk management process to protect DOD operational capabilities and assets. The instruction states that IT systems must address risks such as those associated with inherent IT vulnerabilities, global sourcing and distribution, and adversary threats throughout the IT life cycle. It also includes guidance for high-level management of cybersecurity, technological requirements, and workforce considerations.

Additionally, DOD Instruction 8510.01 documents specific guidance for IT risk management.[25] Under this instruction, all DOD IT systems must be categorized in accordance with Committee on National Security Systems Instruction 1253,[26] and implement a corresponding set of security controls and assessments from National Institute of Standards and Technology Special Publication 800-53.[27] The guidance requires officials responsible for IT systems to identify resources needed to implement DOD's risk management framework, develop and maintain milestones and a plan of action to address known vulnerabilities, and designate an official responsible for authorizing the system's operation based on its risk posture. The instruction also clarifies that the risk management framework will inform acquisition processes for requirements development, procurement, and developmental and operational testing and evaluation.

[24]Department of Defense, *Cybersecurity*, Instruction 8500.01 (Washington, D.C.: Mar. 14, 2014, incorporating Change 1, Oct. 7, 2019).

[25]Department of Defense, *Risk Management Framework (RMF) for DoD Systems*, Instruction 8510.01 (July 2022).

[26]Committee on National Security Systems, *Security Categorization and Control Selection for National Security Systems*, Instruction 1253 (Washington, D.C.: Mar. 27, 2014).

[27]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 Revision 5.2.0 (Gaithersburg, MD: Aug. 27, 2025).

In September 2025, DOD announced the planned implementation of a new cybersecurity risk management construct to address shortcomings of the legacy risk management framework, however, a time frame for programs to fully transition to this construct has not been established.

Federal Requirements and Guidance Addressing Performance Reporting, Adoption of AI, and Zero Trust

In addition to DOD's policies and guidance outlined above, the federal government has established requirements and guidance on performance reporting, adoption of AI, and zero trust cybersecurity.

The Federal IT Dashboard. A provision in what is commonly known as the Federal Information Technology Acquisition Reform Act requires that the Director of OMB make information on major federal IT investments of covered agencies (including DOD) publicly available,[28] in accordance with detailed OMB guidance.[29] This information is displayed on the Federal IT Dashboard, a public, government website that includes streamlined data and information on the performance of major IT investments. The Dashboard is intended to enable agencies and Congress to better understand and manage federal IT portfolios and make better IT planning decisions. In March 2022, the Dashboard's management responsibilities—including collecting, analyzing, and displaying IT budget and performance data—transitioned from OMB to the General Services Administration's (GSA) Office of Government-wide Policy.[30] However, OMB's guidance continues to address many aspects of the reporting requirements for IT investments while GSA provides supporting guidance for complying with the requirements.[31]

Although OMB provides guidance on designating major IT investments and reserves the right to designate them, it gives each covered agency the flexibility to establish specific criteria. According to officials from the

[28]Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 832, 128 Stat. 3292, 3440-3441 (Dec. 19, 2014); codified at 40 U.S.C. § 11302(c)(3).

[29]Office of Management and Budget, *Preparation, Submission, and Execution of the Budget,* Circular No. A-11.

[30]GSA's FY 2019 budget justification included this change.

[31]FY 2026 reporting requirements for IT investments are contained in Section 55 of OMB's Circular No. A-11 guidance and in GSA's supporting guidance for submissions to the Dashboard. Office of Management and Budget, *Preparation, Submission, and Execution of the Budget,* Circular No. A-11; General Services Administration, *BY 2026 IT Collect Submission Overview*.

DOD OCIO and the department's guidance,[32] DOD's major IT investments include: (1) defense business systems with a budget greater than $250 million across the future years defense plan;[33] (2) non-defense business systems with a budget greater than $569 million across the future years defense plan; (3) IT investments designated as major by the DOD CIO; and (4) major defense acquisition programs determined to be IT investments by the DOD CIO.[34]

In addition to information on the cost, schedule, and performance of agencies' major IT investments, each agency's CIO is required to submit ratings to the Dashboard. According to OMB's guidance, these ratings should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals.

The public display of these data is intended to allow oversight bodies and the general public to hold agencies accountable for mission-related outcomes. We have issued a series of reports that noted the significant steps that OMB had previously taken to enhance the oversight, transparency, and accountability of federal IT investments by creating the Dashboard.[35] These reports also addressed issues with the accuracy and

[32]Department of Defense, *FY 2025 IT/CA Budget Guidance Implementation I Guide A*.

[33]DOD's future years defense plan includes planned program costs over a 5-year period.

[34]Major defense acquisition programs generally include programs that are not highly sensitive or classified and defined as programs that are either (1) designated by the Secretary of Defense or (2) estimated to require, for all planned increments, an eventual total expenditure for research, development, test, and evaluation of more than $525 million in FY 2020 constant dollars or procurement of more than $3.065 billion in FY 2020 constant dollars. See 10 U.S.C. § 4201(a); Department of Defense, *Major Capability Acquisition,* Instruction 5000.85, (Aug. 6, 2020, incorporating Change 1, Nov. 4, 2021). Change 1 reflects statutory cost thresholds in FY 2020 constant dollars.

[35]GAO, *IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments*, GAO-16-494 (Washington, D.C.: June 2, 2016); *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to Be More Accurate and Available*, GAO-14-64 (Washington, D.C.: Dec. 12, 2013); *IT Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies*, GAO-13-98 (Washington, D.C.: Oct. 16, 2012); *IT Dashboard: Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Making*, GAO-12-210 (Washington, D.C.: Nov. 7, 2011); *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy*, GAO-11-262 (Washington, D.C.: Mar. 15, 2011); and *Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Improvements Needed*, GAO-10-701 (Washington, D.C.: July 16, 2010).

reliability of the Dashboard's data. Accordingly, we made recommendations to OMB to address these issues, which it implemented.

In April 2026, OMB's Federal CIO announced an effort to sunset the IT Dashboard, with agencies pivoting to streamlined reporting focusing on statutorily required data. DOD OCIO officials indicated that the department continues to await further guidance from OMB regarding the types of data required and the manner in which this data will be reported.

Adoption of AI. AI generally refers to computer systems designed to replicate a range of human functions and continually get better at their assigned tasks. DOD's AI capabilities could be used in various ways, for example in identifying potential threats or targets on the battlefield.

The National Security Commission on Artificial Intelligence—established by law in 2018 to consider ways to advance the development of AI to address U.S. national security and defense needs—concluded in its March 2021 report that the U.S. is not prepared to defend itself in the AI era, and must act quickly to enable AI-readiness by 2025.[36] The commission further concluded that ensuring DOD has the necessary infrastructure, including tools and talent, in place will be essential to developing, acquiring, and scaling AI for weapon systems quickly and effectively.

In January 2025, the White House issued Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, which required the Secretary of Defense, among others, to develop and submit an AI action plan.[37] In January 2026, DOD published its *Artificial Intelligence Strategy*, designating AI a top modernization area to develop AI tools and capabilities.[38] This strategy is intended to help the department accelerate its efforts towards integrating AI technology across all components and become "AI-first." The strategy calls for seven pilot projects in three mission areas—warfighting, intelligence, and

[36]John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1051 (2018). The National Security Commission on Artificial Intelligence, "Final Report" (March 1, 2021), https://irp.fas.org/offdocs/ai-commission.pdf.

[37]Exec. Order No. 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, 90 Fed. Reg. 8741 (Jan. 23, 2025).

[38]Department of Defense, *Artificial Intelligence Strategy for the Department of War* (Jan. 9, 2026).

enterprise—with a focus on, among other things, aggressive timelines and measurable outcomes.

Senate Report 116-236 accompanying the National Defense Authorization Act for Fiscal Year 2021 includes a provision for GAO to review DOD's AI acquisition efforts.[39] In our first report in February 2022, we described the status of DOD's efforts to develop and acquire AI for weapon systems.[40] Our second report described the extent to which the agency has department-wide AI acquisition guidance.[41] Our most recent report described DOD's responsible use of AI, including its policies and guidance, the extent that DOD has incorporated responsible AI tenets into selected AI-enabled activities and systems, and the oversight structure and mechanisms for monitoring responsible AI.[42]

Zero trust cybersecurity. A May 2021 executive order required, among other things, that agencies, including DOD, adopt cybersecurity best practices, which included developing a plan to implement a zero trust architecture.[43] Zero trust is a set of cybersecurity principles that are founded on the concept that no actor, system, network, or service operating outside of or within an organization's security perimeter should be trusted. The principles suggest that organizations must verify anything and everything that attempts to establish access to their systems, services, and networks.

In addition, the NDAA for FY 2022 directed DOD to develop a zero trust strategy, a model architecture, and implementation plans.[44] While the concepts behind zero trust are not new, the implications of shifting away

[39]S. Rep. No. 116-236, at 131 (2020).

[40]GAO, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems*, GAO-22-104765 (Washington, D.C.: Feb. 17, 2022).

[41]GAO, *Artificial Intelligence: DOD Needs Department-Wide Guidance to Inform Acquisitions,* GAO-23-105850 (Washington, D.C.: June 29, 2023). We made four recommendations for DOD and the three military departments to develop guidance on acquiring AI capabilities, leveraging private company factors as appropriate. DOD concurred with the recommendations and as of July 2026 has partially addressed one of the recommendations.

[42]GAO, *Artificial Intelligence: Actions and Opportunities to Promote Responsible Use in DOD,* GAO-26-107837 (Washington, D.C.: September 24, 2026).

[43]Exec. Order No. 14028, *Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 (Washington, D.C.: May 12, 2021).

[44]Pub. L. No. 117-81, § 1528, 135 Stat. 1541, 2044-2048 (Dec. 27, 2021).

from perimeter-based security are new to most enterprises and many federal agencies, including DOD.[45]

GAO Guidance on Developing Agile Software and Framework for Combating Fraud

GAO developed guidance on best practices when adopting Agile software development, and a framework to prevent, detect, and respond to potential fraud.

Agile Assessment Guide. In December 2023, GAO issued its updated *Agile Guide* to help organizations assess their readiness to adopt Agile methods, as well as to enable assessment of an agency's use of these methods.[46] GAO's *Agile Guide* describes best practices, including metrics and management tools, that programs are encouraged to use when pursuing Agile software development. Metrics are the data about a program's performance to help measure an organization's operations and results, while management tools can be used to capture the metrics and support decision-making.

Fraud Risk Management Framework. In February 2025, GAO expanded the DOD financial management High Risk area within its High Risk List to include DOD fraud risk management,[47] highlighting the need to improve DOD's fraud risk assessment and management processes.[48] In July 2015, GAO issued *A Framework for Managing Fraud Risks in Federal Programs* to help managers combat fraud and preserve integrity in government agencies and programs.[49] The Fraud Risk Framework includes leading practices that serve as a guide for program managers when developing or enhancing efforts to combat fraud. These leading practices include establishing an organizational structure and culture that are conducive to fraud risk management, designing and implementing

[45]Perimeter-based security refers to conventional network security practices in which, once a user is inside of an organization's network, that user is considered trusted and is often given broad access to multiple resources.

[46]GAO, *Agile Assessment Guide: Best Practices for Adoption and Implementation*, GAO-24-105506 (Washington, D.C.: Dec. 15, 2023).

[47]The GAO High Risk List highlights areas across the federal government that are seriously vulnerable to waste, fraud, abuse, and mismanagement or that need transformation.

[48]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).

[49]GAO-15-593SP; GAO, *Combating Fraud: Approaches to Evaluate Effectiveness and Demonstrate Integrity*, GAO-26-107609 (Washington, D.C.: Jan. 14, 2026).

controls to prevent and detect potential fraud, and monitoring and evaluating to provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud.

GAO Has Made Recommendations to Improve Management of DOD IT Systems

GAO has included DOD business systems in its High Risk List and has made numerous recommendations to improve the department's management of IT systems.

DOD's business systems modernization efforts on GAO's High Risk List. DOD's business systems modernization efforts have been on GAO's High Risk List since 1995, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments, including for its major IT programs.[50] As we reported in February 2025, DOD developed a draft action plan with specific actions and associated milestones to help the department improve management of its portfolio of defense business systems, including improving its business enterprise architecture (BEA) efforts.[51] However, the draft plan did not include all elements of an effective action plan, such as identifying responsible parties or the resources needed to implement corrective actions, and developing performance metrics to evaluate progress. As of July 2026, there were 28 GAO recommendations within this High Risk area that DOD had not yet implemented.

GAO reports on DOD's major IT business programs. As part of our mandated work (which was first required in the NDAA for FY 2019 and is included in our High Risk oversight area), we began a series of annual reports focused on the performance of DOD's major IT business programs in 2020. Five of the six reports issued as part of this series included recommendations to DOD.

- **June 2021.** We reported on steps DOD was taking to collect and report acquisition program data.[52] For example, we found that DOD

[50]For example, see GAO, *High-Risk Series*, GAO-HR-95-1 (Washington, D.C.: Feb. 1, 1995) and additional work such as GAO-25-107743; *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); and *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[51]GAO-25-107743.

[52]GAO, *Software Development: DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices*, GAO-21-351 (Washington, D.C.: June 23, 2021).

had not developed data strategies and had not finalized metrics for its business system and software acquisition pathways. We recommended that the department improve how it monitors its IT acquisitions by ensuring the data strategies and data collection efforts for the business system and software pathways use appropriate metrics to monitor acquisitions and assess performance. DOD provided updates intended to help address the recommendation in August 2024. However, as of July 2026, it had not fully demonstrated that the department had completed tasks necessary to implement the recommendation.[53]

- **June 2022.** We reported on the performance reporting and cybersecurity and supply chain planning of DOD's major IT business programs.[54] Specifically, we found that not all of the programs fully reported operational performance measures to the Dashboard, had approved cybersecurity strategies, or had supply chain risk management plans that addressed information and communications technology. We made three recommendations to DOD to ensure that the programs, as appropriate, (1) report operational performance measures in their reporting to the Dashboard, (2) develop approved cybersecurity strategies, and (3) develop supply chain risk management plans that address information and communications technology. Although DOD concurred with the recommendations and provided corrective action plans intended to help address the recommendations, as of July 2026, we determined that the department had not yet demonstrated that it completed all tasks needed to implement the recommendations. Additionally, we will monitor updates being made to the Dashboard and evaluate how changes to reporting may affect these and other recommendations.
- **June 2023.** We reported on the performance reporting and user training and deployment planning of DOD's major IT business programs.[55] Specifically, we found that not all programs identified at

[53]The recommendations on the software acquisition and business systems acquisition pathways are consistent with broader concerns we have raised about DOD's acquisition reporting in GAO, *Defense Acquisitions: Additional Action Needed to Implement Proposed Improvements to Congressional Reporting,* GAO-22-104687 (Washington, D.C.: Feb. 28, 2022). As of June 2026, DOD has taken actions to implement the two recommendations from that report.

