United States Government Accountability Office

Report to Congressional Committees

June 2025

IT SYSTEMS ANNUAL ASSESSMENT

DOD Needs to Improve Performance Reporting and Cybersecurity Planning

GAO-25-107649

June 2025

IT SYSTEMS ANNUAL ASSESSMENT

DOD Needs to Improve Performance Reporting and Cybersecurity Planning

GAO Highlights

Highlights of GAO-25-107649, a report to congressional committees

Why GAO Did This Study

Information technology is critical to the success of DOD's major business functions. These functions include 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 sixth such review 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 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 24 DOD IT business programs that DOD listed as major IT investments in its FY 2025 submission to the Federal IT Dashboard. In analyzing the FY 2025 Dashboard data, GAO examined DOD's planned expenditures for these programs from FY 2023 through FY 2025.

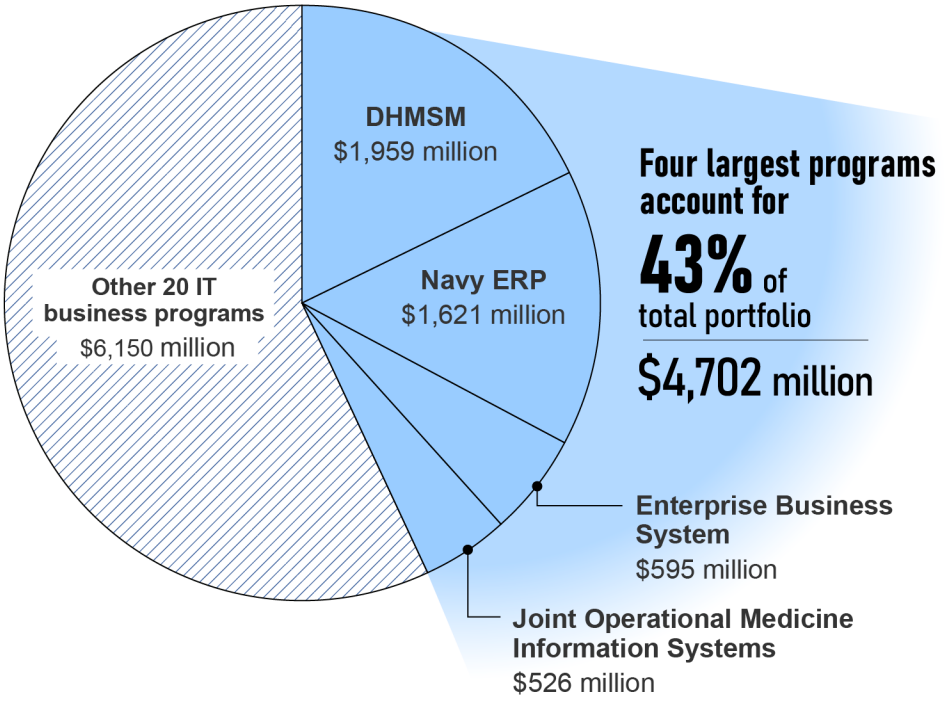
GAO also administered a questionnaire to the 24 program offices to obtain and analyze information about cost and schedule changes that the programs reported experiencing since January 2023.

View GAO-25-107649. For more information, contact Vijay D'Souza at dsouzav@gao.gov.

What GAO Found

According to the Department of Defense's (DOD) fiscal year (FY) 2025 Federal IT Dashboard (Dashboard) data, the department planned to spend $10.9 billion on its portfolio of 24 major IT business programs from FY 2023 through FY 2025. The four largest programs account for 43 percent of the planned spending (see figure).

The Department of Defense's (DOD) Planned Costs for the Four Largest IT Business Programs Compared to the Remaining 20 Selected Programs from Fiscal Year (FY) 2023 through FY 2025



DHMSM = DOD Healthcare Management System Modernization
Navy ERP = Navy Enterprise Resource Planning

Source: GAO analysis of data provided by the Department of Defense CIO officials, as of February 2025. | GAO-25-107649

Officials from 14 of the 24 IT business programs reported cost and/or schedule changes since January 2023. This included 12 programs that reported cost increases of $6.1 million to $815.5 million (a median of $173.5 million) and seven programs that reported a schedule delay ranging from 3 months to 48 months (a median of 15 months).

While DOD improved its performance reporting, not all programs reported required categories of performance and most programs reported mixed progress in achieving performance goals. If they have operational investments, programs are required to identify and track a minimum of five performance metrics in the

Further, GAO compared programs' performance metrics data reported on the Dashboard to OMB guidance and met with DOD Office of the Chief Information Officer officials to determine reasons for differences between how metrics data were reported and reporting guidance.

To address the second objective, the questionnaire also sought information about software development and cybersecurity practices. This included programs' use and documentation of Agile tools and metrics and development of cybersecurity strategies, including zero trust cybersecurity. GAO compared the responses and documentation against relevant 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 (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 and develop AI acquisition guidance. GAO also met with DOD Office of the Chief Information Officer officials to discuss their efforts in these areas.

What GAO Recommends

GAO reiterates that DOD address the five 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 IT business programs identify and report results data on the minimum required number of categories of performance metrics.

DOD concurred with GAO's recommendation and described actions it was taking to address the recommendation.

categories of customer satisfaction, strategic and business results, financial performance, and innovation. Of the 19 IT business programs that had operational investments, 14 identified the minimum required number of performance metrics in each category. However, the remaining five did not do so. Accordingly, the extent to which these five programs were improving customer satisfaction, increasing financial performance, and delivering innovative approaches is unknown.

Regarding achieving performance goals, of the 19 programs that identified metrics, one program met all performance targets, 17 programs met at least one target, and one program met no targets.

Of the 24 programs, 11 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, three of the 11 programs did not use metrics and management tools required by DOD and consistent with GAO's *Agile Assessment Guide* (see table). GAO previously recommended that DOD address this issue.

Department of Defense (DOD) Major IT Business Programs Actively Developing Software Reported Using Iterative Development Approaches and Practices

Development approach or practice	Number of programs that reported using each approach or practice
Using recommended Agile and iterative approaches	11 of 11
Using required metrics and management tools to track customer satisfaction and progress of software development	8 of 11

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

Further, two programs did not have an approved cybersecurity strategy. GAO has previously recommended that all programs develop such a strategy. In addition, four programs had not developed plans to implement zero trust architecture in their cybersecurity frameworks by DOD's 2027 deadline. GAO will continue to monitor the department's progress in developing plans to address zero trust.

Department of Defense (DOD) Major 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	22 of 24
Implementing zero trust architecture as part of the security framework	20 of 24

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

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, and developing AI acquisition guidance. GAO will continue to monitor DOD's efforts to improve how the department manages its IT investments.

Contents

Tables

Figures

Abbreviations

AI	artificial intelligence
AFIPPS	Air Force Integrated Personnel and Pay System
ATP	authority to proceed
BEA	business enterprise architecture
CDAO	Chief Digital and Artificial Intelligence Office
CIO	Chief Information Officer
CON-IT	Contracting Information Technology
DAI	Defense Agencies Initiative
DHMSM	Department of Defense Healthcare Management System Modernization
DBS	Defense Business Systems
DOD	Department of Defense
DevOps	Development and Operations
DevSecOps	Development, Security, and Operations
DME	development, modernization, and enhancement
EBS	Enterprise Business System
EBS-C	Enterprise Business Systems—Convergence
FY	fiscal year
GFEBS	General Fund Enterprise Business System
GSA	General Services Administration
JOMIS	Joint Operational Medicine Information Systems
MRO	Maintenance Repair and Overhaul
NAVAIR-ALE	Naval Air Systems Command—Aviation Logistics Environment
Navy ERP	Navy Enterprise Resource Planning
NDAA	National Defense Authorization Act
N-MRO	Naval—Maintenance, Repair, and Overhaul
O&S	operations and sustainment
OMB	Office of Management and Budget
PIO	Performance Improvement Officer
SMP	Strategic Management Plan
TMIP-J	Theater Medical Information Program—Joint

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

June 12, 2025

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 deter war, DOD relies heavily on the use of 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) 2025, the department requested approximately $64.1 billion for its total FY 2025 IT and cyber activities,[1] including $47.8 billion for its unclassified IT investments.[2] These investments include DOD's major IT business programs, which are intended to help the department sustain its key operations.

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 sixth 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 software development and cybersecurity practices for selected programs, and (3)

[1]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: President's Budget (PB) 2025 Budget Request* (March 2024).

[2]This figure does not reflect all funding requested for DOD's IT investments. For example, classified systems are not included. In addition, not all DOD IT expenditures are reported separately from their respective programs. For instance, our annual assessments of DOD's weapons programs include programs that do not report software expenditures separately. See GAO, *Weapon Systems Annual Assessment: DOD Leaders Should Ensure Programs Are Structured for Speed and Innovation*, GAO-25-107569 (Washington, D.C.: June 11, 2025).

[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-25-107569.

describe actions DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, we selected the 24 major IT business programs that DOD listed as major IT investments in its FY 2025 Federal IT Dashboard (Dashboard) data, as of July 2024, for review.[4] We analyzed the Dashboard data to examine how much DOD reported planning to spend on the 24 major IT business programs during the 3-year period (from FY 2023 through FY 2025). 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). We also analyzed program officials' responses to a questionnaire we developed and administered to all 24 programs in September 2024. The questionnaire focused on programs' cost and schedule, software development, user engagement, cybersecurity, and software risks and challenges. Further, for the 24 programs, we analyzed DOD's performance data included in its FY 2025 reporting to the Dashboard and compared the data to Office of Management and Budget (OMB) guidance.[5]

For the second objective, we analyzed information obtained from our questionnaire on the software development and cybersecurity practices used by the 24 programs, including 11 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,

[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]FY 2025 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. General Services Administration, *BY 2025 IT Collect-Submission Overview* (Washington, D.C.: Dec. 2023).

[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.

and OMB guidance) to identify gaps.[7] We also collected and analyzed key information and supporting documents related to the programs' reported practices and reviewed information about programs' implementation of artificial intelligence (AI) and plans for and implementation of zero trust cybersecurity. Further, 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 reviewed actions DOD has taken to implement previously identified legislative and policy changes that could affect its IT acquisitions.[8] In addition, we reviewed actions DOD has taken to implement legislative requirements on adopting zero trust cybersecurity. To describe the actions DOD has taken toward implementation of these changes, we reviewed policies, plans, and guidance provided by DOD; reports that the department submitted to Congress; and internal program documentation. We also coordinated with the GAO team conducting a companion assessment for FY 2025 examining major defense acquisition programs.[9] Appendix I provides a more detailed discussion of our objectives, scope, and methodology.

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

[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, (incorporating change 2, [Jan. 24, 2020]) (Washington, D.C.: Feb. 2, 2017); 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]The previously identified legislative and policy changes are discussed in 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).

[9]GAO-25-107569.

Background

In support of its military operations, DOD manages many IT investments encompassing communications, command and control, and business systems. For DOD's FY 2025 budget the department requested approximately $64.1 billion for its total IT and cyber activities, including $47.8 billion for its unclassified IT investments. These investments include DOD's major IT business programs, which are intended to help the department sustain its key operations (e.g., human capital, health care, contracting, logistics, and financial management).[10]

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.[11] The department subsequently issued new policies to continue replacing the old approach. In addition, DOD Instruction 5000.02 was updated in June 2022, describing a transition from the department's previous acquisition approach.

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 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

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

[11]Department of Defense, *Operation of the Adaptive Acquisition Framework,* Instruction 5000.02 (Washington, D.C.: Jan. 23, 2020).