[54]GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, GAO-22-105330 (Washington, D.C.: June 14, 2022).

[55]GAO, *IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Development Planning,* GAO-23-106117 (Washington, D.C.: June 13, 2023).

least the minimum required operational performance metrics in their reporting to the Dashboard or had plans for conducting user training and deployment activities. We made two recommendations to DOD to ensure the programs, as appropriate, (1) identify the required operational performance metrics and (2) develop plans to conduct user training and deployment. DOD concurred with the recommendations and has since implemented both recommendations.

- **July 2024.** We reported on DOD's need to strengthen its software metrics and address continued cybersecurity and reporting gaps.[56] Specifically, we found that programs developing software were not using required metrics and management tools. We made one recommendation to DOD to ensure that programs developing software use the metrics and management tools required by DOD and identified in GAO's *Agile Assessment Guide*. Although DOD stated that it planned to address our recommendation, the department had not yet implemented the recommendation as of July 2026.
- **June 2025.** We further reported on the extent to which DOD IT business programs reported on required categories of performance.[57] Specifically, we found that not all programs fully reported the required performance metrics for each of the required categories. We made one recommendation to DOD to ensure that IT business programs identify and report results data on the minimum number of performance metrics in each category, as appropriate, as part of the department's submission to the Federal IT Dashboard. DOD concurred and reported that it implemented audit checks in April 2024 to have components provide all major IT system performance metrics. In addition, DOD also stated that it had recently increased the frequency of its federal IT Dashboard updates to ensure timely data. While DOD reported implementing audit checks and increasing the frequency of data updates, it has not provided evidence that it identified and reported the minimum required number of metrics. As of July 2026, the recommendation remained open.

March 2023 report on DOD's financial management systems. We reported on DOD's guidance for overseeing its business and financial systems, the reliability of the data collected on business and financial

[56]GAO, *IT Systems Annual Assessment: DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps*, GAO-24-106912 (Washington, D.C.: July 11, 2024).

[57]GAO-25-107649.

system compliance with statutory requirements, and workforce planning.[58] Specifically, we found that the department's guidance for initially approving and annually certifying business systems did not fully address statutory requirements, including auditability requirements. In addition, we found that the data collected on business and financial system compliance with statutory requirements were not reliable and that the department did not have a strategic approach to workforce planning for its financial systems. We made nine recommendations, including that DOD (1) fully develop guidance for overseeing business and financial systems, (2) ensure that the data collected on business and financial system compliance with statutory requirements are reliable, and (3) implement a strategic approach to workforce planning. DOD concurred with seven of the recommendations and partially concurred with the remaining two. As of May 2026, six recommendations had been partially addressed while the remaining three had not yet been implemented. We reiterate the need for DOD to address these recommendations.

January 2026 report on DOD systems modernization. We reported on issues related to DOD's Defense Travel System modernization program and DOD's overall business systems modernization.[59] We made 13 recommendations related to deficiencies and challenges, including a recommendation to develop and implement clearly identifiable leadership roles and responsibilities for the department's business systems modernization efforts, by clarifying the entity or entities with leadership responsibility over the Defense Business Council. We also recommended the department document in policy a process to periodically reassess and adapt the common outcomes included in its modernization strategy in response to strategic plan changes and shifting departmental priorities. DOD concurred with 11 of the recommendations and partially concurred with the remaining two. For the two recommendations where the department partially concurred, DOD explained that its OCIO and Office of the Undersecretary of Acquisition and Sustainment would work to update agency-wide guidance to implement the actions we recommended. We will continue to monitor the department's actions to address our recommendations to determine the extent to which they meet the intent of the recommendations.

[58]GAO, *Financial Management: DOD Needs to Improve System Oversight,* GAO-23-104539 (Washington, D.C.: Mar. 7, 2023).

[59]GAO, *DOD Systems Modernization: Further Action Needed to Improve Travel and Other Business Systems*, GAO-26-107663 (Washington, D.C.: Jan. 22, 2026).

Selected IT Business Programs Reported Numerous Cost and Schedule Changes and Mixed Progress on Performance

According to data from DOD's Office of the CIO, the department's planned expenditures for the 18 selected major IT business programs amounted to about $10.3 billion dollars from FY 2024 through FY 2026. The four largest programs accounted for about 50 percent of the planned cost of the selected portfolio. Additionally, 74 percent of the total cost across the 3 years was for operating and maintaining the systems while the remaining 26 percent was for development and modernization.

Program officials for 11 of the 18 business programs reported experiencing cost or schedule changes since January 2024. These 11 programs include four programs that reported cost increases ranging from $2 million to $394 million (a median of about $59 million) and seven programs that reported a schedule delay ranging from 2 months to 12 months (a median of about 3 months). Three of these programs also reported expecting to rebaseline due to the changes.[60] Program officials provided a variety of reasons for the changes, including new requirements, workforce and contractor developments, changes in administrative priorities, challenges associated with migrating to a cloud environment, and efforts to modernize systems.

Additionally, of the 17 programs that fully or partially reported performance metrics, six programs reported meeting all performance targets, 10 reported meeting at least one performance target, and one reported meeting none. We have previously reported on DOD IT business programs not fully reporting performance metric data and made one recommendation to the department to do so as discussed above.[61]

DOD Planned to Spend $10.3 Billion on the 18 Selected Business Programs from FY 2024 to FY 2026

According to data from DOD's OCIO, the department's planned expenditures for the 18 selected IT business programs amounted to about $10.3 billion from FY 2024 through FY 2026. Of this, about $3 billion was reported as actual costs for FY 2024 and $7.2 billion was reported as planned costs between FY 2025 and FY 2026. Table 1 shows

[60]The Office of Management and Budget's guidance states that agencies and contractors should establish a performance measurement baseline to track progress and report cost and schedule variance. Rebaselines are any revision to the investment's baseline and should be reviewed and approved according to agency governance processes.

[61]GAO-25-107649.

DOD's actual and planned costs of the 18 programs during the 3-year period.[62]

Table 1: The Department of Defense's (DOD) Actual and Planned Costs for 18 Selected Information Technology (IT) Business Programs from Fiscal Year (FY) 2024 Through FY 2026

Dollars in millions (at time of reporting)

Program	FY 2024 (actual)	FY 2025 (projected)	FY 2026 (requested)	3-year total
Navy Enterprise Resource Planning	586	616	776	1,978
Department of Defense Healthcare Management System Modernization	532	624	487	1,643
Advancing Analytics	154	168	428	750
Integrated Personnel and Pay System—Army	199	235	310	745
Enterprise Business System	198	271	247	716
Joint Operational Medicine Information Systems	163	217	232	613
Defense Enterprise Accounting and Management System	166	176	145	486
Global Combat Support System—Army	190	168	118	476
Distribution Standard System	140	138	107	385
Defense Agencies Initiative	132	110	133	376
Global Combat Support System—Marine Corps/Logistics Chain Management	125	121	120	365
Navy Continuous Training Environment	107	114	125	346
Enterprise Business Systems—Convergence	79	122	129	329
Naval—Maintenance, Repair, and Overhaul	73	186	51	309
Army Vantage—Non-classified Internet Protocol Router Network	73	65	77	215
Federal Logistics Information System	74	70	64	208
Procurement Integrated Enterprise Environment	37	77	73	187
Accessions Information Environment	42	71	53	166
Totals	**3,070**	**3,550**	**3,671**	**10,292**

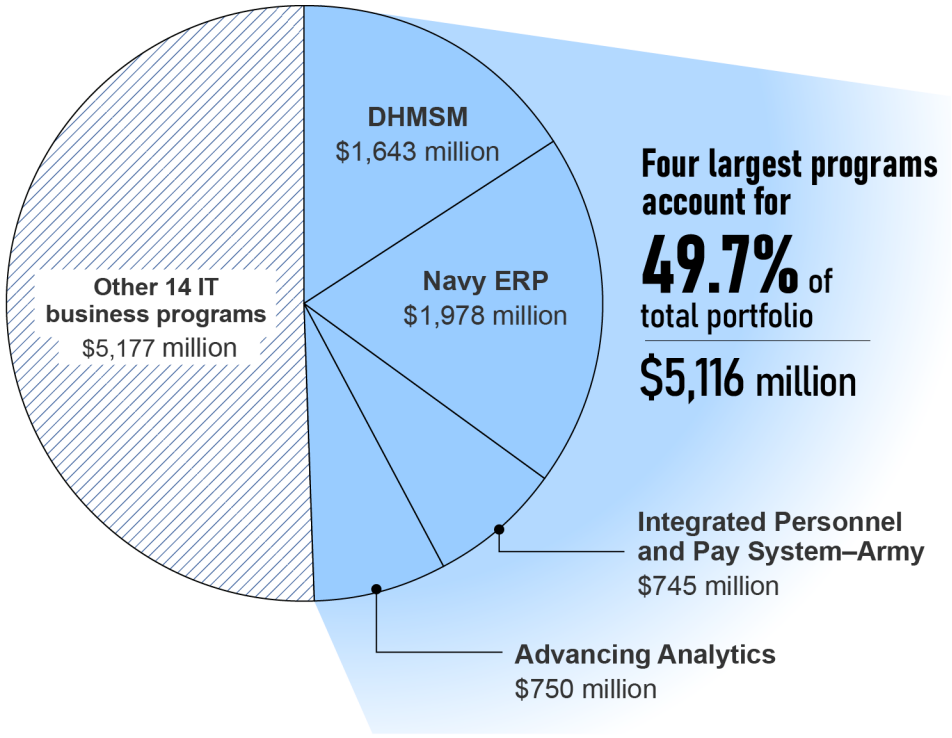
Source: GAO analysis of data from DOD Office of the Chief Information Officer, as of February 2026. | GAO 26-108596

Navy Enterprise Resource Planning (Navy ERP), Department of Defense Healthcare Management System Modernization (DHMSM), Advancing Analytics (Advana), and Integrated Personnel and Pay System–Army (IPPS-A) comprised the top four largest programs in spending. Collectively, these four programs comprised $5.1 billion (49.7 percent) of

[62]Figures are rounded to the nearest million dollars; therefore, subtotals and grand totals may not add precisely due to rounding.

the three-year total allocated to and planned for the portfolio. Figure 3 shows DOD's planned costs for the four largest programs compared to the remaining 14 programs during the 3-year period.

Figure 3: The Department of Defense's (DOD) Planned Costs for the Four Largest Information Technology (IT) Business Programs Compared to the Remaining 14 Selected Programs from Fiscal Year (FY) 2024 through FY 2026



DHMSM = Department of Defense (DOD) Healthcare Management System Modernization, Navy ERP = Navy Enterprise Resource Planning, IT = information technology

Source: GAO analysis of Department of Defense Office of the Chief Information Officer data, as of February 2026. | GAO-26-108596

Based on DOD officials' responses to our questionnaire, three of the four largest programs are in more mature stages of their program life cycles, with one being in mixed stages.

- Navy ERP officials reported that its most recent milestone achieved full deployment ATP in June 2011, with acquisition ATP anticipated as the next milestone for Navy ERP+.[63]
- DHMSM officials reported that its most recent milestone achieved full-rate production in July 2025, with the next milestone being capability support ATP.
- Advana officials reported the program as a data management and software environment which, as such, is designed to evolve with requirements. According to program officials, there is no end to this program's estimated useful life.[64]
- IPPS-A officials reported that its most recent milestone achieved limited deployment ATP in December 2022, with the next milestone being decision authority authorizing entry into the execution phase.

Further, during the 3-year period, DOD's costs for operations and sustainment (O&S)[65] accounted for 74 percent ($7.6 billion) of the total reported $10.3 billion in planned costs for the 18 programs, with the other 26 percent ($2.7 billion) allocated for development, modernization, and enhancement (DME). According to program officials, the average age of all 18 systems is 18 years.[66] We have previously reported on DOD's spending on operating and maintaining systems (e.g., legacy systems), in lieu of spending on development, and that a small number of aging systems can drive portfolio cost growth and put agencies at higher risk of

[63]Navy ERP+ is a modernization effort for the original Navy ERP program, and its costs are included with Navy ERP.

[64]We are currently reviewing Advana as a system DOD is using to help address universe of transactions material weaknesses, which is to be published in a separate GAO report. A universe of transactions is a central repository of financial transactions, such as transactions related to the DOD's inventory, property, or payroll. The universe of transactions is compiled by combining all transactions from multiple accounting systems. A material weakness is a serious deficiency that affects DOD's financial reporting.

[65]*Operations and sustainment* is a term used by DOD to describe a stage of the program's life cycle equivalent to operations and maintenance.

[66]The average age of all the programs was calculated by taking the difference between the starting date, as reported for each program in the questionnaire, and the current year. To account for some programs that reported a specific month along with the year, all program ages were rounded to the year. According to DOD, a legacy business system is a system that the department plans to retire within 36 months. Department of Defense, *Defense Business Systems Investment Management Guidance*, Version 4.1 (Washington, D.C.: June 26, 2018). Based on this definition, these systems include DSS and Navy ERP.

wasteful spending.[67] See appendix II for summaries of all 18 programs that include each program's planned costs for operating and maintaining the systems compared to development.

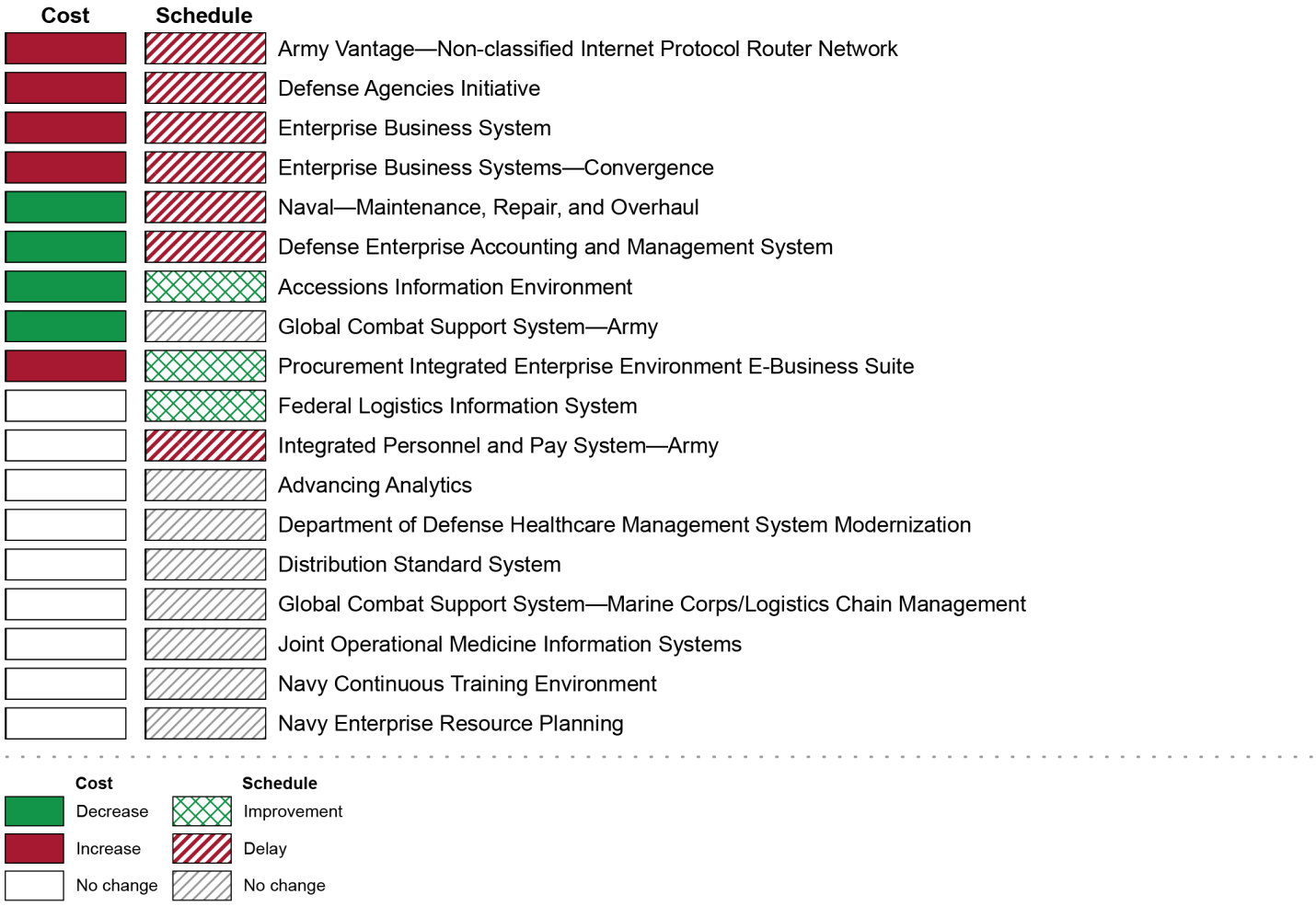
Most Programs Reported Changes in Cost, Schedule, or Both

In addition to our prior reporting on cost and schedule changes, officials for 11 of the selected 18 DOD IT business programs reported cost and/or schedule changes since January 2024.[68] Figure 4 depicts the reported changes.

[67]See, for example, GAO, Information Technology: Federal Agencies Need to Address Aging Legacy Systems, GAO-16-468 (Washington, D.C.: May 25, 2016); *Weapon Systems Annual Assessment: Limited Use of Knowledge-Based Practices Continues to Undercut DOD's Investments*, GAO-19-336SP (Washington, D.C.: May 7, 2019).

[68]See GAO-25-107649, GAO-24-106912, GAO-23-106117, GAO-22-105330, and GAO-21-351.

Figure 4: Selected Department of Defense (DOD) Information Technology (IT) Business Programs Reported Cost and Schedule Changes Since January 2024



Source: GAO analysis of Department of Defense Office of the Chief Information Officer data, as of February 2026. | GAO-26-108596

Officials for nine programs reported cost changes and ten programs reported schedule changes. Specifically, five programs reported cost increases ranging from $2 million to $394 million (a median of about $59 million) and four programs reported cost decreases ranging from $247 million to $330 million (a median of about $247 million).[69] Officials for seven programs reported a schedule delay ranging from 2 months to 12 months (a median of about 3 months) and three programs reported a

[69]Two programs reported cost changes but did not quantify those changes.

schedule improvement ranging from 17 months to 24 months (a median of about 21 months).[70]

Officials for three of the DOD IT business programs reported that they expect to rebaseline their performance measurements as a result of cost or schedule changes. Repeated rebaselines may indicate that programs are not appropriately managing cost, schedule or performance expectations or that they are experiencing other issues.[71] For example, repeated rebaselines might indicate other challenges, such as unexpected technical complexity or issues with program contractors. The three programs that anticipate rebaselining reported the following:

- **Advana.** Advana officials reported expecting to rebaseline every 3 months. The program operates in 3 month increments where new features are planned, capacity is identified, and development within the increment is determined, which could lead to cost and schedule rebaselines.
- **Navy ERP.** Navy ERP officials reported expecting to rebaseline as a result of the federal management budget requirement to reduce contract support services across the Future Years Defense Program.[72]
- **Navy Maintenance, Repair, and Overhaul (N-MRO).** N-MRO officials reported expecting to rebaseline for a new development, integration, testing, training, fielding and deployment plan in response to the cancelation of the N-MRO System Integrator contract.

Program officials for the 11 programs that reported cost or schedule changes and expected rebaselines provided a variety of reasons for the changes, including new requirements asked of the programs, efforts to modernize program systems, challenges associated with migrating to a cloud environment, consolidating service provider contracts, and workforce reductions and reduced contracts.

[70]Five programs reported schedule changes but did not quantify those changes.

[71]Increased costs or extended schedules in updated baselines that reflect additional work directed to programs are not necessarily indicative of the programs mismanaging their originally required work. For example, there could be instances where the program has new requirements as a result of being directed by DOD to provide its services to additional customers.

[72]For additional information about Navy ERP, see GAO, *DOD Financial Management: Navy Needs to Fully Address Strategic Planning and Systems Migration Leading Practices,* GAO-26-107119 (Washington, D.C.: Apr. 14, 2026).

Programs Reported Mixed Progress Towards Achieving Performance Goals

OMB requires DOD to submit current information on the performance of major IT investments to the Federal IT Dashboard. Specifically, according to OMB's Circular No. A-11 guidance, the department is to report on the performance of operational programs in meeting their business or mission purpose. This includes an operational analysis, which is a method of examining the ongoing performance of an operating asset investment and measuring that performance against an established set of cost, schedule, and performance goals.

Additionally, GSA's supporting guidance for complying with OMB's IT investment submission requirements specifies that the programs are to identify a minimum of five performance metrics with achievement data provided.[73] These metrics should best reflect the value of the investment and be consistent with the following four categories:

- **Customer satisfaction (process results).** Measures how well an investment is delivering the goods or services it was designed to deliver. Programs must report a minimum of one metric under this category.
- **Strategic and business results.** Measures the effect an investment has on the performance of the organization itself, including how well the investment contributes to the achievement of the organization's strategic goals. Programs must report a minimum of three metrics under this category. Additionally, at least one of the metrics must have a monthly reporting frequency.
- **Financial performance.** Compares an investment's current performance with a pre-established cost baseline and should support periodic reviews for reasonableness and cost efficiency. Programs are not required to report a metric under this category.
- **Innovation.** Measures an investment's application of new and innovative techniques and demonstrates that the agency has revisited alternative methods of achieving the same mission needs and strategic goals. Programs are not required to report a metric under this category.

The fifth metric can be from any of the four categories. Further, programs are required to use the performance metrics they identified to measure progress toward achieving their goals. Specifically, the guidance states

[73]General Services Administration, *BY 2026 IT Collect Submission Overview*.

that program submissions must include actual results data for all identified metrics.

In our prior reports, we found that not all DOD programs identified the minimum required operational performance metrics in their reporting to the Dashboard and recommended that DOD ensure that the programs do so.[74] In our 2025 report, we noted that officials made changes to address one, but not both of our prior recommendations regarding FY 2025 performance reporting.[75] In April 2026, OMB announced that it was refocusing the Dashboard to report on statutorily required data. We will continue to monitor the data on DOD's major IT programs that are posted to the Dashboard.

Not All Programs Reported Required Categories of Performance

In DOD OCIO's recent performance reports dated February 2026, the majority of the 18 selected programs reported on the required number of metrics. Specifically, of the 17 IT business programs that had operational investments, 15 identified and reported on the minimum required number of performance metrics with data in each category on the Dashboard. However, the remaining two did not do so. Specifically, Army Vantage—Non-classified Internet Protocol Router Network (NIPRNET) only reported one strategic and business metric and no customer satisfaction metrics, and Naval—Maintenance, Repair, and Overhaul only reported one strategic and business metric. According to DOD OCIO officials, one of the 18 selected IT business programs is not yet operational, so DOD did not report performance metrics for that program.

In February 2026, DOD CIO officials responded to our inquiry about obtaining the most recent cost and performance data. They stated that cost and performance metrics data were most recently updated in December 2025, but these changes were not yet reflected on the Dashboard. We will continue to monitor data as it becomes available to understand the department's progress in addressing our prior recommendation about reporting on the correct number of metrics.

Programs Reported Mixed Progress on Performance

Of the 17 programs that identified performance metrics, six programs met all performance targets, 10 met more than one target but not all, and one program, Army Vantage-NIPRNET, met no targets. In total, the 17 programs that identified performance metrics reported 92 metrics (an average of 4.84 metrics per program). Of those 92 total metrics, programs

[74]GAO-22-105330 and GAO-25-107649.

[75]GAO-25-107649.

reported that 67 targets were achieved, 16 targets were not achieved, and programs did not report progress on the remaining nine targets. Table 2 shows the number of metrics reported by each program and the targets met for each reported metric.

Table 2: Reporting of Performance Metrics and Targets by 17 of the 18 Selected Department of Defense (DOD) Information Technology (IT) Business Programs

Program	Number of metrics reported with target achieved	Number of metrics reported with target not achieved
Integrated Personnel and Pay System— Army	7	0
Navy Enterprise Resource Planning	7	3
Advancing Analytics	6	0
Defense Enterprise Accounting and Management System	6	0
Defense Agencies Initiative	5	0
Department of Defense Healthcare Management System Modernization	5	0
Distribution Standard System	5	0
Enterprise Business System	5	0
Navy Continuous Training Environment	5	0
Accessions Information Environment	4	1
Global Combat Support System—Marine Corps/Logistics Chain Management	4	1
Naval—Maintenance, Repair, and Overhaul	2	0
Joint Operational Medicine Information Systems	2	3
Procurement Integrated Enterprise Environment E-Business Suite	2	3
Global Combat Support System—Army	1	0
Federal Logistics Information System	1	4
Army Vantage—Non-classified Internet Protocol Router Network	0	1
Totals[a]	**67**	**16**

Source: GAO analysis of data from DOD's Office of the Chief Information Officer. I GAO-26-108596

[a]Numbers do not add to 92 because programs did not report progress on nine targets.

Selected Programs Reported Mixed Results on Fraud Risk Management, Software Development, and Cybersecurity

As of April 2026, program officials reported mixed results addressing fraud risks. Seven of the 18 programs reported via GAO's questionnaire that their program staff had not received training or did not know about available training over the past two years to recognize and report signs of fraud or tampering in IT systems. Additionally, we found mixed results in terms of programs' use of Agile. Officials for 10 of the 18 selected DOD IT business programs that we identified as actively developing software reported using recommended Agile and iterative approaches and practices.[76] Further, in areas related to tracking customer satisfaction and progress of software development, not all programs used metrics and management tools required by DOD and consistent with ones identified in GAO's *Agile Guide*.[77]

Regarding cybersecurity, 16 of the 18 programs reported conducting a variety of cybersecurity testing and assessments, but six programs had not developed plans to implement zero trust architecture. Additionally, while five programs reported using AI tools to assist in securing systems, three programs did not demonstrate having an approved cybersecurity strategy, as required by DOD.[78]

Program officials reported facing a variety of key challenges related to software development and cybersecurity, including budget constraints, changing customer requirements, and leadership and staff turnover. Officials also reported on program and DOD efforts to address these challenges, which included programs working with product owners for clearer understanding of the requirements earlier in the process, implementing cross training and transition planning, and working to address the absence of key management roles and increase staff.

Programs Reported Mixed Results Implementing Fraud Risk Awareness

GAO's *A Framework for Managing Fraud Risks in Federal Programs* (the Fraud Risk Framework) recommends that program managers develop, document, and communicate an anti-fraud strategy that describes the program's approach to combating fraud.[79] As part of this strategy, developing fraud risk awareness across all staff levels is an important step toward maturing DOD's ability to manage fraud risk. Specifically in

[76]For the purposes of this assessment, we considered programs to be actively developing software if officials reported they were actively developing new software functionality.

[77]GAO-24-105506.

[78]Department of Defense, Instruction 8500.01 and Instruction 5000.89.

[79]GAO-26-107609; GAO-15-593SP.

the IT systems context, people across all staff levels—and particularly those who manage key IT programs that are fundamental to providing reliable financial information for decision-making—need to recognize fraud risks in their functional settings, understand activities involved in a fraud risk assessment, discern how fraud controls might be different from typical financial management controls, receive regular guidance and training, and continue to receive timely anti-fraud messages.

Increasing fraud awareness can enable managers and employees to better detect potential fraud. In addition, increasing fraud awareness externally can help prevent and deter fraud. According to the Fraud Risk Framework, specific features of raising awareness include:

- requiring all employees, including managers, to attend training, initially and on an ongoing basis.
- providing training to stakeholders with responsibility for implementing aspects of a program, including contractors and other external entities. Training and education methods include formal sessions with fraud-specific information tailored to a program's fraud risks. Such information would include the definition of fraud (obtaining something of value through willful misrepresentation) and examples of specific types of fraud. This information can then help participants identify, for example, fraud schemes through red flags or other risk indicators.