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 defense business systems acquisition pathway to align defense 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.[12] 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."

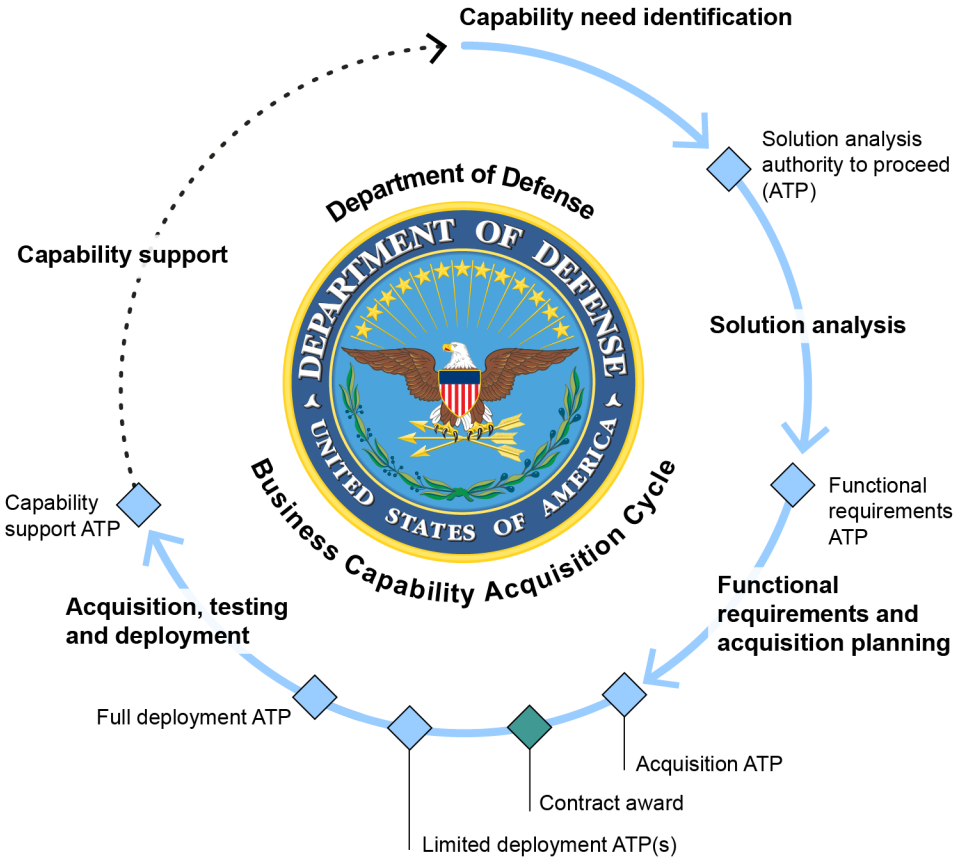
Under the pathway, business system acquisition program officials are to:

- 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.

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

[12]Department of Defense, *Business Systems Requirements and Acquisition, Instruction 5000.75 (Washington, D.C.: Jan. 24, 2020)*.

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



Sources: GAO presentation of DOD information; DOD (logo). | GAO-25-107649

The milestones in Figure 1 fall under the two higher-level phases of the system life cycle, referred to as development and sustainment. Investment expenditures in DOD's annual budget submissions are captured in two categories representing these phases: (1) development, modernization, and enhancement and (2) operations and sustainment.[13]

For the business systems pathway, development is associated with the activities and milestones starting at the beginning of the system lifecycle, at the capability need—identification stage. It includes the development

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

and delivery of new functionality or enhancements through full and limited deployments. Full deployment is the delivery of full functionality to all planned users of the business system in accordance with the full deployment authority to proceed (ATP). A limited deployment is any deployment before the full deployment 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.[14] At the full deployment ATP, the milestone decision authority considers the results of limited deployment(s) and operational testing and approves deployment to the entire user community.

Once the business system has been fully deployed, it moves into sustainment. Sustainment 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 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.[15] In October 2020, the department issued DOD Instruction 5000.87.[16] 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

[14]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.

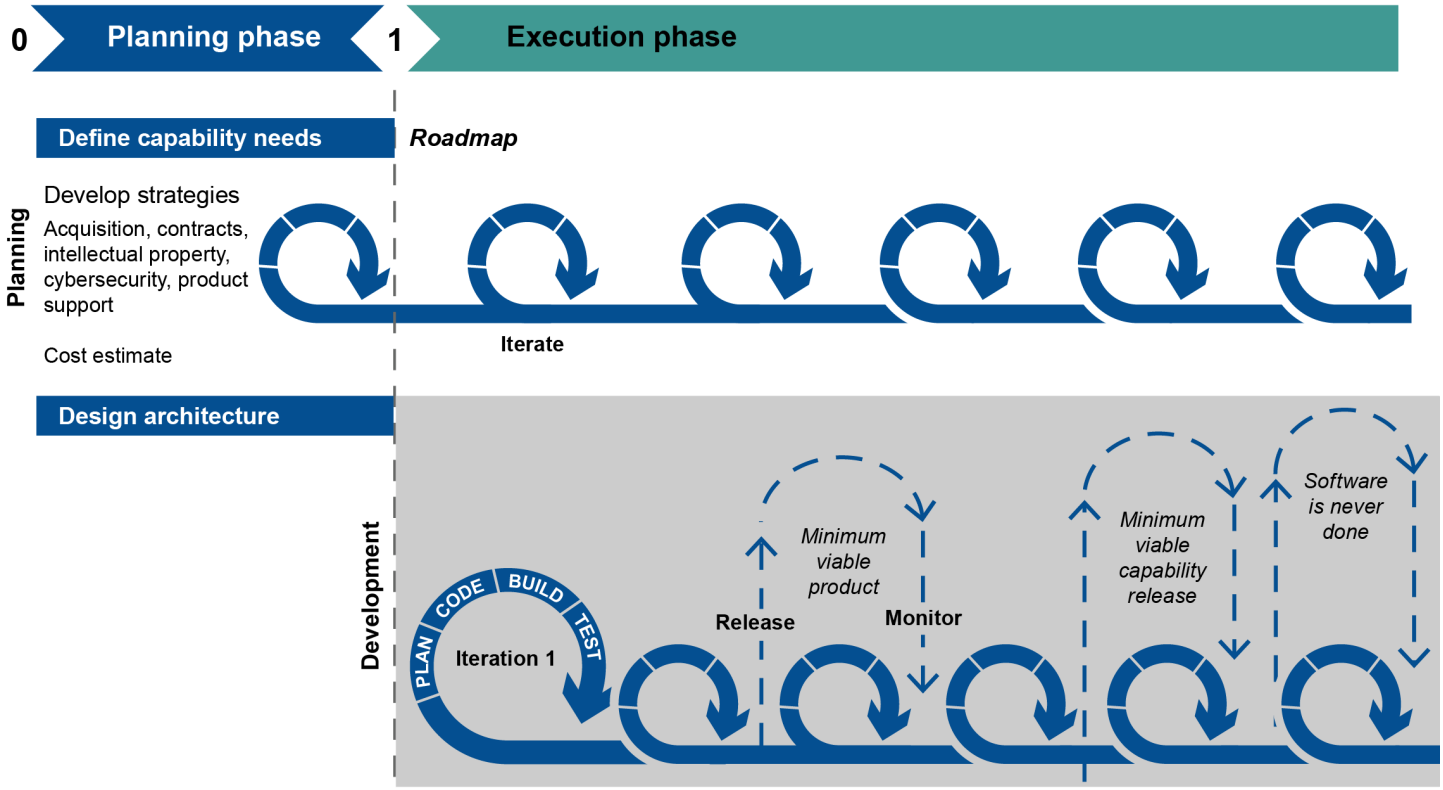
[15]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 800, 133 Stat 1198, 1478 (Dec. 20, 2019).

[16]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).

practices.[17] 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.

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



Source: GAO presentation of Department of Defense information. | GAO-25-107649

[17]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.

Designed for software-intensive systems, the pathway contains three sub-paths: (1) for applications deploying software that runs on commercial hardware and cloud platforms, (2) for upgrades and improvements to software embedded in military systems, and (3) for defense business systems. The guidance in DOD Instruction 5000.87 applies to the deploying application and embedded software sub-paths, while a subsequent August 2024 memo applies to establishing a defense business system sub-path.[18] 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 but 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.[19]

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 Agile development methodology, and the program team is

[18]Department of Defense, *Use of the Software Acquisition Pathway for Defense Business Systems,* (Washington, D.C.: Aug. 22, 2024).

[19]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).

expected to iteratively release functionality. In addition, the software acquisition pathway requires the use of iterative and Agile practices.

Further, sections 873 and 874 of the NDAA for FY 2018 mandated that DOD implement two pilot programs to enable selected acquisition programs to use Agile practices.[20] DOD provided the participating pilot programs with training and tailored Agile guidance. The Section 874 pilot lasted 1 year, and DOD has shared lessons learned from the pilot related to the implementation of these practices. The Section 873 pilot targeted large acquisition programs and continued through FY 2023.

In February 2022, DOD also issued a software modernization strategy, in part to advance its implementation of Agile development.[21] 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. The group is to include membership from offices across the department, including the offices of the DOD Chief Information Officer (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.[22] Broadly, it requires the department to implement a cybersecurity risk management process to

[20]Pub. L. No. 115-91, §§ 873-874, 131 Stat. 1283, 1498-1503 (Dec. 12, 2017).

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

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

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.[23] Under this instruction, all DOD IT systems must be categorized in accordance with Committee on National Security Systems Instruction 1253, and implement a corresponding set of security controls and assessments from National Institute of Standards and Technology Special Publication 800-53.[24] 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.

Federal Legislation and Guidance Addressing Performance Reporting, Zero Trust, and AI

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,[25] in accordance with detailed OMB guidance.[26] 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

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

[24]Committee on National Security Systems, *Security Categorization and Control Selection for National Security Systems*, Instruction 1253 (Washington, D.C.: Mar. 27, 2014); National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 Revision 5 (Gaithersburg, MD: September 2020).

[25]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).

[26]Office of Management and Budget, *Preparation, Submission, and Execution of the Budget,* Circular No. A-11, (Washington, D.C.: July 2024).

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.[27] 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.[28]

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 Office of the DOD CIO and the department's guidance,[29] DOD's major IT investments include: (1) defense business systems with a budget greater than $250 million across the future years defense plan;[30] (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.[31]

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 Federal IT 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

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

[28]FY 2025 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. General Services Administration, *BY 2025 IT Collect Submission Overview*.

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

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

[31]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) (change 1 effective Nov. 4, 2021) (reflecting statutory cost thresholds in FY 2020 constant dollars).

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.[32] These reports also addressed issues with the accuracy and reliability of the Dashboard's data. Accordingly, we made recommendations to OMB to address these issues, which it implemented.

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.[33] 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.[34] While the concepts behind zero trust are not new, the implications of shifting away from perimeter-based security are new to most enterprises and many federal agencies, including DOD.[35]

Adoption of AI. The National Security Commission on Artificial Intelligence—established by law in 2018 to consider ways to advance the

[32]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).

[33]The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

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

[35]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.

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.

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. In our first report in February 2022, we described the status of DOD's efforts to develop and acquire AI for weapon systems.[37] Our second report described the extent to which the agency has department-wide AI acquisition guidance.[38]

GAO's *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.[39] 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 help capture the metrics and support decision-making.

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

[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]S. Rep. No. 116-236, at 131 (2020). GAO, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems*, GAO-22-104765 (Washington, D.C.: Feb. 17, 2022).