Eleven of the 18 programs reported program staff receiving fraud awareness training over the past two years. However, officials for seven of the 18 programs reported program staff not receiving training or not knowing about available training over the past two years to recognize and report signs of fraud or tampering in IT systems. Additionally, while ten programs reported assessing fraud risks facing the program, five programs reported not assessing fraud risks and three programs reported not knowing if they assess fraud risks.

DOD OCIO officials provided several reasons for these shortfalls. They indicated that the department does not currently require training to recognize and report signs of fraud in IT systems, rather that personnel receive mandatory, general fraud awareness training. In addition, programs may not have individual fraud risk management policies in place or program officials may not have been aware of DOD's fraud risk management strategy. Also, officials stated that programs may rely on overarching, enterprise-wide directives and mandatory general training regarding fraud and cybersecurity, among other things, as reflected in

DOD instruction 8500.01.[80] They also stated that fraud risk assessments are integrated into broader risk management frameworks, including continuous evaluation processes and standard cybersecurity vulnerability. While these broad efforts identified are essential to manage fraud risk across the department, programs' reported lack of awareness of training to manage or report fraud specific to the context of their programs highlights the need for more tailored efforts. Without the DOD CIO ensuring that major IT business programs promote and sustain an anti-fraud tone that permeates the programs' organizational culture, there is an increased risk of software development- and cybersecurity-related fraud within IT programs, and the programs risk being vulnerable to exploitation.[81]

Programs Reported Using Recommended Approaches, but Did Not Always Use Required Agile Metrics and Management Tools

The Defense Science Board recommends that DOD implement continuous, iterative software development approaches, such as Agile; development and operations (DevOps); and development, security, and operations (DevSecOps).[82] An iterative development approach is a way of breaking down the development of large applications into smaller pieces or iterations that are continuously evaluated on their functionality, quality, and customer satisfaction. Information obtained during these frequent iterations can effectively assist in measuring progress and allowing developers to respond quickly to feedback, thus reducing technical and programmatic risk. The board assessed that the iterative approach to software development is applicable to DOD and should be adopted as quickly as possible. Table 3 describes the recommended iterative software development approaches.

[80]Department of Defense, Instruction 8500.01.

[81]In addition to this report, GAO has two ongoing reviews looking at fraud-related topics within DOD.

[82]Defense Science Board, *Design and Acquisition of Software for Defense Systems*. The Defense Science Board provides independent advice and recommendations on science, technology, manufacturing, acquisition process, and other matters of special interest to the DOD to the Secretary of Defense.

Table 3: Software Development Approaches Recommended by the Defense Science Board

Approach	Description
Agile	Software is delivered in increments throughout the project, and built iteratively by refining or discarding portions as required based on user feedback.
DevOps	“Development” and “operations” are combined, emphasizing communication, collaboration, and continuous integration between software developers and users.
DevSecOps	“Development,” “security,” and “operations” are combined, emphasizing communication, collaboration, and continuous integration between software developers and users.

Source: GAO analysis of Defense Science Board Information. | GAO 26-108596

According to the Defense Science Board, the main benefit of continuous, iterative software development is that it allows program staff to catch errors quickly and continuously, integrate new code with ease, and obtain user feedback throughout the application development process. This contrasts to the more traditional “Waterfall” software development approach. A Waterfall approach uses linear and sequential phases of development that may be implemented over a longer period before resulting in a single delivery of software capability. Although this more traditional type of approach may be appropriate in some circumstances, the Defense Innovation Board concluded that iterative software development may reduce cost growth compared to a Waterfall approach.[83]

As of April 2026, officials for all 10 IT business programs that we identified as actively developing software reported using at least one of, or a mix of, the recommended iterative development approaches that could result in cost or schedule benefits. Table 4 describes the programs’ reported use of iterative development approaches.

[83]Defense Innovation Board, *Software Is Never Done*.

Table 4: Department of Defense's (DOD) Major Information Technology (IT) Business Programs Actively Developing Software Reported Using Iterative Development Approaches

Program	Agile	DevOps	DevSecOps
Accessions Information Environment	✓	✗	✓
Defense Enterprise Accounting and Management System	✓	✓	✓
Distribution Standard System	✓	✗	✗
Enterprise Business Systems—Convergence	✓	✗	✓
Federal Logistics Information System	✓	✗	✗
Global Combat Support System—Army	✓	✗	✓
Integrated Personnel and Pay System—Army	✓	✓	✗
Joint Operational Medicine Information Systems	✓	✗	✗
Navy Continuous Training Environment	✓	✓	✓
Procurement Integrated Enterprise Environment	✓	✗	✓

Legend: ✓ = Yes; ✗ = No; DevOps = Development and Operations; DevSecOps = Development, Security, and Operations

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

Programs in Active Development Reported Using a Variety of Recommended Practices that Support Iterative Development

The Defense Science Board also recommended that DOD implement certain practices that support continuous, iterative software development, including use of a software factory. A software factory is cloud-based computing used to assemble a set of software tools enabling developers, users, and management to work together on a daily tempo. Furthermore, the board recommended using the creation of a software factory as a key evaluation criterion in the source selection process for software development. Additionally, the Defense Innovation Board also stated that the department should adopt commercial-off-the-shelf software wherever possible.

Officials for each of the 10 programs actively developing software reported using a variety of the recommended iterative practices. For example, officials for nine of the 10 programs reported delivering a minimum viable product (i.e., an early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on). However, only five of the 10 programs reported using a software factory for software development. Table 5 describes the iterative development practices that programs reported using.

Table 5: Department of Defense's (DOD) Major Information Technology (IT) Business Programs Actively Developing Software Reported Using Recommended Iterative Practices

Practice	Description	Number of programs that reported using each practice
Iterative development training for program managers and staff	Development of a training curriculum to create and train a cadre of software-informed program managers, sustainers, and software acquisition specialists.	10 of 10
Software documentation provided at each production milestone	Written text or illustration that accompanies computer software or is embedded in the source code.	10 of 10
Delivery of minimum viable product, followed by successive next viable product[a]	An early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on.	9 of 10
Use of a software factory for development	A low-cost, cloud-based computing technique used to assemble a set of software tools enabling developers, users, and management to work together on a daily basis.	5 of 10
Establishing the creation of a software factory as a key evaluation criterion in the source selection process	Development of a software factory as a factor in evaluating proposals for a potential government contractor.	1 of 10

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

[a]Minimum viable product is an early, usable version of the software to deliver or field basic capabilities to users to evaluate and provide feedback to inform future development.

In 2024, officials from DOD's OCIO stated that the reason the majority of these programs reported not using or creating a software factory is because the business systems heavily leverage commercial off-the-shelf products to deliver their services.

Programs Reported Using AI or Related Tools for Software Development

As mentioned earlier, White House Executive Order 14179 and DOD's *Artificial Intelligence Strategy* were intended to help the department accelerate its efforts towards integrating AI technology across all components and become "AI-first" with a focus on aggressive timelines and measurable outcomes.[84] Using AI tools for software development could support DOD's AI Strategy. Nine of the 18 programs reported using

[84]Exec. Order No. 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, 90 Fed. Reg. 8741 (Jan. 23, 2025). Department of War, *Artificial Intelligence Strategy for the Department of War*.

or planning to use AI as part of their software development efforts.[85] Seven of the 10 programs actively developing software reported currently using or planning to use AI as part of the software development process. Programs reported using AI for requirements development, code generation, testing automation, and model deployment, among other areas, as part of the software development process. Table 6 describes the programs' reported use of AI or other related tools for software development.

Table 6: The Selected Department of Defense (DOD) Information Technology (IT) Business Programs Reported Use of Artificial Intelligence (AI) or Other Related Tools for Software Development

AI system/tool[a]	Description of tool	Number of programs that reported use of each practice
Robotic Process Automation	Interacts with existing applications and automates routine, rules-based tasks by mimicking user interactions.	7 of 18
Generative AI	Creates content, including text, images, audio, or video when prompted by a user.	4 of 18
Machine learning	Detects patterns in datasets and makes predictions based on what the computer learned from those patterns.	3 of 18
Deep learning	Uses many layers of deep neural networks to process data in a way that is inspired by the human brain. Unlike machine learning, which requires supervised inputs, deep learning can also include unsupervised learning.	1 of 18
Other tools		2 of 18

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

[a]These AI systems and tools provide a few examples and are not an exhaustive list.

One program that is using other tools reported using AI to update and create standard operating procedures, functional design specifications and technical design specifications updates. One program that is developing AI features to be incorporated into software noted that the features will be implemented once approved for use.

[85]None of the programs reported using AI for the hardware development process. Section 5002 of the National Defense Authorization Act for Fiscal Year 2021 defines AI as: a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to—(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action. Pub. L. No. 116-283, § 5002(3), 134 Stat. 3388, 4524 (Jan. 1, 2021), codified at 15 U.S.C. § 9401(3).

Eight of the 10 Programs Reported Delivering Software at Least Every 6 Months

OMB guidance calls for certain agency CIOs and chief acquisition officers to ensure and certify that acquisition strategies and plans apply adequate incremental development.[86] OMB defines incremental development as planned and actual delivery of new or modified technical functionality to users at least every 6 months. Additionally, the Defense Innovation Board calls for program staff using Agile and DevSecOps practices to deliver working software to users on a continuing basis—as frequently as every week. According to the Defense Innovation Board, if program officials do not allow for more frequent software delivery, they may lose opportunities to obtain information from users and may face challenges adjusting requirements to meet customer needs.

Officials for eight of the 10 programs in active development reported delivering software functionality every 6 months or less, as called for in OMB's guidance. Officials for one of the two remaining programs, Enterprise Business Systems—Convergence (EBS-C), reported that the average length of time between software releases was 10 to 12 months. EBS-C officials explained that the number of months between each release will vary with the complexity of the release and the available funding. For the other remaining program, Distribution Standard System (DSS) officials reported that its legacy component entered a sustainment-only posture in October 2022, and all regular functional releases have ceased. They added that the only changes applied to the legacy system are mandatory security patches or minor, non-functional performance updates required to maintain operations until the system is decommissioned in 2026.

Eight of the 10 Programs Did Not Use All Required Agile Metrics and Management Tools

DOD's *Agile Metrics Guide* includes guidance for Agile development teams related to metrics for Agile products and services and identifies key metrics, such as those related to the efficiency, quality, and value.[87] DOD's *Agile Metrics Guide* states that it is meant to be a starting point, and that the metrics should be tailored to the program. In addition, DOD's guidebook for DevSecOps activities and tools includes required activities for all programs using the DevSecOps approach to track progress of

[86]OMB, Memorandum M-15-14. OMB's guidance applies to agencies covered by the Chief Financial Officers Act and their divisions and offices, except where otherwise noted. At DOD, the Under Secretary of Defense for Acquisition and Sustainment is the chief acquisition officer.

[87]Department of Defense, *Agile Metrics Guide; Strategy Considerations and Sample Metrics for Agile Development Solutions*, Version 1.2 (Washington, D.C.: Nov. 11, 2020).

software development efforts.[88] This includes tracking customer satisfaction, the number of defects or bugs, and cumulative flow metrics. Programs are also required to use a cumulative flow diagram, a product backlog, and a release plan as management tools.

As previously mentioned, GAO's *Agile Assessement Guide* discusses various metrics and management tools that programs are encouraged to use when pursuing Agile software development.[89] These metrics and management tools are used to measure performance and outcomes intended to help meet customer needs and are best practices for Agile adoption and implementation. Additionally, the Guide describes management tools that programs may use to help capture the metrics and support decision-making. Several of these metrics and management tools are consistent with those required in DOD's guidance.

Officials for the 10 selected DOD IT business programs actively developing software and using Agile, and iterative approaches consistent with Agile, used various metrics and management tools identified in GAO's *Agile Guide*. Table 7 shows the Agile metrics that the DOD IT business programs reported using. Table 8 shows the Agile management tools that the DOD IT business programs demonstrated using through documentation they provided.

[88]Department of Defense, DOD Enterprise *DevSecOps: Activities and Tools Guidebook*, Version 2.5 (Washington, D.C., Sept. 15, 2025).

[89]GAO-24-105506.

Table 7: The Selected Department of Defense (DOD) Information Technology (IT) Business Programs Reported Using Metrics Identified in GAO's *Agile Assessment Guide*

Metric	Description	Number of programs reported using metric
Features or user stories delivered	User stories[a] or story points committed versus user stories or story points accepted.	9 of 10
Number of defects or bugs	Number of defects identified after deploying a product into the production environment.	9 of 10
Velocity	Volume of work accomplished in a specific time by a team,[b] compared against a metric that quantifies the work developers can deliver in each iteration.	8 of 10
Customer satisfaction	Level of satisfaction measured by customers and monitored throughout the development cycle.	7 of 10
Time required to restore service after outage	A measure of time to restore service after an outage.	7 of 10
Metrics that measure a team's adherence to Agile software development best practices	A measure of a team's effort to adhere to Agile software development practices.	7 of 10
Cumulative flow	Flow of work over a period of time represented by a cumulative flow diagram or by reporting the number of features or capabilities delivered in each iteration or release.	6 of 10
Time required for full regression test	A measure of time to complete a full regression test.[c]	6 of 10
Other	Other measures defined by the program.	4 of 10

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

[a]User stories are high-level requirements definitions written in everyday or business language; they are communication tools written by or for users to guide developers, although they can also be written by developers to express non-functional requirements (e.g., security, performance, quality). User stories are weighted for complexity using story points (i.e., units of measure for expressing the overall size of a user story, feature, or other piece of work).

[b]Velocity is unique for each team and should not be used to track overall program progress, compare teams, or to estimate future programs.

[c]Regression tests are the re-running of functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a software change.

Table 8: The Selected Department of Defense (DOD) Information Technology (IT) Business Programs Demonstrated Using Management Tools Identified in GAO's Agile Assessment Guide

Tools used to evaluate software development efforts	Description of tools	Number of programs demonstrated using tool
Sprint backlogs	Ordered list of tasks to be accomplished during the sprint.	8 of 10
Burn up or burn down charts	A visual tool displaying progress via a simple line chart representing work accomplished or remaining work over time.	8 of 10
Release plans	Plans that identify different sets of usable functionality or products scheduled for delivery to customers.	8 of 10
Product backlog	A high-level backlog that contains all the requirements for the entire program.	7 of 10
Cumulative flow diagram	An analytical tool that allows teams to visualize their effort and the program's progress.	5 of 10
Budget baseline	A cost baseline used to measure program performance.	2 of 10
Other	Other tools defined by the program.	1 of 10

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

However, of the 10 programs listed above, eight programs did not report or demonstrate using all the required metrics and tools. Specifically, three programs that reported using only Agile did not report the use of metrics and management tools required of these programs by DOD and consistent with those identified in GAO's Agile Guide, or did not provide documentation demonstrating their use. In addition, five of the six that reported using DevSecOps did not report or demonstrate the use of required metrics and tools. Of these five, two programs did not use either cumulative flow metrics or a cumulative flow diagram. One program did not track customer satisfaction. Two programs did not provide documentation of the product backlog, and one program did not provide documentation demonstrating use of a release plan. Programs that did not use these required Agile metrics and management tools, or did not provide documentation demonstrating their use, reported a variety of reasons for not doing so. These included the programs not yet establishing the management tools and tracking similar metrics but not in the specified format.

In 2024, we recommended that DOD ensure that IT business programs developing software use the metrics and management tools required by DOD and consistent with those identified in GAO's *Agile Guide*.[90]

[90]GAO-24-106912.

Implementing our prior recommendation will provide programs needed information to measure performance and progress of their Agile software development efforts in meeting customer needs.

Programs Reported Conducting Cybersecurity Testing and Using Tools, but Some Continued to Lack Plans and Strategies

DOD Instruction 5000.89 requires that DOD IT program staff complete developmental and operational cybersecurity testing.[91] According to DOD's *Cybersecurity Test and Evaluation Guidebook*,[92] developmental testing is intended to identify cybersecurity issues and vulnerabilities early in the system life cycle to facilitate the remediation and reduction of impact on cost, schedule, and performance. Operational testing is intended to provide information that helps identify vulnerabilities, describe operational effects of discovered vulnerabilities, and resolve operational cybersecurity issues.

Officials for most of the selected IT business programs reported conducting developmental cybersecurity testing, operational cybersecurity testing, or both. Programs may have conducted certain types of cybersecurity testing and not others due, in part, to being in different phases of the system life cycle. For example, systems in an earlier life cycle phase can conduct developmental testing but may not be mature enough to conduct operational testing. Table 9 summarizes the types of cybersecurity testing that the programs reported conducting.

Table 9: The Selected Department of Defense (DOD) Information Technology (IT) Business Programs Reported Conducting Developmental and Operational Cybersecurity Testing

Testing phase	Description	Number of programs that reported conducting testing
Developmental testing	Identifies cybersecurity vulnerabilities before program deployment to help remediate vulnerabilities and reduce the risk of negative impacts on cost, schedule, or performance.	15 of 18
Operational testing	Evaluates operational programs' cybersecurity for effectiveness, suitability, and survivability.	14 of 18

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

[91]Department of Defense, Instruction 5000.89.

[92]Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0.

Additionally, DOD Instructions 5000.75 and 5000.90 require IT program staff to conduct cybersecurity assessments.[93] The assessments are included in programs' cybersecurity testing processes and, according to the *Test and Evaluation Guidebook*, are intended to identify and mitigate exploitable system vulnerabilities.

Officials from 16 of the 18 IT business programs reported conducting some form of cybersecurity assessment. For example, several programs reported conducting full system assessments, tabletop exercises, and penetration tests.[94] Several programs also reported conducting other types of cybersecurity assessments, such as privacy impact assessments.

Six Programs Have Not Yet Implemented Zero Trust Architecture

In addition to conducting cybersecurity testing, programs also reported using zero trust to secure their systems. As previously mentioned, DOD is required to adopt zero trust cybersecurity, and the department has developed a plan to implement a zero trust architecture and strategy by 2027.[95] Officials from 12 of the 18 IT business programs reported implementing zero trust as part of their security framework to varying extents.

However, six programs reported not implementing zero trust architecture. Of those, three reported they have plans to implement zero trust architecture in the future. The remaining three reported not having plans to implement it. DOD CIO officials stated that some programs are leveraging a concurrent strategy as they are part of a larger effort. For example, DSS (a program within DLA) leverages a DLA enterprise strategy which incorporates the principles of zero trust architecture. Regardless, it will be important that these programs establish plans to

[93]Department of Defense, Instruction 5000.75; Department of Defense, *Cybersecurity For Acquisition Decision Authorities and Program Managers*, Instruction 5000.90 (Washington D.C.: Dec. 31, 2020).

[94]Full-system assessments are performed on a complete system to evaluate its compliance with specified requirements. Tabletop exercises involve small teams who discuss how they would respond to various simulated emergency or rapid response situations and prepare briefings on potential threat scenarios and responses. Penetration tests involve independent assessors typically working under specific constraints, who attempt to circumvent or defeat the security features of an information system.

[95]Exec. Order No. 14028. Pub. L. No. 117-81, § 1528, 135 Stat. 1541, 2044-2048 (Dec. 27, 2021). Department of Defense, *DOD Zero Trust Capability Execution Roadmap (COA 1)* (Jan. 06, 2023).

meet the 2027 deadline, and we will continue to monitor the progress of these programs' efforts.

Five Programs Reported Using Artificial Intelligence Tools to Secure Systems

Programs using AI tools, such as threat detection or prevention, or vulnerability assessment, to assist in securing systems could support the previously mentioned Executive Order 14179 and DOD's *Artificial Intelligence Strategy*.[96] Officials from five of the 18 programs reported using AI software tools to assist in securing systems to some extent. Seven of the 18 programs reported having no plans to use these tools, while six programs plan to use AI software tools in the future to assist in securing systems. Officials from programs that are not currently using AI software tools reported reasons for not using it, including that they have not assessed AI's potential to assist in securing systems or are piloting a team to explore AI capabilities. Others noted they have not been directed to use AI tools to secure systems.

Three Programs Did Not Have an Approved Cybersecurity Strategy

DOD Instruction 8500.01, *Cybersecurity*, and DOD Instruction 5000.89 require that DOD IT program officials use an approved cybersecurity strategy.[97] This strategy is to include information such as cybersecurity and resilience requirements and key system documentation for cybersecurity testing and evaluation analysis and planning. Such information is intended to ensure that program staff plan for and document cybersecurity risk management efforts, which begin early in the program's life cycle.

In our June 2022 report, we found that 10 of DOD's major IT business programs had not demonstrated having an approved cybersecurity strategy.[98] We recommended that DOD's CIO ensure that these programs develop such a strategy, as appropriate, and DOD concurred with our recommendation. However, in our last three annual assessments we found that several of the department's major IT business programs lacked an approved strategy and reiterated the importance of ensuring that these programs develop one.[99]

[96]Exec. Order No. 14179, 90 Fed. Reg. 8741, *Removing Barriers to American Leadership in Artificial Intelligence* (Jan. 23, 2025). Department of War, *Artificial Intelligence Strategy for the Department of War*.

[97]Department of Defense, Instruction 8500.01 and Instruction 5000.89.

[98]GAO-22-105330.

[99]GAO-23-106117, GAO-24-106912, and GAO-25-107649.

As of April 2026, three out of 18 programs had not provided us with documentation of their approved strategy.[100] Officials for one of the programs reported planning to develop such a strategy by September 2026. The second program reported having a strategy but did not provide us with documentation. Officials from the last program reported not being required to have a strategy as their program is not an official DOD program of record. However, this program began in 2016 and has been listed as a major IT investment on the Dashboard, signifying the importance of the program and the need for such a strategy. Implementation of our prior recommendation in this area should help position the programs to effectively manage cybersecurity risks and mitigate threats.

Officials Reported Key Software Development and Cybersecurity Challenges and Efforts to Address Them

Officials from the 18 selected IT business programs included in our review reported facing a number of key challenges associated with software development and cybersecurity and reported actions they have taken to address them. Table 10 summarizes the reported challenges and actions taken by the programs.

[100]We did not evaluate the content of these cybersecurity strategies.

Table 10: The Selected Department of Defense (DOD) Information Technology (IT) Business Programs Reported Key Software Development and Cybersecurity Challenges and Actions to Address Them

Challenge	Reported action taken by programs to address challenge	Number of programs that reported challenge
Budget constraints	• Prioritizing requirements, balancing limited resources and competing needs • Making trade-offs between functionality, security, and timelines	10 of 18
Changing customer requirements	• Providing user training • Working with owners for clearer understanding of the requirements earlier in the process	8 of 18
Technical issues related to software development and commercial off-the-shelf software	• Slowing down and pausing adoption of new tools	7 of 18
Leadership and staff turnover	• Implementing cross training and transition planning • Working to address the absence of key management roles and increase staff	7 of 18
Rapidly evolving cybersecurity requirements	• Leveraging continuous monitoring to comply with cybersecurity requirements	5 of 18

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

DOD Continues to Implement Legislative and Policy Changes

DOD continues to make efforts to improve its management of IT investments as a result of legislative and policy changes. DOD's efforts include revising its business systems investment management guidance, modernizing its BEA, adopting zero trust cybersecurity, developing AI acquisition guidance, updating its agency strategic plan, and implementing activities in support of cost efficiency initiatives.

Defense business systems investment management guidance. In October 2024, DOD published the Defense Business Systems (DBS) Certification & Management Guidance.[101] This guidance is intended to provide the background and instruction necessary to execute DBS certification and management processes. It identifies which DBS are subject to DBS certification and management processes; describes process enablers; and outlines the relationship between key governing bodies and certification and management execution. The department also

[101]Department of Defense, Office of the Chief Information Officer, *Defense Business Systems Certification and Management Guidance* (October 2024).

publishes an annual certification guidance memorandum. The most recent guidance addresses the FY 2026 certification process for priority DBS.[102] However, DOD did not demonstrate that these documents fully address all statutory requirements discussed in our March 2023 report on DOD's financial management systems.[103] In that report, we recommended that DOD address this issue. We will continue to monitor the department's efforts to fully implement the recommendation.

Business enterprise architecture modernization. In April 2026, DOD published the BEA Guidebook.[104] DOD officials indicated that the guidebook will build upon the BEA framework and is to provide the instructions necessary to develop and maintain a modernized BEA.[105] Further, the guidebook outlines procedures for DOD organizations to (1) assign the implementation of laws, regulations, and policies to operational activities, and (2) align Defense Business Systems to operational activities within DOD's architecture capability.

Zero trust cybersecurity. In July 2024, we reported that, to accelerate zero trust adoption, the department was to develop complementary capability roadmap courses of action, including those that would address commercial and government-owned services to support these efforts.[106] In our June 2025 report, the department indicated that it had not developed additional roadmaps, but was continuing to make efforts to adopt zero trust across the department.[107] For example, the department identified progress made in the development of zero trust proof of concepts and functional assessments.

In December 2025, the department indicated that it continues to actively foster zero trust adoption through various initiatives towards achieving its

[102]Department of Defense, *FY26 Defense Business Systems Annual Certification Guidance* (June 2025).

[103]GAO-23-104539.

[104]Department of War, *DoW Business Enterprise Architecture Guidebook* (April 2026).

[105]The BEA framework, published in January 2024, establishes DOD's modernization approach and highlights component roles and responsibilities for BEA development, maintenance, and usage. DOD further elaborated that the framework is a high-level document intended to establish a federated, question-based, and data-centric architecture.

[106]GAO-24-106912.

[107]GAO-25-107649.

FY 2027 target goals. These initiatives include engaging with components and conducting comprehensive zero trust training. In February 2026, the department indicated that many components are experiencing resource gaps to procure zero trust solutions and conduct zero trust assessments. Specifically, DOD CIO officials reported that there are only two approved teams to conduct zero trust assessments within the department. These officials also reported that the Zero Trust Portfolio Management Office is working on addressing the resource gaps and increasing the number of zero trust assessment teams.

AI acquisition guidance. In our June 2023 report, we recommended that the Secretary of Defense ensure that the Chief Digital and AI Officer, in conjunction with other DOD acquisition policy offices as appropriate, prioritize establishing department-wide AI acquisition guidance.[108] In that report, we noted that it is especially important for DOD to have guidance that provides critical oversight, resources, and provisions for acquiring AI given that the U.S. will face AI-enabled adversaries in the future.

DOD concurred with our recommendation and in response DOD's Chief Digital and Artificial Intelligence Office (CDAO) developed the *DOD Data, Analytics and Artificial Intelligence Adoption Strategy*, released in November 2023.[109] It provides a foundation and strategic guidance for DOD components on adopting, scaling, and leveraging emerging AI capabilities. In August 2024, the department indicated that the CDAO was developing the "*Adopt, Buy, Create*" framework appendix to the strategy that was to aid DOD components in deciding whether to adopt an existing government or DOD solution, buy a commercial solution, or create a custom solution when acquiring data, analytics, and AI capabilities. However, in December 2025, the department reported that CDAO did not publish an appendix to the 2023 strategy but plans to issue a new AI strategy and future guidance on AI adoption based on this new strategy.

As mentioned earlier, in 2026, DOD published the *Artificial Intelligence Strategy*.[110] This strategy is intended to help the department accelerate its efforts towards integrating AI technology across all components and become "AI-first." It also directs the CDAO to ensure that all existing AI policy guidance at the department aligns with directives in this strategy.

[108]GAO-23-105850.

[109]Department of Defense, *Data, Analytics, and Artificial Intelligence Adoption Strategy* (November 2023).

[110]Department of Defense, *Artificial Intelligence Strategy for the Department of War*.

The strategy calls for seven pilot projects in three mission areas—warfighting, intelligence, and enterprise—with a focus on, among other things, aggressive timelines and measurable outcomes. We will continue to monitor DOD's efforts towards adoption of AI and determine if these efforts fully address our prior recommendation.

Agency strategic plan. Following the repeal of the position of DOD's Chief Management Officer in January 2021, the Director of Administration and Management was designated as the Performance Improvement Officer (PIO) and serves as the senior official for defense reform under the Deputy Secretary of Defense.[111]

10 U.S.C. §132a, as added by Section 902 of the NDAA for FY 2025, establishes the PIO in statute and mandates certain duties and responsibilities to the position.[112] The PIO is responsible for overseeing business process modernization, overseeing the implementation of solutions to issues identified in GAO's High-Risk List, and serving as the co-chair for the Defense Business Council with the DOD CIO. Further, the PIO has the responsibility of updating and implementing DOD's Strategic Management Plan (SMP).