[38]GAO, *Artificial Intelligence: DOD Needs Department-Wide Guidance to Inform Acquisitions,* GAO-23-105850 (Washington, D.C.: June 29, 2023).

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

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.[40] GAO uses the High-Risk Program to highlight government programs in need of transformation. As we reported in April 2023, DOD's efforts to develop an action plan to address high-risk areas had stalled since 2021. In September 2023, DOD described a revised approach for efforts underway to address the DOD business systems modernization high-risk area. These efforts included an action plan with tasks and associated milestones for updating its business enterprise architecture (BEA). As of January 2025, there were 21 GAO recommendations that DOD had not yet implemented associated with this high-risk area.

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. Four of the five 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.[41] For example, we found that DOD 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. Although DOD provided updates intended to help address the recommendation in August 2024, as of March 2025, it had not fully demonstrated that

[40]For example, see GAO, *High-Risk Series*, GAO-HR-95-1 (Washington, D.C.: Feb. 1, 1995) and additional work such as *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025), *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).*

[41]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).

the department had completed tasks necessary to implement the recommendation.[42]

- **June 2022.** We reported on the performance reporting and cybersecurity and supply chain planning of DOD's major IT business programs.[43] 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 ensure the programs, as appropriate, (1) report operational performance measures in its 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 GAO's recommendations and provided corrective action plans intended to help address the recommendations, as of March 2025, we determined that the department had not yet demonstrated that it completed all tasks needed to implement the recommendations.
- **June 2023.** We reported on the performance reporting and user training and deployment planning of DOD's major IT business programs.[44] Specifically, we found that not all programs identified at 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 GAO's recommendations and provided corrective action plans that addressed both recommendations.

[42]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 August 2023, DOD has taken some actions to implement the two recommendations from that report but neither has been implemented yet.

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

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

- **July 2024.** We reported on DOD's need to strengthen its software metrics and address continued cybersecurity and reporting gaps.[45] 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 indicated that it made plans to address our recommendation, the department has not yet implemented the recommendation as of March 2025.
- **March 2023 report on DOD's financial management systems.** We reported on issues related to DOD's accounting for its physical assets and spending.[46] This included reporting on DOD's guidance for overseeing its business and financial systems, the reliability of the data collected on business and financial system compliance with statutory requirements, and workforce planning. 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 March 2025, 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.

[45]GAO-24-106912.

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

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

According to DOD's FY 2025 Federal IT Dashboard data, the department's planned expenditures for the 24 selected IT business programs amounted to $10.9 billion from FY 2023 through FY 2025. The four largest programs accounted for just over 40 percent of the planned cost of the portfolio. Additionally, 69 percent of the total cost across the 3 years was for operating and maintaining the systems while the remaining 31 percent was for development and modernization.

Officials for 14 of the 24 business programs reported experiencing cost or schedule changes since January 2023. These 14 programs include 12 programs that reported cost increases ranging from $6.1 million to $815.5 million (a median of $173.5 million) and seven programs that reported a schedule delay ranging from 3 months to 48 months (a median of 15 months). Four of these programs also reported expecting to rebaseline due to the changes. Program officials provided a variety of reasons for the changes, including new requirements asked of the programs, workforce and contractor developments such as increased contractor prices and revised staffing estimates, challenges associated with migrating to a cloud environment, and efforts to modernize program systems.

Additionally, not all programs fully reported performance metrics in each of the required categories. Five of the 19 programs that had operational investments reported less than the required metrics for one of the categories. Of the 19 programs that did fully or partially report performance metrics, one program reported meeting all performance targets, 17 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 recommendations to the department to do so.[47]

DOD Planned to Spend $10.9 Billion on the 24 Selected Business Programs from FY 2023 to FY 2025

According to DOD's FY 2025 Federal IT Dashboard data as of February 2025, the department's planned expenditures for the 24 selected IT business programs amounted to $10.9 billion from FY 2023 through FY 2025. Of this, $3.1 billion was reported as actual costs for FY 2023 and $7.7 billion was reported as planned costs between FY 2024 and FY 2025. Table 1 shows DOD's actual and planned costs of the 24 programs during the 3-year period.

[47]GAO-22-105330 and GAO-23-106117.

Table 1: The Department of Defense's (DOD) Actual and Planned Costs for 24 Selected IT Business Programs from Fiscal Year (FY) 2023 through FY 2025

Dollars in millions (at time of reporting)

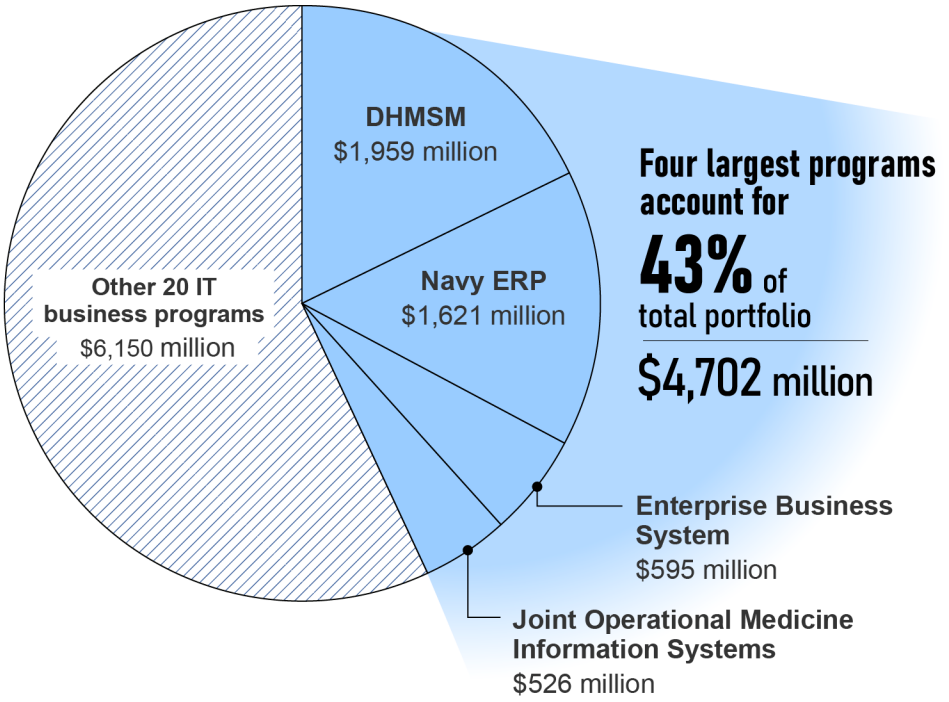
Program	FY 2023 (actual)	FY 2024 (projected)	FY 2025 (requested)	3-Year Total
Department of Defense Healthcare Management System Modernization	792	539	628	1959
Navy Enterprise Resource Planning	431	574	616	1621
Enterprise Business System	120	204	271	595
Joint Operational Medicine Information Systems	141	174	212	526
Global Combat Support System—Army	141	185	171	497
Distribution Standard System	152	182	138	471
Defense Enterprise Accounting and Management System	130	157	174	461
Navy Personnel and Pay	117	143	164	425
Advancing Analytics	102	139	163	404
Naval—Maintenance, Repair, and Overhaul	102	75	211	388
Defense Agencies Initiative	104	133	121	358
Navy Maritime Maintenance Enterprise Solution	115	117	123	355
Military Health System Information Platform	110	83	151	344
Global Combat Support System-Marine Corps/Logistics Chain Management	81	120	131	333
Real-Time Automated Personnel Identification System and Common Access Card	89	101	97	287
General Fund Enterprise Business System	70	99	113	283
Maintenance Repair and Overhaul	45	78	146	269
Defense Enrollment Eligibility Reporting System	78	96	94	268
Enterprise Business Systems—Convergence	<1	102	139	241
Air Force Integrated Personnel and Pay System	47	65	67	180
Theater Medical Information Program—Joint Increment 2	32	70	69	171
Naval Air Systems Command—Aviation Logistics Environment	55	55	51	162
Contracting Information Technology	32	50	56	137
Navy Electronic Procurement System	26	30	60	116
Totals	**3,114**	**3,573**	**4,166**	**10,852**

Source: GAO analysis of DOD's FY 2025 Federal IT Dashboard data as of February 2025. | GAO-25-107649

Department of Defense Healthcare Management System Modernization (DHMSM), Navy Enterprise Resource Planning (Navy ERP), Enterprise Business System (EBS), and Joint Operational Medicine Information Systems (JOMIS) comprised the top four largest programs in spending. Collectively, these four programs comprised $4.7 billion (43 percent) of

the total $10.9 billion allocated to and planned for the portfolio. Figure 3 shows DOD's planned costs for the four largest programs compared to the remaining 20 programs during the 3-year period.

Figure 3: The Department of Defense's (DOD) Planned Costs for the Four Largest IT Business Programs Compared to the Remaining 20 Selected Programs from Fiscal Year (FY) 2023 through FY 2025



DHMSM = DOD Healthcare Management System Modernization
Navy ERP = Navy Enterprise Resource Planning

Source: GAO analysis of data provided by the Department of Defense CIO officials, as of February 2025. | GAO-25-107649

Based on 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.

- DHMSM reported most recently achieving full deployment ATP, with the next milestone being capability support ATP.

- Navy ERP also reported achieving full deployment ATP most recently, with acquisition ATP anticipated as the next milestone for Navy ERP+.[48]
- EBS reported both its most recent milestone and the next milestone as capability support ATP.
- JOMIS reported that it has multiple products in mixed stages of their program life cycles and that the current milestones for three of these products as operational assessment/operational testing, operational assessment, and production. JOMIS' next milestones are operational assessment and operational testing for four of its products.

Further, during the 3-year period, DOD's costs for operations and sustainment (O&S)[49] accounted for 69 percent ($7.5 billion) of the total reported $10.9 billion in planned costs for the 24 programs, with the other 31 percent ($3.4 billion) allocated for development, modernization, and enhancement (DME). According to program officials, the average age of all 24 systems is 16 years.[50] 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 wasteful spending.[51] See appendix II for summaries of all 24 programs that include each program's planned costs for operating and maintaining the systems compared to development.

[48]Navy ERP+ is a modernization effort included in the original Navy ERP program and its costs are included with Navy ERP.

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

[50]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 the Distribution Standard System and Navy ERP.