We previously reported on the 2022-2026 SMP, which served as the department's agency strategic plan and included DOD's Annual Performance Plan for FY 2025 defining specific performance goals and measures along with targets to help ensure successful implementation of the plan.[113] In December 2025, the department stated that it is pivoting from the SMP to the Department of War Strategic Plan in support of the President's Management Agenda.[114] This Strategic Plan sets four agency priority goals for the FY 2026-2027 cycle, which are intended to drive near-term improvements towards achieving long-term strategic objectives. Further, this plan includes the department's FY 2027 Agency Performance Plan, which identifies specific agency priority goals, performance goals, measures, and targets to ensure successful

[111]Pub. L. No. 116-283, § 901, 134 Stat. 3388, 3794 (Jan. 1, 2021); Deputy Secretary of Defense Memorandum, *Disestablishment of the Chief Management Officer, Realignment of Functions and Responsibilities, and Related Issues* (Sept. 1, 2021).

[112]Pub. L. No. 118-159, § 902, 138 Stat. 1773, 2025 (Dec. 23, 2024) (10 U.S.C. 132a).

[113]Department of Defense, *DOD Strategic Management Plan-Fiscal Years 2022–2026* (updated April 2024).

[114]Department of War, *Department of War Strategic Plan in Support of the President's Management Agenda Fiscal Years 2026 – 2030.*

implementation. For example, one of the goals is to retire legacy and duplicative defense business systems. Specifically, department components must be 80 percent compliant with their planned retirements of these systems by September 30, 2026, and 95 percent compliant by September 30, 2027.

Cost efficiency initiatives. In response to Executive Order 14222,[115] the Secretary of Defense issued two IT service contract implementation memoranda in May 2025 to DOD components.[116] The memoranda required DOD components to obtain approval from the Deputy Secretary of Defense and a Department of Government Efficiency (DOGE) team within DOD prior to executing a new IT service contract or task order, within certain parameters. On June 23, 2025, the Under Secretary of Defense for Acquisition and Sustainment issued a third memorandum which directed components to provide requirements packages for new IT service contracts or task orders, within certain parameters, to the DOD DOGE team for review prior to execution.[117] The memorandum described the DOGE review process and the contents of the package that would be required for the review. Senate Report 119-39, accompanying the National Defense Authorization Act for Fiscal Year 2026,[118] directs GAO to conduct a review of the potential impacts of these memoranda. This review is ongoing with an expected reporting date later this year.

We will continue to monitor actions DOD is taking to address how it manages IT investments, including through this series of annual reports (mandated under 10 U.S.C. § 3072), and review the potential impacts of

[115]Executive Order No. 14222, *Implementing the President's "Department of Government Efficiency" Cost Efficiency Initiative*, 90 Fed. Reg. 11095 (Feb. 26, 2025).

[116]Department of Defense, Secretary of Defense, *Implementation of Executive Order 14222 – Department of Government Efficiency Cost Efficiency Initiative*, Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, and Defense Agency and DOD Field Activity Directors (Washington, D.C: May 27, 2025); and *Implementation of Executive Order 14222 – Department of Government Efficiency Cost Efficiency Initiative: Contract Guidance*, Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, and Defense Agency and DOD Field Activity Directors (Washington, D.C.: May 27, 2025).

[117]Department of Defense, Under Secretary of Defense for Acquisition and Sustainment, *Implementation of Department of Government Efficiency Cost Efficiency Initiative*, Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, and Defense Agency and DOD Field Activities Directors (Washington, D.C: June 23, 2025).

[118]S. Rep. No. 119-39, at 160 (2025).

the memoranda on cost efficiency initiatives.[119] Additionally, we will monitor DOD's efforts associated with its business systems modernization, approach to business transformation within high-risk areas, and adoption of AI and zero trust cybersecurity.

Conclusions

DOD planned to spend $10.3 billion from FY 2024 through FY 2026 on the 18 selected IT business programs, with several programs reporting that they have experienced cost increases and schedule delays. While DOD improved its performance reporting, not all programs reported required categories of performance and most programs reported mixed progress in achieving performance goals. Not identifying and reporting results data on performance metrics in each category makes it harder to determine if these programs are achieving their intended goals. We previously made recommendations to DOD to address these reporting shortfalls.

Programs reported mixed results implementing fraud risk awareness. While 11 of the 18 programs reported staff receiving fraud awareness training over the past two years, the remaining seven programs reported that staff were either unaware of or did not receive training to recognize and report signs of fraud or tampering in IT systems. Until the department's CIO ensures that all major IT business system programs have in place IT fraud awareness practices to reduce fraud risk, it remains at increased risk of software development- and cybersecurity-related fraud within IT programs.

Regarding software development and cybersecurity, eight of the programs developing software did not demonstrate use of Agile metrics and management tools, as required by DOD. In addition, while five programs used AI tools to secure their systems, six programs had not developed plans to implement zero trust in their cybersecurity frameworks by DOD's 2027 deadline, and three programs did not have an approved cybersecurity strategy. Implementing our prior recommendations regarding use of Agile metrics and cybersecurity planning will further

[119]Pub. L. No 115-232, § 833, 132 Stat. 1636, 1858 (Aug. 13, 2018), adding a new section 2229b, Comptroller General assessment of acquisition programs and initiatives, to Title 10 of the U.S. Code, since renumbered § 3072. We are to report on these assessments no later than March 30 of each year. The provision has been amended several times, most recently extending our reviews until 2029. Pub. L. No. 118-159, § 813(a)(3), 138 Stat. 1773, 1980 (Dec. 23, 2024). S. Rep. No. 119-39, at 160 (2025).

DOD's goals of efficient and secure business software development efforts.

Recommendation for Executive Action

We reiterate that DOD should address the six recommendations previously made that have not yet been implemented from our prior DOD IT business systems annual assessment reviews. In addition, we are making one new recommendation to the Department of Defense:

The Secretary of Defense should direct the Chief Information Officer, in collaboration with the Office of the Under Secretary of Defense (Comptroller), to ensure that major IT business programs promote and sustain an anti-fraud tone that permeates the program's organizational culture through training focused on increasing awareness of fraud and fraud risk, recognition of fraud risks in relevant functional settings, and awareness of fraud risk assessment activities. (Recommendation 1)

Agency Comments and Our Evaluation

In written comments provided via email, a Principal Director from the Office of the Chief Information Officer at the Department of Defense stated that the agency partially agreed with our recommendation. The department stated that to promote and sustain an enterprise-wide anti-fraud posture, the DOD CIO's office integrates comprehensive financial management functional requirements into the annual Defense Business Systems Certification Guidance. In addition, the department reported that it has designated its Office of the Under Secretary of Defense (Comptroller) as the dedicated entity to oversee fraud risk management at the department since July 2020. Despite these efforts, we emphasize the importance of coordination between offices to ensure that relevant fraud and fraud risk training is offered and provided, and that staff of major IT business programs are aware of training opportunities. We will monitor DOD's actions in response to our recommendation. In addition, DOD provided technical comments, which we have incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretary of Defense; the Secretaries of the Army, Navy, and Air Force; and the Chief Information Officer. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions on matters discussed in this report, please contact me at dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

//SIGNED//

Vijay A. D'Souza
Director, Information Technology and Cybersecurity

List of Committees

The Honorable Roger Wicker
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Mitch McConnell
Chair
The Honorable Christopher Coons
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Ken Calvert
Chairman
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our specific objectives for this assessment were to (1) examine what progress selected Department of Defense (DOD) information technology (IT) business programs have made on cost, schedule, and performance, (2) determine the extent to which DOD has implemented key fraud risk management, software development, and cybersecurity practices for selected programs, and (3) describe actions that DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address objectives 1 and 2, we identified and selected 18 business programs among 31[1] that DOD listed as major IT investments in its fiscal year (FY) 2026 Federal IT Dashboard (Dashboard) data at time of initial collection in July 2025.[2] We developed a questionnaire that focused on programs' cost and schedule, software development, cybersecurity, software risks and challenges, and fraud risk management. We conducted a pretest of the questionnaire with one program to ensure that the questions were clear, unbiased, and would be consistently interpreted. The pretest allowed us to obtain initial program feedback and helped ensure that officials within each program would understand the questions. We then administered the questionnaire to the 18 program offices in September 2025 and asked program staff to provide their responses. We also analyzed program officials' responses to the questionnaire and followed up with programs through April 2026.

Regarding the data collected via our questionnaire, we took steps to reduce measurement error and non-response error. We did not validate all responses provided by the program offices, although we followed up with programs when responses were unclear or inconsistent. Where we discovered discrepancies, we clarified the responses accordingly. In addition to pretesting the questionnaire, we also corroborated selected responses with supporting documentation and interviews with program

[1]Of the 20 programs that we initially selected, we excluded two during our review. Specifically, Navy Personnel and Pay within the MyNavy Human Resource portfolio was canceled in February 2026, and program officials for the Warfighting Training Tools—Simulation, Training and Instrumentation investment did not submit their questionnaire responses in time for us to conduct a review of the program's efforts.

[2]The Federal IT Dashboard is a public, government website operated by the General Services Administration (GSA) at https://itdashboard.gov. It includes streamlined data on IT investments to enable agencies and Congress to better understand and manage federal IT portfolios. In April 2026, the Chief Information Officer of the United States announced that the IT Dashboard is refocusing on reporting statutorily required data.

officials. We determined that the data were reliable for the purposes of this report.

To address the first objective, we selected the 18 major IT business programs from the 31 that DOD listed as major IT investments in its FY 2026 Federal IT Dashboard data as of July 2025, for review. The criteria used to select the 18 programs among 31 included those that had a FY2024-2025 funding amount of $250 million or higher, and programs that DOD designated as new major IT investments for 2026.[3] We also analyzed data provided by DOD's Office of the Chief Information Officer (OCIO) as of February 2026, to examine DOD's costs for the 18 selected IT business programs during the 3-year period from FY 2024 through FY 2026. Additionally, we analyzed investment spending data provided by DOD's OCIO to determine the costs for operating and maintaining the systems compared to developing and modernizing the system.

To assess and ensure the reliability of the budget data DOD's OCIO provided, we compared the data to cost information and supporting documentation provided by program officials to identify any obvious inconsistencies. In addition, we prepared and sent program summaries to the 18 program offices in April 2026 and asked program staff to review them to confirm their accuracy. These summaries are included in appendix II. We also met with officials in DOD's OCIO and asked them to validate program cost information included in the report. We determined that the cost data were sufficiently reliable for our reporting purposes.

We also analyzed program officials' responses to the questionnaire described above. The questionnaire addressed issues such as whether (1) programs had experienced cost or schedule changes since January 1, 2024, and (2) whether programs had rebaselined or expected to rebaseline as a result of the changes.[4] Additionally, we collected and analyzed supporting documentation, including key program documents pertaining to each program's life cycle cost, schedule estimates, and baselines (e.g., acquisition program baseline reports).

[3]We used $250 million because it was a natural break in the funding amount of potential investments to select for this review.

[4]The Office of Management and Budget's guidance states that agencies and contractors should establish a performance measurement baseline to track progress and report cost and schedule variance. Rebaselines are any revision to the investment's baseline and should be reviewed and approved according to agency governance processes.

Further, we analyzed programs' performance metrics data provided by the DOD OCIO, and compared the data to Office of Management and Budget (OMB) guidance.[5] We inspected the data for missing or incomplete records, inconsistencies, and other obvious errors. We determined that the performance data were sufficiently reliable for our reporting purposes.

To address the second objective, we analyzed information obtained from our questionnaire on the fraud risk management, software development, and cybersecurity practices used by the 18 programs, including 10 programs that we identified as actively developing software.[6] We aggregated the program office responses to our questionnaire and compared the information to relevant guidance and best practices (e.g., Defense Science Board and Defense Innovation Board reports, DOD instructions, DOD's zero trust framework, and OMB guidance) to identify gaps.[7] Further, we collected responses from program officials about the extent of their fraud risk management practices regarding training staff to recognize and report fraud in IT systems. We compared these responses against best practices relevant to fraud risk awareness in GAO's *Framework for Managing Fraud Risks in Federal Programs* to identify gaps and risks.[8] In addition, we collected and analyzed key information and supporting documents related to the programs' reported practices,

[5]FY 2026 reporting requirements for IT investments are contained in Section 55 of OMB's Circular No. A-11 (July 2024) guidance and in GSA's supporting guidance for complying with OMB's submission requirements. Office of Management and Budget, *Preparation, Submission, and Execution of the Budget,* Circular No. A-11, (Washington, D.C.: July. 2024); General Services Administration, *BY 2026 IT Collect Submission Overview* (Washington, D.C.: Dec. 2024).

[6]For the purposes of this assessment, we considered programs to be actively developing software if officials reported that they were actively developing new software functionality. Officials for the other eight programs reported either that their software development efforts were to sustain existing functionality, involved minor enhancements, or that they were not actively developing software.

[7]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 (Washington, D.C.: Feb. 2, 2017, incorporating Change 2, Jan. 24, 2020); Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense*, Test and Evaluation*, Instruction 5000.89 (Nov. 19, 2020); OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[8]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

including their use of metrics and management tools identified in GAO's Agile Assessment Guide for developing software, and compared it to DOD's guidance.[9] In doing so, we identified risks associated with not following the guidance and best practices that may affect acquisition outcomes relative to cost, schedule, and performance. For programs that did not follow the guidance or demonstrate having such documentation, we followed up with program officials and officials within the DOD OCIO for reasons why they did not do so.

We also reviewed information on each program's reported implementation of artificial intelligence (AI) as part of DOD's cybersecurity efforts. In addition, we assessed information from program officials about having approved cybersecurity strategies, and their plans for and implementation of zero trust and security frameworks. We compared this information against plans DOD has in place for the department to implement zero trust architecture targets by 2027. Finally, we obtained information from program officials about key challenges the programs were facing related to software development and cybersecurity and actions these programs reported taking to mitigate them. We also obtained information from DOD CIO officials about actions the department was taking to address the challenges.