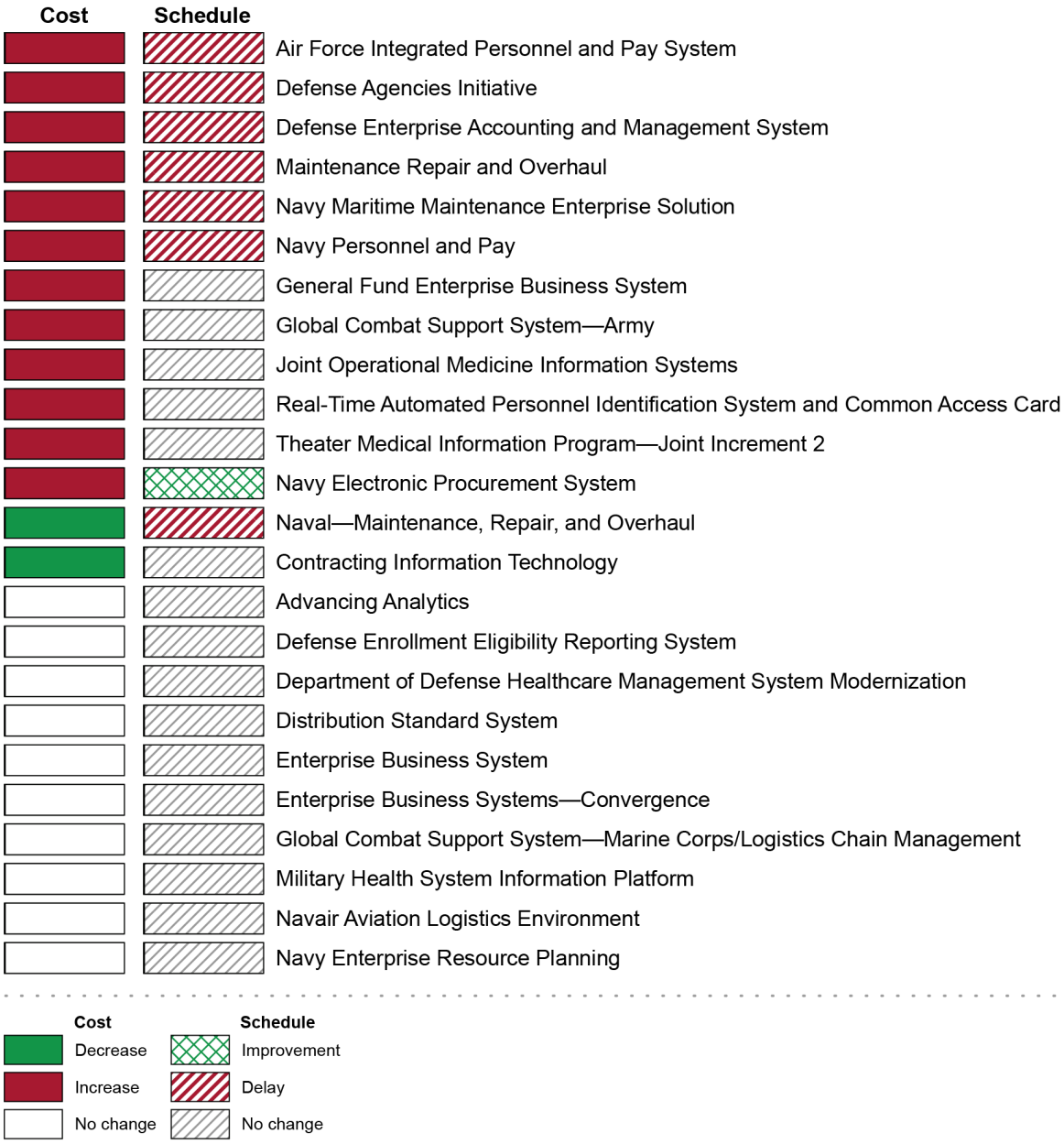
[51]See, for example, GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016); GAO, *Weapon Systems Annual Assessment: Limited Use of Knowledge-Based Practices Continues to Undercut DOD's Investments*, GAO-19-336SP (Washington,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

Programs Reported Cost and Schedule Changes

In addition to our prior reporting on cost and schedule changes, officials for 14 of the selected 24 DOD IT business programs reported cost or schedule changes since January 2023.[52]

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

Figure 4: Selected Department of Defense (DOD) IT Business Programs Reported Cost and Schedule Changes Since January 2023



Source: GAO analysis of DOD program questionnaire responses as of February 2025. | GAO-25-107649

Officials for 14 programs reported cost changes. This includes 12 programs that reported cost increases ranging from $6.1 million to $815.5 million (a median of $173.5 million) and two programs that reported decreases ranging from $33.7 million to $340 million (a median of $186.9 million). For example, officials for Maintenance Repair and Overhaul (MRO) reported a cost increase of $815.5 million since January 2023. This increase is due to additional customizations required for planned capabilities, efforts to mitigate schedule risk, and additional requirements that were identified. Officials for seven programs reported a schedule delay ranging from 3 months to 48 months (a median of 15 months) and one program reported a schedule improvement of two months.

Officials for four of the DOD IT business programs reported that they expect to rebaseline as a result of cost or schedule changes. Repeated rebaselines may indicate that programs are not appropriately managing cost, schedule, or performance expectations or are experiencing other issues.[53] For example, repeated rebaselines might indicate other challenges, such as unexpected technical complexity or issues with program contractors. The four programs that anticipate rebaselining reported the following:

- Air Force Integrated Personnel and Pay System (AFIPPS). AFIPPS officials reported expecting to rebaseline as a result of adding new incremental deployments to mitigate full deployment technical risks, performing activities to improve data accuracy, stakeholder requested re-designs, and increased management costs to support the requested redesigns while preserving the original deployment schedule. Officials reported an associated cost increase of $682 million and a schedule delay of 12 months due to these reasons.
- Defense Agencies Initiative (DAI). DAI officials reported expecting to rebaseline due to deploying the system to new organizations and increases in program support.[54] These changes were made in response to new functional sponsor requirements. Officials reported a

[53]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 their services to additional customers.

[54]Deploying organizations refers to additional customer organizations adopting DAI. A program official indicated that U.S. Cyber Command deployed DAI in 2024, and the program's sponsor directed staff to study the possibility of more organizations deploying DAI in the future.

cost increase of $333 million and a schedule delay of 48 months to implement these changes.

- Maintenance Repair and Overhaul (MRO). MRO officials reported expecting to rebaseline as a result of the program's scope expanding to accommodate new supply requirements. Officials also reported that an effort to reduce schedule risk in the program is contributing to the expected rebaselining. Additionally, officials reported a cost increase and schedule delay. The cost increase of $815.5 million is intended to support additional customizations to complete planned capability, the surge effort to mitigate schedule risk, and additional requirements. The schedule delay of 15 months is intended to accommodate the additional customizations.
- Naval—Maintenance, Repair, and Overhaul (N-MRO). N-MRO officials reported expecting to rebaseline as a result of a budget reduction due to reprioritization of funding by the Department of the Navy. Officials reported an associated total funding reduction of $340 million, as well as a schedule delay of 3 months due to software stability issues preventing the completion of testing and a change in the intended installation site.

Program officials for the 14 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, increased contractor prices and revised staffing estimates, challenges associated with migrating to a cloud environment, and efforts to modernize program systems.

Programs Reported Mixed Progress Towards Achieving Performance Goals

Not All Programs Reported Required Categories of Performance

OMB requires DOD to submit current information on the performance of major IT investments to the Dashboard. Specifically, according to OMB's Circular No. A-11 guidance, the department is to report on the performance of the programs in meeting their business or mission purpose. This includes 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. 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 that program submissions must include actual results data for all identified metrics.

In our prior reports, we found that not all programs identified the minimum required operational performance metrics in their reporting to the Dashboard and recommended that DOD ensure the programs identify the required operational performance metrics.[55] In our 2024 report we noted that officials from DOD's Office of the CIO acknowledged that gaps persisted in FY 2024 performance reporting. The officials stated that they had implemented additional audit checks that should have ensured full reporting of performance metrics in the FY 2025 data submission. We

[55]GAO-22-105330 and GAO-23-106117.

found that changes had been made in the FY 2025 data submission to address one, but not both, of our prior recommendations.

According to DOD, five of the 24 selected IT business programs are not yet operational, so DOD did not report performance metrics for these programs.[56] Of the 19 IT business programs that had operational investments, 14 identified and reported on the minimum required number of performance metrics with data in each category on the Federal IT Dashboard. However, the remaining five did not do so. Specifically, Contracting Information Technology (CON-IT) and JOMIS were missing data from one strategic and business results metric, Naval Air Systems Command—Aviation Logistics Environment (NAVAIR-ALE) was missing data from one customer satisfaction metric, and DHMSM and Theater Medical Information Program—Joint Increment 2 (TMIP-J) only reported a total of four metrics with results data.

According to DOD CIO officials in March 2025, some reporting categories are only updated on an annual basis which may lead to missing information in certain categories. The officials stated that the office is establishing processes to update data on a more frequent basis (e.g., monthly), but these changes are not yet reflected on the Dashboard. As a result, the extent to which these five programs were improving customer service, increasing financial performance, and delivering innovative approaches is unknown. Additionally, the department must still take action to address our prior recommendation for programs to report operational performance metrics to the Dashboard.

Programs Reported Mixed Progress on Performance

Of the 19 programs that identified performance metrics, one program, EBS, met all performance targets, 17 met more than one target but less than all, and one program, General Fund Enterprise Business System (GFEBS), met no targets. In total, the 19 programs that identified performance metrics reported 110 metrics (an average of 5.79 metrics per program). Of those 110 total metrics, programs reported that 72 targets were achieved, 32 targets were not achieved, and programs didn't report progress on the remaining 6 targets. Table 2 shows the number of metrics reported by each program and the targets met for each reported metric.

[56]According to staff in DOD's Office of the CIO, the four programs that are in development and not operational are AFIPPS, MRO, N-MRO, and Navy Personnel and Pay. The fifth program that is exempt from performance metric reporting is EBS-C as program officials reported that the program has had zero releases to end users.

Table 2: Reporting of Performance Metrics and Targets by 19 of the 24 Selected Department of Defense (DOD) IT Business Programs[a]

Program	Number of Metrics Identified with Target Achieved	Number of Metrics Identified with Target Not Achieved
Navy Enterprise Resource Planning	9	0
Contracting Information Technology	6	1
Defense Enrollment Eligibility Reporting System	6	4
Enterprise Business System	5	0
Navy Electronic Procurement System	5	1
Advancing Analytics	4	2
Defense Agencies Initiative	4	1
Defense Enterprise Accounting and Management System	4	1
Department of Defense Healthcare Management System Modernization	4	0
Distribution Standard System	4	1
Navy Maritime Maintenance Enterprise Solution	4	1
Real-Time Automated Personnel Identification System and Common Access Card	4	1
Global Combat Support System—Marine Corps/Logistics Chain Management	3	2
Joint Operational Medicine Information Systems	3	1
Military Health System Information Platform	3	2
Global Combat Support System—Army	2	3
Naval Air Systems Command—Aviation Logistics Environment	1	3
Theater Medical Information Program—Joint Increment 2	1	3
General Fund Enterprise Business System	0	5
Totals[b]	**72**	**32**

Source: GAO analysis of DOD's FY 2025 Federal IT Dashboard data. | GAO-25-107649

[a]Five of the 24 selected IT business programs are not yet operational, so DOD did not report performance metrics for these programs.

[b]Numbers do not add to 110 because programs did not report progress on six targets.

Selected Programs Reported Using Software Development and Cybersecurity Practices, but Some Lacked Metrics and Plans

As of March 2025, officials for 11 (of the 24) selected DOD IT business programs that we identified as actively developing software reported using recommended Agile and iterative approaches and practices.[57] However, in areas related to tracking customer satisfaction and progress of software development, three of the 11 programs did not demonstrate use of metrics and management tools required by DOD and consistent with ones identified in GAO's Agile Guide.[58] Also, four programs have not developed plans to implement Zero Trust architecture. Lastly, while 23 of the 24 programs reported conducting a variety of cybersecurity testing and assessments, two programs did not have an approved cybersecurity strategy, as required by DOD.[59]

Program officials reported facing a variety of key challenges related to software development and cybersecurity, including budget constraints, changing requirements, and leadership and staff turnover. Officials also reported program and DOD efforts to address these challenges, which included programs working with a sponsor to establish a committee to review requirements and working to address the absence of key management roles and increase staff.

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

In February 2018, the Defense Science Board recommended that DOD implement continuous, iterative software development approaches, such as Agile; development and operations (DevOps); and development, security, and operations (DevSecOps).[60] An iterative development approach is a way of breaking down the development of large applications into smaller pieces or iterations that are being 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

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

[58]GAO-24-105506.

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

[60]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington, D.C.: February 2018). 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.

applicable to DOD and should be adopted as quickly as possible. Table 3 describes the recommended iterative software development approaches.

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

Approach	Description
Agile	Software is delivered in increments throughout the project, but 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-25-107649

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, in May 2019 the Defense Innovation Board concluded that iterative software development may reduce cost growth compared to a Waterfall approach.[61]

As of March 2025, officials for all 11 major 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 and include:

- **Programs using Agile:** AFIPPS, Navy Personnel and Pay, Global Combat Support System—Army, Defense Enterprise Accounting and Management System, JOMIS
- **Programs using DevSecOps:** NAVAIR-ALE
- **Programs using both Agile and DevSecOps:** GFEBS, MRO, Navy Electronic Procurement System, N-MRO, CON-IT.

[61]Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (March 2019).

In addition, all 11 programs actively developing software reported collecting some form of user feedback during requirements development and refinement. Officials for 23 of the 24 IT business programs reported involving users in testing, 21 of the 24 programs reported surveying users about customer experience, and four of the 24 programs reported having user agreements in place with end users.

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. Furthermore, the board recommended using the creation of a software factory as a key evaluation criterion in the source selection process for software development.

Officials for each of the 11 programs actively developing software reported using a variety of the recommended iterative practices. For example, officials for all 11 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, three programs reported using a software factory. Table 4 describes the iterative development practices that programs reported using.

Table 4: Department Of Defense's (DOD) Major IT Business Programs Actively Developing Software Reported Using Recommended Iterative Practices

Practice	Description	Number of programs that reported using each practice
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	11 of 11
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	11 of 11
Software documentation provided at each production milestone	Written text or illustration that accompanies computer software or is embedded in the source code	11 of 11
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	3 of 11
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	0 of 11

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

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

Officials from DOD's Office of the CIO previously 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.

Nine of the 11 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.[62] 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 nine of the 11 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, MRO, reported that the average length of time between software releases was 7 to 9 months. The other remaining program, AFIPPS, reported that it is coordinating with the Department of the Air Force senior leadership on a timetable for future payroll functionality deployments.

[62]OMB, Memorandum M-15-14, *Management and Oversight of Federal Information Technology* (Washington, D.C.: June 10, 2015). 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.

Programs Reported Using AI or Related Tools for Software Development

Programs reported using AI as part of their software development efforts.[63] Table 5 describes the programs' reported use of AI or other related tools for software development.

Table 5: Department of Defense (DOD) 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 automate routine, rules-based tasks by mimicking user interactions	5 of 24
Generative AI	Creates content, including text, images, audio, or video when prompted by a user	2 of 24
Machine Learning	Detects patterns in datasets and make predictions based on what the computer learned from those patterns	1 of 24
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	0 of 24
Other Tools		3 of 24

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

[a]These AI Systems and Tools provide a few examples and are not an exhaustive list.

Programs that reported using AI for software development are still in the early stages of implementation. These programs reported still being in the process of developing formal documented plans and roadmaps. In addition, programs that are developing or planning to develop AI features to be incorporated into a software product provided some examples of their approaches. These included programs developing a generative AI product for recommending edits to draft work documentation, using AI to improve processing times, and predicting future cost requirements. We discuss DOD's efforts to develop guidance for acquiring and implementing AI later in this report.

[63]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).

Three of the 11 Programs Did Not Use Required Agile Metrics and Management Tools

DOD's *Agile Metrics Guide (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.[64] DOD's *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 customer satisfaction and progress of software development efforts.[65] 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.

Additionally, as mentioned in the background, GAO's *Agile Guide* encourages programs to use various metrics and management tools when pursuing Agile software development.[66] These metrics and management tools measure performance and outcomes to help meet customer needs and are best practices for Agile adoption. Several of these metrics and management tools are consistent with ones required in DOD's guidance.

Officials for the 11 selected DOD IT business programs actively developing software using Agile, and iterative approaches consistent with Agile, reported using metrics and management tools identified in GAO's *Agile Guide*. Table 6 shows the Agile metrics that the DOD IT business programs reported using. Table 7 shows the Agile management tools that the DOD IT business programs demonstrated using.

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

[65]Department of Defense, *DevSecOps Fundamentals Guidebook: DevSecOps Activities and Tools*, Version 2.2 (Washington, D.C., May 25, 2023).

[66]GAO-24-105506.

Table 6: The Selected Department of Defense (DOD) IT Business Programs Reported Using Metrics Identified in GAO's A*gile Assessment Guide*

Metric	Description	Number of programs reporting using metric
Velocity	Volume of work accomplished in a specific time by a team[a], compared against a metric that quantifies the work developers can deliver in each iteration	10 of 11
Features or user stories delivered	User stories[b] or story points committed versus user stories or story points accepted	10 of 11
Number of defects or bugs	Number of defects identified after deploying a product into the production environment	9 of 11
Customer satisfaction	Level of satisfaction measured by customers and monitored throughout the development cycle	9 of 11
Time required to restore service after outage	A measure of time to restore service after an outage	9 of 11
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	9 of 11
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	8 of 11
Time required for full regression test	A measure of time to complete a full regression test[c]	8 of 11
Other	Other measures defined by the program	2 of 11

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

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

[b]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).

[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 7: The Selected Department of Defense (DOD) 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 reporting using tool
Burn up or burn down charts	A visual tool displaying progress via a simple line chart representing work accomplished or remaining work over time	10 of 11
Product backlog	A high-level backlog that contains all the requirements for the entire program	10 of 11
Sprint backlogs	Ordered list of tasks to be accomplished during the sprint	9 of 11

Release plans	Plans that identify different sets of usable functionality or products scheduled for delivery to customers	9 of 11
Cumulative flow diagram[a]	An analytical tool that allows teams to visualize their effort and the program's progress	6 of 11
Budget baseline	A cost baseline used to measure program performance	5 of 11
Other	Other tools defined by the program	1 of 11

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

[a]Refers to the cumulative flow diagram tool, which is different from the cumulative flow metric in Table 6.

However, of the 11 programs, three of the six that reported using DevSecOps did not use metrics and management tools required of these programs by DOD or did not provide evidence of their use. Specifically, the three programs did not use cumulative flow metrics and a cumulative flow diagram. Additionally, one program did not use product backlogs or release plans, and one did not track customer satisfaction or the number of defects or bugs.

Programs that did not demonstrate use of these required Agile metrics and management tools reported a variety of reasons for not doing so. These included the programs not yet establishing the management tools or tracking similar metrics but not in the specified format. In March 2025, officials from DOD's Office of the CIO acknowledged that the adoption of modern software approaches like Agile and DevSecOps may be in the early stages of implementation and certain individual programs have not yet fully implemented these metrics and tools.

We previously recommended that DOD ensure that IT business programs developing software use the metrics and management tools required by DOD.[67] 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 Lacked Plans and Strategies

DOD Instruction 5000.89 requires that DOD IT program staff complete developmental and operational cybersecurity testing.[68] According to

[67]GAO-24-106912.

[68]Department of Defense, Instruction 5000.89.

DOD's *Cybersecurity Test and Evaluation Guidebook*,[69] 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 may conduct developmental testing but may not be mature enough to conduct operational testing. Table 8 summarizes the types of cybersecurity testing that the programs reported conducting.

Table 8: The Selected Department of Defense (DOD) 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	20 of 24
Operational testing	Evaluates operational programs' cybersecurity for effectiveness, suitability, and survivability	19 of 24

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

Additionally, DOD Instructions 5000.75 and 5000.90 require IT program staff to conduct cybersecurity assessments.[70] 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 23 of the 24 major IT business programs also reported conducting some form of cybersecurity assessment. For example, a

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

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

majority of the programs reported conducting full system assessments, table top exercises, and penetration tests.[71] Several programs also reported conducting other types of cybersecurity assessments, such as static code and privacy impact assessments. Officials for the remaining program reported that it had not yet conducted any of the assessments, but that it had planned to do so. Specifically, the officials reported that a contract was awarded in September 2024, but no assessments had been completed yet.

Four Programs Have Not Developed Plans to Implement Zero Trust Architecture

In addition to conducting cybersecurity testing, programs also reported using zero trust to secure their systems. As previously mentioned, a May 2021 executive order requires that DOD adopt zero trust cybersecurity, including developing a plan to implement a zero trust architecture.[72] Additionally, the NDAA for FY 2022 directed DOD to develop a zero trust strategy, a model architecture, and implementation plans.[73] As part of the agency's response to these requirements, in January 2023, DOD published the *Zero Trust Capability Execution Roadmap—Course of Action 1 (COA 1)* where it identified a timeline that all DOD organizations achieve the planned zero trust targets by the end of FY 2027.[74] Officials from 14 of the 24 major IT business programs reported implementing zero trust as part of their security framework to varying extents.

However, 10 programs reported not implementing zero trust architectures. Of those, 6 reported they have plans to implement it. The remaining 4 reported not having plans to implement it. In March 2025, DOD CIO officials provided reasons that these programs do not have plans to implement zero trust architecture, including one program that was leveraging a concurrent strategy with a larger organization. It will be important that these programs establish plans to meet the 2027 deadline, and we will continue to monitor the progress of these programs' efforts.

[71]Full-system assessments are performed on a complete system to evaluate its compliance with specified requirements. Table top 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.

[72]The White House, *Improving the Nation's Cybersecurity,* Executive Order 14028.

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

[74]Department of Defense, *DOD Zero Trust Capability Execution Roadmap (COA 1)* (Jan. 06, 2023); Department of Defense News Release, *Department of Defense Releases Zero Trust Strategy and Roadmap* (November 22, 2022).

Two Programs Did Not Have an Approved Cybersecurity Strategy

DOD Instruction 8500.01, *Cybersecurity*, and DOD Instruction 5000.89, *Test and Evaluation*, require that DOD IT program officials use an approved cybersecurity strategy.[75] 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 programs' 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.[76] We recommended that DOD's CIO ensure that these programs develop such a strategy, as appropriate, and DOD concurred with our recommendation. Further, in our June 2023 and June 2024 reports, we also found that six of the department's major IT business programs lacked an approved strategy and reiterated the importance of ensuring that these programs develop one.[77]

As of March 2025, two programs still did not have an approved strategy.[78] Officials for the programs reported planning to develop such a strategy by December 2025 or that they do not yet have a planned date for implementing 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 of the 24 selected IT business programs reported facing a number of key challenges associated with software development and cybersecurity and collectively reported actions taken by the programs to address them. Common challenges cited by the business program officials included budget constraints and changing customer requirements. Officials noted actions to address these challenges including working with other offices to address funding needed and articulating clearer requirements.

[75]Department of Defense, Instruction 8500.01 and Instruction 5000.89 (Nov. 19, 2020).

[76]GAO-22-105330.

[77]GAO-23-106117. The six programs that lacked an approved strategy as part of these two reviews are not all the same six.

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

Table 9 summarizes the reported challenges and actions taken by the programs.

Table 9: The Selected Department of Defense (DOD) 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	Working with a sponsor and other offices to address funding levels to meet full operational capabilities	14 of 24
Changing customer requirements	Participating in the process of generating and articulating clearer requirements Working with a sponsor to establish a committee to review requirements	11 of 24
Rapidly evolving cybersecurity requirements	Engaging with leadership to reduce redundancy and delays caused by requiring two types of authorization Briefings to leadership to ensure awareness of ongoing cybersecurity efforts	9 of 24
Technical issues related to software development and commercial off-the-shelf software	Working with vendors to make necessary configuration changes	7 of 24
Leadership and staff turnover	Working to address the absence of key management roles and increase staff	6 of 24

Source: GAO analysis of DOD program questionnaire responses as of March 2025. | GAO-25-107649

Additionally, DOD CIO officials stated that using modern software practices that leverage cloud computing and software factories can be more efficient and help with budget constraints. To address changing customer requirements, the CIO is advancing DevSecOps as the preferred software delivery model to replace legacy waterfall practices, which should allow for customer requirements to be incrementally delivered.