To address the third objective, we reviewed and summarized DOD's actions to implement previously identified legislative and policy changes that could affect its IT acquisitions.[10] The scope of the objective included planned improvements to the department's IT portfolio management (i.e., updates to its investment management guidance and business enterprise architecture modernization), adoption of zero trust principles, establishment of a department-wide AI acquisition guidance, overview of DOD's agency strategic plan, and execution of cost efficiency initiatives. To describe the actions DOD has taken toward implementation of these changes, we summarized policies, plans, and guidance provided by DOD. We also met with DOD CIO officials to discuss their efforts in these areas

[9]GAO, *Agile Assessment Guide: Best Practices for Adoption and Implementation*, GAO-24-105506 (Washington, D.C.: Dec. 15, 2023).

[10]The previously identified legislative and policy changes are discussed in GAO, *IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Cybersecurity Planning*, GAO-25-107649 (Washington, D.C.: June 12, 2025).

and coordinated with the GAO team conducting a companion assessment examining weapon system acquisition programs.[11]

We conducted this performance audit from June 2025 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[11]GAO, *Weapon Systems Annual Assessment: Requiring Mature Technologies Could Enable Shift to Rapid Delivery*, GAO-26-108457 (Washington, D.C.: July 2, 2026).

Appendix II: Program Summaries

This appendix provides summaries of the 18 selected Department of Defense (DOD) information technology (IT) business programs included in our review. Each summary provides key information about the program, including the program's planned expenditures and reported software development practices. These programs are:

•Advancing Analytics

•Accessions Information Environment

•Army Vantage—Non-classified Internet Protocol Router Network

•Defense Agencies Initiative

•Defense Enterprise Accounting and Management System

•DOD Healthcare Management System Modernization

•Distribution Standard System

•Enterprise Business System

•Enterprise Business Systems—Convergence

•Federal Logistics Information System

•Global Combat Support System—Army

•Global Combat Support System—Marine Corps/Logistics Chain Management

•Integrated Personnel and Pay System—Army

•Joint Operational Medicine Information Systems

•Navy Enterprise Resource Planning

•Navy Continuous Training Environment

•Naval—Maintenance, Repair, and Overhaul

•Procurement Integrated Enterprise Environment

Advancing Analytics (Advana)

Program
Advancing Analytics (Advana)

Software development approaches
Agile; Incremental; Development, Operations (DevOps); Development, Security, and Operations (DevSecOps)

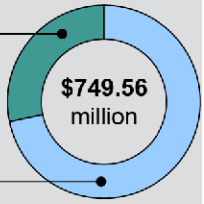
Average time of software deliveries

1-3 Months | 4-6 | 7-9 | 10-12 | 13+

Cost, fiscal years 2024–2026

Total operations and maintenance (O&M) **$211.91 mil**

Total development, modernization and enhancement (DME) **$537.66 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *No change*

Schedule: *No change*

Rebaseline: *Expects to at 3 month increments*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

Advana is an operational enterprise technology platform that automates the collection, normalization, and tabulation of disparate sources of business and mission data, providing DOD's military and business decision-makers with decision support analytics, visualizations, and data tools.

Program essentials (reported by DOD officials as of May 2026)

Lead DOD component: Defense-wide	**Program owner:** Chief Digital and Artificial Intelligence Officer	**Year investment began:** 2016
Acquisition pathway: Software acquisition		**Last milestone achieved:** Deliver capabilities
Next planned milestone: Program of record decision		**CIO evaluation rating:** 2 – Moderately high risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 11: Advancing Analytics's (Advana) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	Yes
Software development approach	Agile, Incremental, DevOps, DevSecOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	317
Planned releases	Unknown
Average time between releases	1-3 months

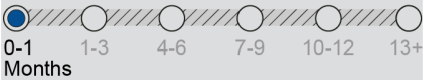
Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Accessions Information Environment (AIE)

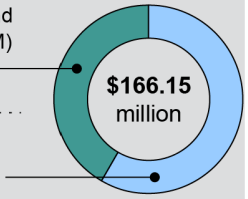
Program
Accessions Information Environment (AIE)

Software development approaches
Agile; Incremental; Development, Security, and Operations (DevSecOps)

Average time of software deliveries



Cost, fiscal years 2024–2026



Cost and Schedule Changes
(since January 2024)

Cost: *Decrease*

Schedule: *Improvement*

Rebaseline: *Yes. In March 2024.*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

AIE is an integrated enterprise system intended to support Army-wide talent acquisition and serve as the Army's accessions system of record to interface and synchronize with multiple Army human resource agencies and systems.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Army	**Program owner:** Army	**Year investment began:** 2017
Acquisition pathway: Software acquisition execution phase Defense Business System sub-pathway		**Last milestone achieved:** Decision authority authorized entry into execution phase and delivery of minimum viable capability release
Next planned milestone: Deliver enlisted mission Minimum viable product		**CIO evaluation rating:** 5 – Low risk
Year investment is estimated to reach end of useful life: Not applicable - Army's enterprise recruiting and accessioning system using continuous agile delivery		

Table 12: Accessions Information Environment's (AIE) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile, Incremental/Iterative, DevSecOps
Use of artificial intelligence in software development	Yes
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	19
Planned releases	19
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Army Vantage—Non-classified Internet Protocol Router Network (Army Vantage-NIPRNET)

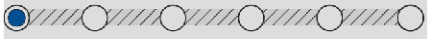
Program

Army Vantage—Non-classified Internet Protocol Router Network (Army Vantage-NIPRNET)

Software development approaches

Other: Defense Data Orchestration Framework

Average time of software deliveries

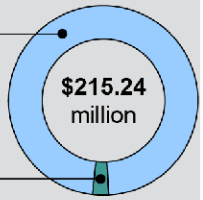


0-1 Months | 1-3 | 4-6 | 7-9 | 10-12 | 13+

Cost, fiscal years 2024–2026

Total operations and maintenance (O&M) **$209.33 mil**

Total development, modernization and enhancement (DME) **$5.91 mil**



Combined total (O&M + DME)

Cost and Schedule Changes *(since January 2024)*

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

Army Vantage-NIPRNET is intended to serve as the Army's authoritative data source, providing senior leaders with data to inform strategic decisions, display total force data types, produce predictive analytics, and facilitate real-time or near real-time decision-making. It is also intended to support the Army's execution of its primary functions to organize, train, and sustain forces in support of the National Military Strategy.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Army	**Program owner:** Army	**Year investment began:** 2019
Acquisition pathway: Acquisition of service		**Last milestone achieved:** Capability support authority to proceed (ATP)
Next planned milestone: Declaring the system as authoritative		**CIO evaluation rating:** 5 – Low risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 13: Army Vantage—Non-classified Internet Protocol Router Network (Army Vantage-NIPRNET) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	Yes
Software development approach	Defense Data Orchestration Framework
Use of artificial intelligence in software development	Yes
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	Not specified
Planned releases	N/A
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Defense Agencies Initiative (DAI)

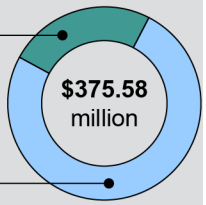
Program
Defense Agencies Initiative (DAI)

Software development approaches
Incremental

Average time of software deliveries

Cost, fiscal years 2024–2026
Total operations and maintenance (O&M) **$283.47 mil**

Total development, modernization and enhancement (DME) **$92.11 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *Yes. In November 25, 2025.*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

DAI is intended to transform the budget, finance, and accounting operations of DOD components to achieve accurate and reliable information in support of financial accountability and improved decision-making. The initiative is a critical part of the department's financial management modernization efforts.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Defense-wide	**Program owner:** Defense Logistics Agency (DLA)	**Year investment began:** 2017
Acquisition pathway: Defense business systems		**Last milestone achieved:** Limited deployment ATP
Next planned milestone: Limited deployment ATP		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2040		

Table 14: Defense Agencies Initiative's (DAI) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	Yes
Software development approach	Incremental
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	No
Use of commercial off-the-shelf products	Yes
Software releases to date	8
Planned releases	13
Average time between releases	10-12 months

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Defense Enterprise Accounting and Management System (DEAMS)

Program
Defense Enterprise Accounting and Management System (DEAMS)

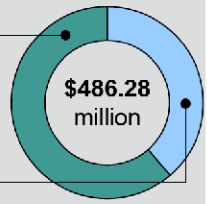
Software development approaches
Agile; Development, Operations (DevOps); Development, Security, and Operations (DevSecOps)

Average time of software deliveries

Cost, fiscal years 2024–2026

Total operations and maintenance (O&M) **$298.11 mil**

Total development, modernization and enhancement (DME) **$188.17 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *Decrease*

Schedule: *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

DEAMS integrates Air Force financial information to produce accurate and timely financial statements, support accurate budget forecasting, and allow for the retirement of certain legacy systems.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Air Force	**Program owner:** Air Force	**Year investment began:** 2003
Acquisition pathway: Defense business systems		**Last milestone achieved:** Full deployment ATP
Next planned milestone: Capability support ATP		**CIO evaluation rating:** 3 – Medium risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 15: Defense Enterprise Accounting and Management System's (DEAMS) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile, DevOps, DevSecOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	No
Use of commercial off-the-shelf products	Yes
Software releases to date	114
Planned releases	N/A, about 100 releases a year over the course of the total software development effort
Average time between releases	Less than 1 month (every 2.4 days)

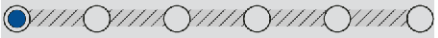
Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

DOD Healthcare Management System Modernization (DHMSM)

Program
Department of Defense Healthcare Management System Modernization (DHMSM)

Software development approaches
N/A (Deploys commercial off-the-shelf products)

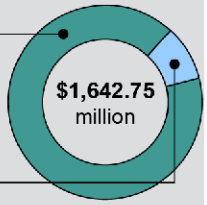
Average time of software deliveries



Cost, fiscal years 2024–2026

Total operations and maintenance (O&M) **$1,492.02 mil**

Total development, modernization and enhancement (DME) **$150.73 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

DOD established DHMSM to acquire and field a configurable and scalable electronic health record system to replace DOD's legacy healthcare systems. DHMSM is to replace these systems with a modernized, commercial-off-the-shelf system that enables improved sustainability, flexibility, and continuity of care.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Defense-wide	**Program owner:** Defense Health Agency (DHA)	**Year investment began:** 2014
Acquisition pathway: Defense business systems		**Last milestone achieved:** Full-rate production (full deployment decision)
Next planned milestone: Capability support ATP		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2034		

Table 16: Department of Defense Healthcare Management System Modernization's (DHMSM) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	N/A (deploys commercial off-the-shelf products)
Software development approach	N/A
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	N/A
Software documentation provided at specified intervals	N/A
Iterative development training for program managers and staff	N/A
Use of a software factory	N/A
Use of commercial off-the-shelf products	Yes
Software releases to date	10,700+
Planned releases	89 planned through end of fiscal year 2026
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Distribution Standard System (DSS)

Program
Distribution Standard System (DSS)

Software development approaches
Agile; Waterfall

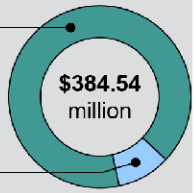
Average time of software deliveries

N/A, in sustainment

Cost, fiscal years 2024–2026

Total operations and maintenance (O&M) **$347.38 mil**

Total development, modernization and enhancement (DME) **$37.16 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

DSS is the Defense Logistic Agency's (DLA) standard automated system for managing warehouse operations and distributing DOD materiel (i.e., equipment and supplies). The legacy system provides service and support to the warfighter, peacekeepers, and federal and civilian customers.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Defense-wide	**Program owner:** DLA	**Year investment began:** 1992
Acquisition pathway: Defense business systems		**Last milestone achieved:** Capability support ATP
Next planned milestone: N/A (program is in sustainment)		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2026		

Table 17: Distribution Standard System's (DSS) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	48
Planned releases	92
Average time between releases	N/A

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Enterprise Business System (EBS)

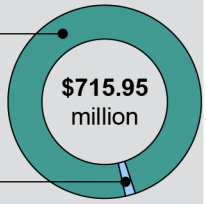
Program
Enterprise Business System (EBS)

Software development approaches
Agile; Incremental; Development, Security, and Operations (DevSecOps)

Average time of software deliveries

Cost, fiscal years 2024–2026
Total operations and maintenance (O&M) **$702.94 mil**

Total development, modernization and enhancement (DME) **$13.02 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

EBS is the Defense Logistic Agency's (DLA) financial system of record and is intended to provide business capabilities enabling supply chain management for energy and non-energy commodities, including enterprise procurement and property.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Defense-wide	**Program owner:** DLA	**Year investment began:** 2001
Acquisition pathway: Defense business systems		**Last milestone achieved:** Capability support ATP
Next planned milestone: Capability support ATP		**CIO evaluation rating:** 3 – Moderate risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 18: Enterprise Business System's (EBS) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	Yes
Software development approach	Agile; DevSecOps; Incremental
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	2,010
Planned releases	2,688
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Enterprise Business Systems—Convergence (EBS-C)

Program
Enterprise Business Systems—Convergence (EBS-C)

Software development approaches
Agile; Development, Security, and Operations (DevSecOps)

Average time of software deliveries

Cost, fiscal years 2024–2026
Total operations and maintenance (O&M)
$0 mil

Total development, modernization and enhancement (DME)
$328.83 mil

Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)
Cost: *Increase*
Schedule: *Delay*
Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

EBS-C is intended to modernize and consolidate five Army Enterprise Resource Planning (ERP) business systems through a cloud-native, integrated finance-logistics transactional core, with a simplified warfighter/workforce interface, and fundamentally transformed business processes to become as "commercial-as-possible and military-as-necessary" while improving the security of data.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Army	**Program owner:** Army	**Year investment began:** 2024
Acquisition pathway: Software acquisition pathway as a Defense Business System		**Last milestone achieved:** Decision authority authorized entry into software acquisition pathway execution phase in September 2024
Next planned milestone: Deliver capabilities for Ammunition Warehouse Management		**CIO evaluation rating:** 5 – Low risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 19: Enterprise Business Systems—Convergence's (EBS-C) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile, DevSecOps
Use of artificial intelligence in software development	Yes
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	1
Planned releases	Minimum of 8
Average time between releases	Maximum of 1 year

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Federal Logistics Information System (FLIS)

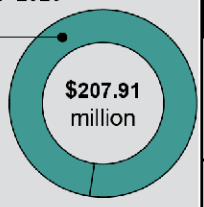
Program
Federal Logistics Information System (FLIS)