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. These efforts include revising its business systems investment management guidance, modernizing its business enterprise architecture (BEA), adopting zero trust cybersecurity, developing AI acquisition guidance, and updating its Strategic Management Plan.

Defense business systems investment management guidance. In October 2024, DOD published the Defense Business Systems (DBS) Certification & Management Guidance. 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.

Business enterprise architecture modernization. We previously reported that in March 2024, DOD planned to publish a BEA guidebook by September 30, 2024.[79] The guidebook is to detail BEA governance, roles, and responsibilities, use cases, use of enterprise-level tools, and development best practices. In January 2024, DOD noted that the guidebook will build upon the BEA framework and is to provide the instruction necessary to develop and maintain a modernized BEA.[80]

In October 2024, DOD indicated that developing the BEA guidebook required additional time to coordinate with key stakeholders. In March 2025, officials from the CIO office indicated that the current estimated publication date is the third quarter of FY 2025.

Zero trust cybersecurity. We previously 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.[81] Since our last report, the department indicated that it has not developed additional roadmaps, but continues to make efforts to adopt zero trust across the department. For example, the department identified progress made in the development of zero trust proof of concepts and functional assessments.

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.[82] In that

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

[80]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.

[81]GAO-24-106912.

[82]GAO-23-105850.

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.[83] 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 is developing the "*Adopt, Buy, Create*" framework appendix to the strategy that will 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.

In addition, in October 2023, DOD described creating an AI implementation plan by the fourth quarter of FY 2023. Specifically, CDAO created a plan for federated development and adoption of AI capabilities, including processes for defining AI capabilities being developed by CDAO and identifying and promoting best practices. In March 2025, DOD provided this implementation plan, and we are currently reviewing the document to determine if it fully implements our recommendation.

Strategic management plan. In January 2021, section 901 of the William M. (Mac) Thornberry NDAA for FY 2021 repealed the position of the Chief Management Officer within DOD.[84] The NDAA also mandated that the department transfer the responsibilities, personnel, functions, and assets of the Chief Management Officer to other officials, organizations, and elements no later than January 1, 2022. Effective October 1, 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.

10 U.S.C. §132a, as added by Section 902 of the National Defense Authorization Act for FY 2025, establishes the PIO in statute and mandates certain duties and responsibilities to the position.[85] The PIO is responsible for overseeing business process modernization, overseeing

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

[84]Pub. L. No. 116-283, § 901, 134 Stat. 3388, 3794 (Jan. 1, 2021).

[85]Pub. L. No. 118-159, § 902 (Dec. 23, 2024) codified at 10 U.S.C. 132a(c)(1).

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).[86] According to DOD, this plan is published annually and represents the agency's roadmap for advancing the National Defense Strategy.

The 2022–2026 SMP included DOD's Annual Performance Plan for FY 2025 which defined specific performance goals and measures along with targets to help ensure successful implementation of the SMP. For example, one of the strategic objectives outlined in the plan is to modernize DOD business systems. It specifies that the goal is for DOD to manage business systems as a strategic asset and deploy efforts to modernize, integrate, and optimize its business systems portfolio.

For the strategic objective of modernizing DOD business systems, the described measure for success is to decommission, retire, or migrate 100 percent of business systems, for each FY, on schedule per planned dates in DOD's information technology portfolio repository. However, in FY 2023 and 2024, the DOD CIO reported achieving 40 percent and 67 percent of this goal, respectively. To help achieve future targets, the DOD CIO outlined efforts to improve. Specifically, the CIO plans to work with DOD components to validate retirement targets prior to the start of the FY, set up regular engagements with components to mitigate risk and resolve issues, and implement a reporting process to track and communicate schedule delays and changes in retirement timelines.

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 a review of reforms to improve the department's efficiency and effectiveness (required under the FY 2021 NDAA).[87] Additionally, we will monitor DOD's efforts associated with its business systems modernization, approach to business transformation high-risk areas, and adoption of AI and zero trust cybersecurity.

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

[87]Pub. L. No. 116-283, § 911, 134 Stat. 3388, 3801-3802 (Jan. 1, 2021) mandated a GAO review of DOD's framework for these reforms. See GAO, *Defense Management: Action Needed to Advance Progress on Reform Efforts*, GAO-24-105793 (Washington, D.C.: Oct. 18, 2023).

Conclusions

DOD planned to spend $10.9 billion from FY 2023 through FY 2025 on the selected 24 IT business programs with several 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.

Regarding software development, three of the programs developing software did not demonstrate use of Agile metrics and management tools, as required by DOD. In addition, two programs did not have an approved cybersecurity strategy, as required by DOD. Implementing our prior recommendations regarding use of Agile metrics and cybersecurity planning will further DOD's goals of efficient and secure business software development efforts.

Recommendation for Executive Action

We reiterate that DOD address the five recommendations previously made that have not yet been implemented from prior 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 and Under Secretary of Defense for Acquisition and Sustainment 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. (Recommendation 1)

Agency Comments

DOD provided written comments on a draft of this report, which are reproduced in appendix III. In its comments, the department concurred with our recommendation. The department stated that it requires major information technology business programs to report the minimum performance metrics data in each category, as appropriate, as part of the department's federal IT Dashboard submission. In addition, the department reported that it implemented audit checks in April 2024 to have components provide all major IT system performance metrics. DOD also stated that it had recently increased the frequency of its federal IT Dashboard updates to ensure more timely data. Despite these efforts, we identified programs with missing results data on the IT Dashboard in May 2025. 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 Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

//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 the current status of cost, schedule, and performance of selected Department of Defense IT business programs, (2) assess the extent to which DOD has implemented key 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 24 programs that DOD listed as major IT investments in its fiscal year (FY) 2025 Federal IT Dashboard (Dashboard) data at time of initial collection in July 2024.[1] We developed a questionnaire that focused on programs' cost and schedule, software development, user engagement, cybersecurity, and software risks and challenges. 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 24 program offices in September 2024 and asked program staff to provide their responses. We also analyzed program officials' responses to the questionnaire and followed up with programs through March 2025.

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

To address the first objective, we selected the 24 major IT business programs that DOD listed as major IT investments in its FY 2025 Federal IT Dashboard data, as of July 2024, for review. We also analyzed the

[1]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. We excluded seven new programs that were added to the list of major IT programs as of October 2024 because they were added after the initiation of the engagement.

Dashboard data, as of February 2025, to examine DOD's planned costs for the 24 selected IT business programs during the 3-year period from FY 2023 through FY 2025, including a breakdown of the costs for operating and maintaining the systems compared to for development and modernization. In addition to the FY 2025 data, we analyzed the 5 previous years of Dashboard data to examine any changes in the department's actual spending on major IT business programs over the 5-year period (from FY 2019 through FY 2023), including a breakdown of the spending on operating and maintaining the systems compared to development.

To assess and ensure the reliability of the budget data DOD reported on the Federal IT Dashboard, 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 summaries to the 24 program offices 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 Office of the Chief Information Officer (CIO) 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, 2023, and (2) programs had rebaselined or expected to rebaseline as a result of the changes.[2] 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).

Further, we analyzed programs' performance metrics data included in DOD's FY 2025 reporting to the Dashboard and compared the data to Office of Management and Budget (OMB) guidance.[3] We also met with

[2]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.

[3]FY 2025 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. General Services Administration, *BY 2025 IT Collect Submission Overview* (Washington, D.C.: Dec. 2023).

officials within the department's Office of the CIO to determine reasons for differences between how the performance data were reported and guidance for such reporting.

To assess and ensure the reliability of the programs' performance metrics data, we compared the data to performance metrics documentation provided by the programs to identify any obvious inconsistencies and met with DOD CIO officials to understand why data was missing for programs in certain categories. 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 software development and cybersecurity practices used by the 24 programs, including 11 programs that we identified as actively developing software.[4] 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.[5] In addition, we collected and analyzed key information and supporting documents related to the programs' reported practices, including their use of metrics and management tools identified in GAO's *Agile Assessment Guide* and development of approved cybersecurity strategies and compared it to DOD's guidance.[6] 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,

[4]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 13 programs reported either that their software development efforts were to sustain existing functionality, involved minor enhancements, or that they were not actively developing software.

[5]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, Incorporating Change 2, Jan. 24, 2020 (Washington, D.C.: Feb. 2, 2017); 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).

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

we followed up with program officials and officials within the DOD CIO for reasons why they did not do so.

We reviewed information of each program's implementation of artificial intelligence as part of DOD's software development and cybersecurity efforts. In addition, we also assessed information from program officials about their plans for and implementation of zero trust in cybersecurity strategies and security frameworks. We compared this information against plans DOD has in place for the department to implement zero trust architecture targets by 2027.

Further, 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 DOD actions to implement previously identified legislative and policy changes that could affect its IT acquisitions.[7] The scope of the objective included the role of DOD's Performance Improvement Officer, a role that is responsible for various duties previously designated to the Chief Management Officer, planned improvements to the department's IT portfolio management (i.e., updates to its investment management guidance and business enterprise architecture), adoption of zero trust principles, and establishment of a department-wide AI acquisition guidance, and overview of DOD's Strategic Management Plan. To describe the actions DOD has taken toward implementation of these changes, we requested and reviewed policies, plans, and guidance provided by DOD; reports that the department submitted to Congress; and internal program documentation. We also met with DOD CIO officials to discuss their efforts in these areas and coordinated with the GAO team conducting a companion assessment examining weapon system acquisition programs.[8]

We conducted this performance audit from June 2024 to March 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

[7]The previously identified legislative and policy changes are discussed in GAO, *IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Development Planning*, GAO-23-106117 (Washington, D.C.: June 13, 2023).

[8]GAO-25-107569.

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.

Appendix II: Program Summaries

This appendix provides summaries of the 24 selected Department of Defense (DOD) 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
- Air Force Integrated Personnel and Pay System
- Contracting Information Technology
- Defense Agencies Initiative
- Defense Enrollment Eligibility Reporting System
- Defense Enterprise Accounting and Management System
- Distribution Standard System
- DOD Healthcare Management System Modernization
- Enterprise Business System
- Enterprise Business System—Convergence
- General Fund Enterprise Business System
- Global Combat Support System—Army
- Global Combat Support System—Marine Corps/Logistics Chain Management
- Joint Operational Medicine Information Systems
- Maintenance Repair and Overhaul
- Military Health System Information Platform
- Naval—Maintenance, Repair, and Overhaul
- Naval Air Systems Command—Aviation Logistics Environment
- Navy Electronic Procurement System
- Navy Enterprise Resource Planning
- Navy Maritime Maintenance Enterprise Solution
- Navy Personnel and Pay
- Real-Time Automated Personnel Identification System and Common Access Card
- Theater Medical Information Program—Joint Increment 2

Advancing Analytics (Advana)

Program
Advancing Analytics (Advana)

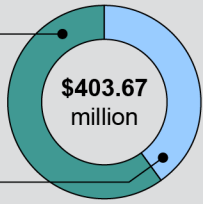
Software development approaches
Agile; Incremental; Development, Operations (DevOps); Development, Security, and Operations (DevSecOps)

Average time of software deliveries

Cost, fiscal years 2023–2025

Total operations and maintenance (O&M) **$241.21 mil**

Total development, modernization and enhancement (DME) **$162.46 mil**



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

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 February 2025)

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: Deliver capabilities		**CIO evaluation rating:** 3 – Medium risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 10: 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	Yes
Iterative development training for program managers and staff	No
Use of a software factory	Yes
Use of commercial off-the-shelf products	Yes
Software releases to date	246
Planned releases	Unknown
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Air Force Integrated Personnel and Pay System (AFIPPS)

Program
Air Force Integrated Personnel and Pay System (AFIPPS)

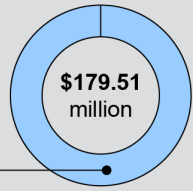
Software development approaches
Agile

Average time of software deliveries

Unknown

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$0 mil

Total development, modernization and enhancement (DME)
$179.51 mil



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *Expects to*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

AFIPPS is intended to integrate existing personnel and pay processes into one self-service system. The system is to support how Air Force owns and operates the human resource management domain.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Air Force	**Program owner:** Air Force	**Year investment began:** 2009
Acquisition pathway: Defense business systems	**Last milestone achieved:** Acquisition authority to proceed (ATP)	
Next planned milestone: Limited deployment ATP	**Chief Information Officer (CIO) evaluation rating:** 3 – Medium risk	
Year investment is estimated to reach end of useful life: 2037		

Table 11: Air Force Integrated Personnel and Pay System's (AFIPPS) 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	0
Planned releases	2-3
Average time between releases	Unknown

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

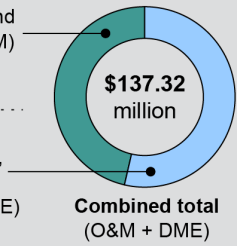
Contracting Information Technology (CON-IT)

Program
Contracting Information Technology (CON-IT)

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

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *Decrease*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

The purpose of CON-IT is to become the enterprise-wide Contract Writing System (CWS) for the Department of the Air Force (DAF).

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Air Force	**Program owner:** Air Force	**Year investment began:** 2016
Acquisition pathway: Software acquisition Defense business systems		**Last milestone achieved:** Deliver capabilities
Next planned milestone: Full sustainment		**CIO evaluation rating:** 5 – Low risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 12: Contracting Information Technology's (CON-IT) 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	60 (12-14 major releases per year)
Planned releases	3-week development sprints and 2 weeks of testing
Average time between releases	3 weeks

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

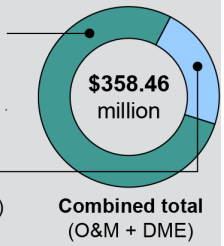
Defense Agencies Initiative (DAI)

Program
Defense Agencies Initiative (DAI)

Software development approaches
Incremental

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: ↑ *Increase*

Schedule: ↑ *Delay*

Rebaseline: *Expects to*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

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 February 2025)

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 ATPs	
Next planned milestone: Limited deployment ATPs	**CIO evaluation rating:** 5 – Low risk	
Year investment is estimated to reach end of useful life: 2038		

Table 13: 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	6
Planned releases	11
Average time between releases	10-12 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Defense Enrollment Eligibility Reporting System (DEERS)

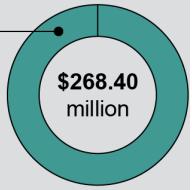
Program
Defense Enrollment Eligibility Reporting System (DEERS)

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

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$268.40 mil

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



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

DEERS is the authoritative data repository for all DOD workforce, personnel benefits, eligibility, and military health care system enrollment information.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Defense-wide	**Program owner:** Office of the Under Secretary of Defense for Personnel and Readiness, Defense Human Resource Activity (DHRA), Defense Manpower Data Center (DMDC)	**Year investment began:** 1978
Acquisition pathway: Defense business systems		**Last milestone achieved:** Capability support 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 14: Defense Enrollment Eligibility Reporting System's (DEERS) 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, DevSecOps
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	Unknown
Planned releases	Unknown
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Defense Enterprise Accounting and Management System (DEAMS)

Program
Defense Enterprise Accounting and Management System (DEAMS)

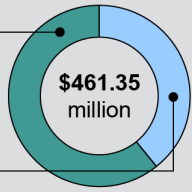
Software development approaches
Agile; Development, Operations (DevOps)

Average time of software deliveries

Cost, fiscal years 2023–2025

Total operations and maintenance (O&M) **$279.55 mil**

Total development, modernization and enhancement (DME) **$181.80 mil**



Combined total (O&M + DME)

Cost and Schedule Changes *(since January 2023)*

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

DEAMS is intended to enable integration of all 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 February 2025)

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:** 4 – Moderately low 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	587
Planned releases	N/A, releases on a 3-week iteration until capability is released into production
Average time between releases	Less than 1 month (every 3 days)

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

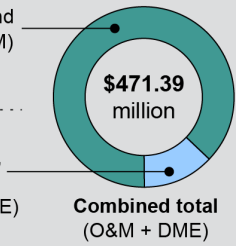
Distribution Standard System (DSS)

Program
Distribution Standard System (DSS)

Software development approaches
Agile

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

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 is intended to provide worldwide service and support to the warfighter, peacekeepers, and federal and civilian customers.

Program essentials (reported by DOD officials as of February 2025)

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:** 5 – Low risk
Year investment is estimated to reach end of useful life: 2026		

Table 16: Distribution Standard System's (DSS) 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	Yes
Iterative development training for program managers and staff	Yes
Use of a software factory	Yes
Use of commercial off-the-shelf products	No
Software releases to date	48
Planned releases	None
Average time between releases	Monthly

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

DOD Healthcare Management System Modernization (DHMSM)

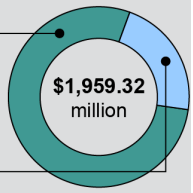
Program
Department of Defense Healthcare Management System Modernization (DHMSM)

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

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$1533.09 mil

Total development, modernization and enhancement (DME)
$426.23 mil



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

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 February 2025)

Lead DOD component: Defense-wide	**Program owner:** Defense Health Agency (DHA)	**Year investment began:** 2014
Acquisition pathway: Defense business systems		**Last milestone achieved:** Full deployment ATP
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 17: 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
Delivery of a minimum viable product	N/A
Software documentation provided at each production milestone	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	7,139
Planned releases	60 (minimum)
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Enterprise Business System (EBS)

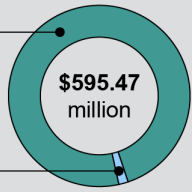
Program
Enterprise Business System (EBS)

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

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$584.46 mil

Total development, modernization and enhancement (DME)
$11.02 mil



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *No Change*

Schedule: *No Change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

EBS is DLA's 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 February 2025)

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:** 4 – Moderately low 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; DevOps; DevSecOps; Incremental
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	898
Planned releases	28
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Enterprise Business Systems—Convergence (EBS-C)

Program
Enterprise Business Systems—Convergence (EBS-C)

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

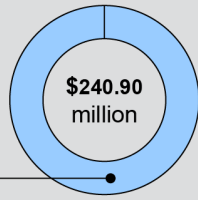
Average time of software deliveries

Unknown

Cost, fiscal years 2023–2025

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

Total development, modernization and enhancement (DME)
$240.90 mil



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

EBS-C is intended to converge Army business systems through an integrated finance-logistics transactional core, simplify the warfighter/workforce interface, and fundamentally transform operations to become as “commercial-as-possible and military-as-necessary" while improving the security of data.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Army	**Program owner:** Army	**Year investment began:** 2024
Acquisition pathway: Software acquisition Defense business systems		**Last milestone achieved:** Decision authority authorizes entry into execution phase
Next planned milestone: Deliver capabilities		**CIO evaluation rating:** 2 – Moderately high 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	No
Use of an iterative development approach	Yes
Software development approach	Agile, DevSecOps
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	Minimum of 8
Average time between releases	Maximum of 1 year

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

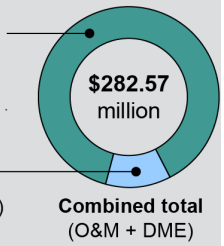
General Fund Enterprise Business System (GFEBS)

Program
General Fund Enterprise Business System (GFEBS)

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

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

GFEBS is Army's core financial management system intended to administer its general fund finances, improve financial visibility and information reliability, and standardize business processes.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Army	**Program owner:** Army	**Year investment began:** 2005
Acquisition pathway: Defense business systems		**Last milestone achieved:** Capability support ATP
Next planned milestone: N/A (program is in sustainment)		**CIO evaluation rating:** 5 – Low risk
Year investment is estimated to reach end of useful life: 2032		

Table 20: General Fund Enterprise Business System's (GFEBS) 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, Incremental, DevSecOps
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	244
Planned releases	258
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

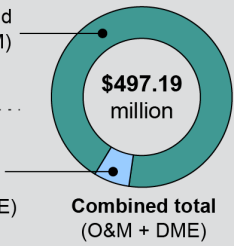
Global Combat Support System—Army (GCSS-A)

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

Software development approaches
Agile

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

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 February 2025)

Lead DOD component: Army	**Program owner:** HQ Army 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: N/A (program is in sustainment)		**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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	84
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 February 2025. | GAO-25-107649

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)

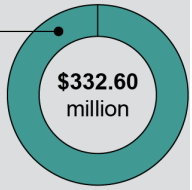
Software development approaches
Agile

Average time of software deliveries

Cost, fiscal years 2023–2025

Total operations and maintenance (O&M)
$332.60 mil

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



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2022)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

GCSS-MC/LCM provides the foundation for all ground 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 February 2025)

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: No estimated end date		

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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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 February 2025. | GAO-25-107649

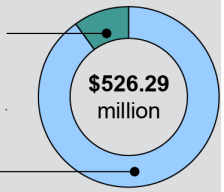
Joint Operational Medicine Information Systems (JOMIS)

Program
Joint Operational Medicine Information Systems (JOMIS)

Software development approaches
Agile

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *No changes*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

JOMIS 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 February 2025)

Lead DOD component: Defense-wide	**Program owner:** 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:** MedCOP-S - Operational assessment/testing HCD - Initial operational assessment. OMDS-S - Production	
Next planned milestone: Operational assessment and operational testing for multiple JOMIS products.	**CIO evaluation rating:** 3 – Medium risk	
Year investment is estimated to reach end of useful life: 2045		

Table 23: 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	Agile
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	Medical Common Operating Picture (MEDCOP) has delivered 110 releases
Planned releases	MEDCOP has one release every 2 weeks, with plans to continue releasing biweekly for the full life cycle of the product
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Maintenance Repair and Overhaul Initiative (MRO)

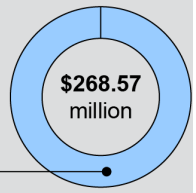
Program
Maintenance Repair and Overhaul (MRO)

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

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$0 mil

Total development, modernization and enhancement (DME)
$268.57 mil



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *Expects to*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

MRO will provide the Air Force Sustainment Center (AFSC) with the capability to support Agile planning, optimized workload assignment, resource allocation, integrated quality, and financials auditability.

Program essentials (reported by DOD officials as of March 2025)

Lead DOD component: Air Force	**Program owner:** Air Force	**Year investment began:** 2013
Acquisition pathway: Defense business systems		**Last milestone achieved:** Limited deployment ATP(s)
Next planned milestone: Limited deployment ATP(s)		**CIO evaluation rating:** 3 – Medium risk
Year investment is estimated to reach end of useful life: 2035		

Table 24: Maintenance, Repair and Overhaul Initiative's (MRO) 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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
Planned releases	6
Average time between releases	7-9 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Military Health System Information Platform (MIP)

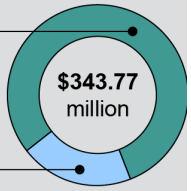
Program
Military Health System (MHS) Information Platform (MIP)

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

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$297.53 mil

Total development, modernization and enhancement (DME)
$46.24 mil



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

MIP serves to deliver health data to inform decision-making, including patient information and clinical decision support tools.