Software development approaches
Agile; Waterfall

Average time of software deliveries

Cost, fiscal years 2024–2026
Total operations and maintenance (O&M)
$207.91 mil

Total development, modernization and enhancement (DME)
$0 mil



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *No change*

Schedule: *Improvement*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

FLIS is a government-wide program implemented by the Defense Logistics Agency (DLA) intended to manage the common logistics language known as the Federal Catalog Program (FCP). FLIS is a suite of applications which enables users to create, store, maintain, and share logistics information. This information is used to procure, requisition, fulfill, and dispose of supplies and equipment for the U.S. Military Services and other federal and civil agencies.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Defense-wide	**Program owner:** DLA	**Year investment began:** 1987
Acquisition pathway: Defense business systems		**Last milestone achieved:** Development contract award decision or development decision (milestone B)
Next planned milestone: Low-rate initial production (LRIP) or limited deployment and operational test (milestone C)		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 20: Federal Logistics Information System's (FLIS) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile; Waterfall
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	No
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	No
Use of commercial off-the-shelf products	Yes
Software releases to date	14
Planned releases	26
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

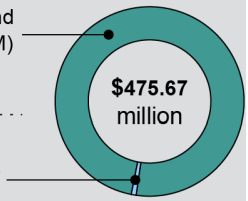
Global Combat Support System—Army (GCSS-A)

Program
Global Combat Support System—Army (GCSS-A)

Software development approaches
Agile; Incremental; Development, Security, and Operations (DevSecOps)

Average time of software deliveries

Cost, fiscal years 2024–2026



Cost and Schedule Changes
(since January 2024)

Cost: *Decrease*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

GCSS-A is intended to provide functional services to Army's business mission areas. The system is focused on supply operations, tactical maintenance, and enterprise aviation logistics, along with associated logistics management and tactical finance functionality.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Army	**Program owner:** HQ Army Defense Clandestine Services (DCS) G-4 (Logistics), Program Executive Office Enterprise; Project Manager, Defense Integrated Business Systems (DIBS)	**Year investment began:** 2002
Acquisition pathway: Business capability acquisition cycle (BCAC)		**Last milestone achieved:** BCAC Phase 5: Capability support
Next planned milestone: Deliver capabilities		**CIO evaluation rating:** 5 – Low risk
Year investment is estimated to reach end of useful life: 2032		

Table 21: Global Combat Support System-Army's (GCSS—A) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile; DevSecOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	No
Use of commercial off-the-shelf products	Yes
Software releases to date	96
Planned releases	4 major quarterly, 8 minor per year
Average time between releases	1-3 months

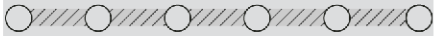
Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Global Combat Support System—Marine Corps/Logistics Chain Management (GCSS-MC/LCM)

Program
Global Combat Support System—Marine Corps/Logistics Chain Management (GCSS-MC/LCM)

Software development approaches
Agile

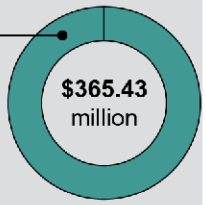
Average time of software deliveries



0-1 1-3 4-6 7-9 10-12 13+
Unknown

Cost, fiscal years 2024–2026
Total operations and maintenance (O&M)
$365.43 mil

Total development, modernization and enhancement (DME)
$0 mil



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

GCSS-MC/LCM provides the foundation for all logistics information required by the Marine Corps. The system's future functions will be focused on enhancing capabilities in the areas of warehousing, distribution, logistics, decision support, depot maintenance, and integration with emerging technologies to increase asset visibility.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Navy, Marine Corps	**Program owner:** Marine Corps	**Year investment began:** 2004
Acquisition pathway: Defense business systems		**Last milestone achieved:** Full deployment
Next planned milestone: Currently in capability support		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2035		

Table 22: Global Combat Support System—Marine Corps/Logistics Chain Management's (GCSS-MC/LCM) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	No
Software development approach	Agile
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	No
Use of a software factory	No
Use of commercial off-the-shelf products	Yes
Software releases to date	N/A (only software updates and security patches)
Planned releases	N/A
Average time between releases	N/A (software updates and security patches conducted monthly)

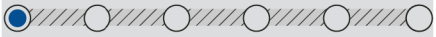
Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Integrated Personnel and Pay System—Army (IPPS-A)

Program
Integrated Personnel and Pay System—Army (IPPS-A)

Software development approaches
Agile; Development, Operations (DevOps)

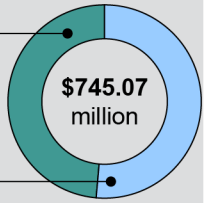
Average time of software deliveries



Cost, fiscal years 2024–2026

Total operations and maintenance (O&M) **$361.58 mil**

Total development, modernization and enhancement (DME) **$383.49 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *No changes*

Schedule: *Delay*

Rebaseline: *Yes. In 2020.*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

IPPS-A is intended to deliver a single, integrated personnel and pay system to all Army components that streamlines Army human resources, enhances the efficiency and accuracy of Army personnel and pay procedures, provides audit compliance with law, terminates legacy systems, and supports over 1 million soldiers.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Army	**Program owner:** Army	**Year investment began:** 2014
Acquisition pathway: Defense Business System		**Last milestone achieved:** Limited deployment ATP(s)
Next planned milestone: Decision authority authorizes entry into software acquisition pathway execution phase		**CIO evaluation rating:** 5 – low risk
Year investment is estimated to reach end of useful life: Not applicable; IPPS-A is using continuous Agile delivery		

Table 23: Integrated Personnel and Pay System—Army's (IPPS-A) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile, DevOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	884
Planned releases	1,600
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

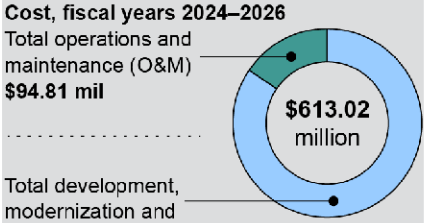
Joint Operational Medicine Information Systems (JOMIS)

Program
Joint Operational Medicine Information Systems (JOMIS)

Software development approaches
Agile

Average time of software deliveries

Cost, fiscal years 2024–2026



Cost and Schedule Changes
(since January 2024)

Cost: *No changes*

Schedule: *No changes*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

JOMIS is a portfolio of products/information systems that pursues efforts to sunset costly and difficult-to-maintain legacy systems and modernizes medicine information systems to provide integrated, timely, and accurate information to make critical command and control and medical decisions.

Program essentials (reported by DOD officials as of May 2026)

Lead DOD component: Defense-wide	**Program owner:** Defense Health Agency (DHA), Program Executive Office Defense Healthcare Management Systems	**Year investment began:** 2016
Acquisition pathway: Software acquisition, defense business systems, middle tier of acquisition, major capability acquisition, acquisition of service	**Last milestone achieved:** JOMIS has multiple products in the process of development and delivery. For example, Theater Blood-Mobile (TBLD-M) is at milestone decision authority (MDA) approval	
Next planned milestone: TBLD-M – Limited deployment	**CIO evaluation rating:** 4 – Moderately low risk	
Year investment is estimated to reach end of useful life: 2045		

Table 24: Joint Operational Medicine Information Systems' (JOMIS) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	SAFe Agile
Use of artificial intelligence in software development	Yes
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	N/A
Use of commercial off-the-shelf products	Yes
Software releases to date	For example, one system has delivered 140 releases.
Planned releases	Depending on the JOMIS system, capability block releases are delivered twice annually and those that follow a sprint cycle deliver releases on a 2-week or 3-month cadence.
Average time between releases	4-6 months

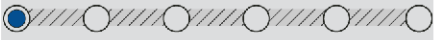
Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Navy Enterprise Resource Planning (Navy ERP)

Program
Navy Enterprise Resource Planning (NAVY ERP)

Software development approaches
Agile; Waterfall; Incremental; Development, Security, and Operations (DevSecOps)

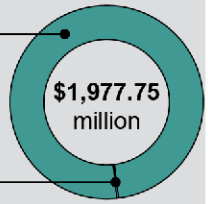
Average time of software deliveries



Cost, fiscal years 2024–2026

Total operations and maintenance (O&M) **$1,968.96 mil**

Total development, modernization and enhancement (DME) **$8.79 mil**



Combined total (O&M + DME)

Cost and Schedule Changes *(since January 2024)*

Cost: *No change*

Schedule: *No change*

Rebaseline: *Expects to*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

Navy ERP is Navy's legacy financial system of record. The system is intended to streamline Navy's business operations and is focused on financial and supply chain management.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Navy	**Program owner:** Navy	**Year investment began:** 2004
Acquisition pathway: Defense business systems		**Last milestone achieved:** Full deployment ATP
Next planned milestone: N/A (program is in sustainment)		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2045		

Table 25: Navy Enterprise Resource Planning's (Navy ERP) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	Yes
Software development approach	Agile, Waterfall, Incremental, DevSecOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	No
Use of commercial off-the-shelf products	Yes
Software releases to date	220
Planned releases	220
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Navy Continuous Training Environment (NCTE)

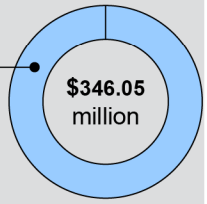
Program
Navy Continuous Training Environment (NCTE)

Software development approaches
Agile; Incremental; Development, Operations (DevOps); Development, Security, and Operations (DevSecOps)

Average time of software deliveries

Cost, fiscal years 2024–2026
Total operations and maintenance (O&M)
$346.05 mil

Total development, modernization and enhancement (DME)
$0 mil



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

NCTE is an integrated architecture that combines live training ranges with the synthetic environment (e.g., a system of networks, constructive simulation, simulation routing equipment, and data translation devices) to form a distributed range for training and experimentation to expose deploying forces to threats they may encounter while deployed.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Navy	**Program owner:** Navy	**Year investment began:** 2004
Acquisition pathway: N/A		**Last milestone achieved:** N/A (program does not follow DOD acquisition milestones and timelines)
Next planned milestone: N/A (program does not follow DOD acquisition milestones and timelines)		**CIO evaluation rating:** 5 – Low risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 26: Navy Continuous Training Environment's (NCTE) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile, DevOps, DevSecOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	No
Use of commercial off-the-shelf products	Yes
Software releases to date	48
Planned releases	4 releases a year through life of the software
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Naval—Maintenance, Repair, and Overhaul (N-MRO)

Program

Naval—Maintenance, Repair, and Overhaul (N-MRO)

Software development approaches

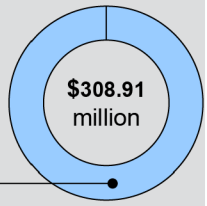
Agile; Incremental; Development, Operations (DevOps); Development, Security, and Operations (DevSecOps)

Average time of software deliveries

Cost, fiscal years 2024–2026

Total operations and maintenance (O&M)
$0 mil

Total development, modernization and enhancement (DME)
$308.91 mil



Combined total (O&M + DME)

Cost and Schedule Changes *(since January 2024)*

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *Expects to*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

N-MRO is a replacement program of record for designated aviation and maritime organizational, intermediate, and depot-level maintenance tool suites.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Navy	**Program owner:** Navy	**Year investment began:** 2017
Acquisition pathway: Software acquisition		**Last milestone achieved:** Planning phase
Next planned milestone: Execution phase		**CIO evaluation rating:** 3– Medium risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 27: Naval—Maintenance, Repair, and Overhaul's (N-MRO) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	No
Use of an iterative development approach	Yes
Software development approach	Agile; Incremental; DevOps; DevSecOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	0
Planned releases	Not identified
Average time between releases	10-12 months

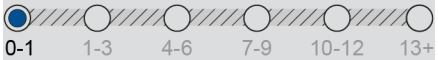
Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Procurement Integrated Enterprise Environment (PIEE)

Program
Procurement Integrated Enterprise Environment (PIEE)

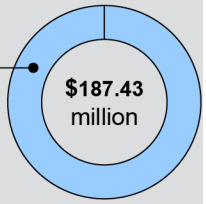
Software development approaches
Agile; Incremental; Development, Security, and Operations (DevSecOps)

Average time of software deliveries



Cost, fiscal years 2024–2026
Total operations and maintenance (O&M)
$187.43 mil

Total development, modernization and enhancement (DME)
$0 mil



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2024)

Cost: *Increase*

Schedule: *Improvement*

Rebaseline: *Yes. October 1, 2025*

Source: GAO analysis of Department of Defense data, as of February 2026; DOD program questionnaire responses as of April 2026. | GAO-26-108596

Program description

PIEE is a DOD enterprise procurement portfolio that leverages a cloud-based platform to support rapid development and deployment of capabilities. The portfolio of systems automates procurement transactions from award to payment, connecting procurement systems across DOD.

Program essentials (reported by DOD officials as of April 2026)

Lead DOD component: Defense Logistics Agency (DLA)	**Program owner:** DLA	**Year investment began:** 1999
Acquisition pathway: Defense business systems		**Last milestone achieved:** Capability support ATP
Next planned milestone: Capability support		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: No estimated end date as there are no plans to retire or decommission the system		

Table 28: Procurement Integrated Enterprise Environment's (PIEE) Reported Software Development Approaches and Practices

Approach or practice	Program response
Developing new software functionality	Yes
Use of an iterative development approach	Yes
Software development approach	Agile, incremental, DevSecOps
Use of artificial intelligence in software development	No
Delivery of a minimum viable product	Yes
Software documentation provided at specified intervals	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	5
Planned releases	6
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of April 2026. | GAO-26-108596

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Vijay A. D'Souza, dsouzav@gao.gov.

Staff Acknowledgments

In addition to the contact named above, principal contributors to this report were Eric Trout (Assistant Director), Gerard Aflague (Analyst in Charge), Madison Brown, Andrea Harvey, Smith Julmisse, Jess Lionne, and Richard Sayoc. Other key contributors included Beatrice Alff, Amanda Andrade, Irina Carnevale, Erin Carson, Alissa Czyz, Heather Dunahoo, Amanda Gill, Michael Holland, Igor Koshelev, Jennifer Leotta, Melissa Melvin, Scott Pettis, Daniel Ramsey, Nolan Roosa, Claire Saint-Rossy, Walter Vance, Adam Vodraska, Marshall Williams, Jr., and Merry Woo.