Program essentials (reported by DOD officials as of March 2025)

Lead DOD component: Defense-wide	**Program owner:** Enterprise Intelligence and Data Solutions, Program Management Office	**Year investment began:** 2019
Acquisition pathway: Defense business systems Acquisition of service		**Last milestone achieved:** Deliver capabilities
Next planned milestone: Deliver capabilities		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2035 at minimum		

Table 25: Military Health System Information Platform's (MIP) 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	9
Planned releases	14 per year
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

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

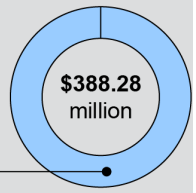
Program
Naval—Maintenance, Repair, and Overhaul (N-MRO)

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

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$0 mil

Total development, modernization and enhancement (DME)
$388.28 mil



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *Decrease*

Schedule: *Delay*

Rebaseline: *Expects to*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

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 February 2025)

Lead DOD component: Navy	**Program owner:** Navy	**Year investment began:** 2017
Acquisition pathway: Defense business systems, other transaction authority		**Last milestone achieved:** Requirements approved
Next planned milestone: Limited deployment ATP(s)		**CIO evaluation rating:** 3 – Medium risk
Year investment is estimated to reach end of useful life: 2043		

Table 26: Naval—Maintenance, Repair, and Overhaul's (N-MRO) 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; Incremental
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	20
Planned releases	29 (projected)
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

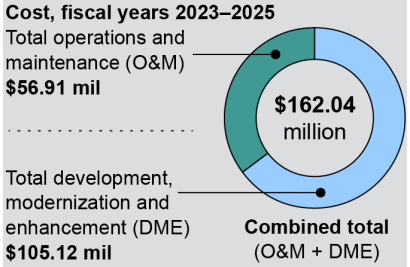
Naval Air Systems Command—Aviation Logistics Environment (NAVAIR-ALE)

Program
NAVAIR Aviation Logistics Environment (NAVAIR-ALE)

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

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

NAVAIR-ALE provides a global logistics enterprise solution, delivering capabilities via a net-centric, shared data environment that supports shore-based, afloat, and expeditionary operations. It also consolidates aging systems and aligns requirements.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Navy	**Program owner:** Navy	**Year investment began:** 2019
Acquisition pathway: Defense business systems		**Last milestone achieved:** Limited deployment ATPs
Next planned milestone: Continued modernization with limited deployments to migrate capabilities and sunset legacy fleet systems		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2030		

Table 27: Naval Air Systems Command—Aviation Logistics Environment's (NAVAIR-ALE) 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	DevSecOps
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	10
Planned releases	2 per year
Average time between releases	4-6 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

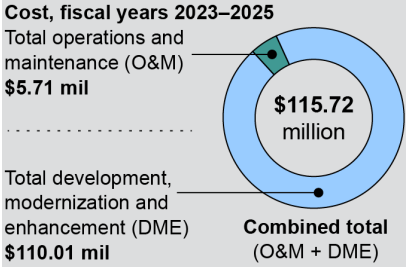
Navy Electronic Procurement System (Navy EPS)

Program
Navy Electronic Procurement System (NAVY EPS)

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

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *Decrease*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

Navy EPS is intended to modernize and consolidate Navy's legacy contract writing systems and other ancillary procurement systems.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Navy	**Program owner:** Navy	**Year investment began:** 2013
Acquisition pathway: Software acquisition		**Last milestone achieved:** Deliver capabilities
Next planned milestone: Deliver capabilities		**CIO evaluation rating:** 3 – Medium risk
Year investment is estimated to reach end of useful life: No estimated end date		

Table 28: Navy Electronic Procurement System's (Navy EPS) 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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 major release, 5 minor releases, 22 maintenance releases, and 50 patches
Planned releases	3 major releases, 22 minor releases, 107 maintenance releases
Average time between releases	Less than 1 month; quarterly for minor releases

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Navy Enterprise Resource Planning (Navy ERP)

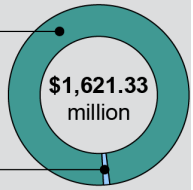
Program
Navy Enterprise Resource Planning (NAVY ERP)

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

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$1601.73 mil

Total development, modernization and enhancement (DME)
$19.60 mil



Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

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 March 2025)

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: 2027		

Table 29: 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	268
Planned releases	268
Average time between releases	Less than 1 month

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

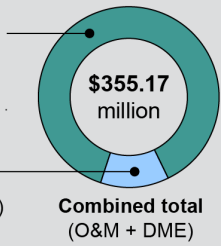
Navy Maritime Maintenance Enterprise Solution (NMMES)

Program
Navy Maritime Maintenance Enterprise Solution (NMMES)

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

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

NMMES is intended to consolidate select business applications supporting the management and execution of intermediate and depot-level maintenance of ships and submarines at the Naval Shipyards and Regional Maintenance Centers.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Navy	**Program Owner:** Navy	**Year investment began:** 2012
Acquisition pathway: Defense business systems, software acquisition, acquisition of service	**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: No estimated end date		

Table 30: Navy Maritime Maintenance Enterprise Solution's (NMMES) 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; DevOps; DevSecOps; Waterfall
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	361 (37 software releases, 317 production data fix releases, and 7 emergent releases)
Planned releases	37
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Navy Personnel and Pay (NP2)

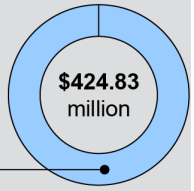
Program
Navy Personnel and Pay (NP2)

Software development approaches
Agile; Incremental

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$0 mil

Total development, modernization and enhancement (DME)
$424.83 mil



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

NP2 is Navy's human resources management business solution intended to provide integrated personnel and pay capabilities supporting over 400,000 active and reserve sailors and their families worldwide that replaces existing legacy human resource management systems.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Navy	**Program owner:** Navy	**Year investment began:** 2019
Acquisition pathway: Defense business systems	**Last milestone achieved:** Navy Personnel and Pay System technical delivery FY2023	
Next planned milestone: Fiscal year 2027 treasury direct disbursement / initial operating capability	**CIO evaluation rating:** 3 – Medium risk	
Year investment is estimated to reach end of useful life: No estimated end date		

Table 31: Navy Personnel and Pay's (NP2) 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
Delivery of a minimum viable product	Yes
Software documentation provided at each production milestone	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	32
Planned releases	32
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

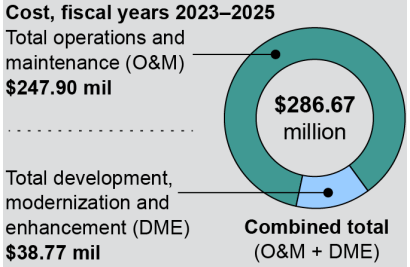
Real-Time Automated Personnel Identification System and Common Access Card (RAPIDS)

Program
Real-Time Automated Personnel Identification System and Common Access Card (RAPIDS)

Software development approaches
Waterfall

Average time of software deliveries

Cost, fiscal years 2023–2025



Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *No chnage*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

RAPIDS is DOD's enterprise system for producing identification cards. This includes the Common Access Card and Uniformed Services ID which facilitate access, provide official affiliation with DOD, and satisfy identification requirements.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Defense-wide	**Program owner:** Defense Human Resource Activity (DHRA), Defense Manpower Data Center (DMDC)	**Year investment began:** 1997
Acquisition pathway: Defense business systems		**Last milestone achieved:** Capability support ATP
Next planned milestone: Decommission		**CIO evaluation rating:** 3 – Medium risk
Year investment is estimated to reach end of useful life: No current end date		

Table 32: Real-Time Automated Personnel Identification System and Common Access Card's (RAPIDS) 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	Waterfall
Delivery of a minimum viable product	No
Software documentation provided at each production milestone	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	Unknown due to the age of the program
Planned releases	7 per 12-month contractual period
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Theater Medical Information Program—Joint Increment 2 (TMIP-J)

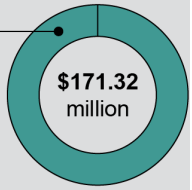
Program
Theater Medical Information Program—Joint Increment 2 (TMIP-J)

Software development approaches
Agile; Development, Operations (DevOps)

Average time of software deliveries

Cost, fiscal years 2023–2025
Total operations and maintenance (O&M)
$171.32 mil

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



Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2023)

Cost: *Increase*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2025 Federal IT Dashboard data; DOD program questionnaire responses as of February 2025. | GAO-25-107649

Program description

TMIP-J integrates components of the Military Health System base systems and the Services' medical information systems to ensure timely interoperable medical support and documentation for mobilization, deployment, and sustainment of all theater and deployed forces in support of any mission.

Program essentials (reported by DOD officials as of February 2025)

Lead DOD component: Defense-wide	**Program owner:** DHA, Program Executive Office Defense Healthcare Management Systems, Program Management Office JOMIS	**Year investment began:** 2009
Acquisition pathway: Defense business systems		**Last milestone achieved:** Deliver capabilities
Next planned milestone: Decommissioning		**CIO evaluation rating:** 4 – Moderately low risk
Year investment is estimated to reach end of useful life: 2029 for maritime medical modules, 2025 for other sections of TMIP-J		

Table 33: Theater Medical Information Program—Joint Increment 2's (TMIP-J) 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; DevOps
Delivery of a minimum viable product	No
Software documentation provided at each production milestone	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	637
Planned releases	637
Average time between releases	1-3 months

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2025. | GAO-25-107649

Appendix III: Comments from the Department of Defense

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

MAY 19 2025

Mr. Vijay D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. D'Souza,

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-25-107649, "IT SYSTEM ANNUAL ASSESSMENT: DOD Needs to Improve Performance Reporting and Cybersecurity Planning" dated March 28, 2025 (GAO Code 107649). The Department concurs with the content of the draft report. Enclosed are the detailed comments on the report recommendation.

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

Sincerely,

Kevin M. Mulvihill
Deputy Chief Information Officer
for Command, Control, and Communication

Enclosure:
As stated

GAO DRAFT REPORT DATED MARCH 28, 2025
GAO-25-107649 (GAO CODE 107649)

"IT SYSTEMS ANNUAL ASSESSMENT: DOD NEEDS TO IMPROVE PERFORMANCE REPORTING AND CYBERSECURITY PLANNING"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The Secretary of Defense should direct the Chief Information Officer and Under Secretary of Defense for Acquisition and Sustainment 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 RESPONSE: Concur. The DoD already requires major information technology (IT) business programs to report their minimum performance metrics data in each category, as appropriate, as part of the department's federal IT Dashboard submission, per the OMB A-11 and Capital Planning Guidance. The DoD implemented audit checks in April 2024 to have Components provide all major IT system performance metrics. In addition, the DoD Chief Information Officer (CIO) provides training and releases specific IT budget guidance that requires Components to report major IT investments' performance metrics data. The DoD increased the frequency of ITDB updates to ensure more timely data.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

Principal contributors to this report were Eric Trout (Assistant Director), Gerard Aflague (Analyst in Charge), Bryson Brading, Elizabeth Harris, Tyler Hodges, Smith Julmisse, Jess Lionne, Bradley Pedone, and Richard Sayoc. Other key contributors included Bea Alff, Amanda Andrade, Erin Carson, Andrea Harvey, Michael Holland, Jennifer Leotta, Scott Pettis, Daniel Ramsey, Claire Saint-Rossy, Henry Sutanto, Walter Vance, and Adam Vodraska, Jonathan Wall, and Merry Woo.