June 2023

IT SYSTEMS ANNUAL ASSESSMENT

DOD Needs to Improve Performance Reporting and Development Planning

Revised, August 22, 2024, to correct figure on page 34 and its associated supporting text.

IT SYSTEMS ANNUAL ASSESSMENT

DOD Needs to Improve Performance Reporting and Development Planning

Why GAO Did This Study

For FY 2023, DOD requested approximately $45.2 billion for its unclassified IT investments, encompassing essential infrastructure, communications, and business systems. This includes the department's major IT programs, which are intended to help sustain key business operations such as contracting, logistics, human resources, and financial management.

The NDAA for FY 2019, as amended, includes a provision for GAO to assess selected DOD IT programs annually through March 2026. GAO's objectives were to (1) examine how DOD's portfolio of major IT business programs has performed, (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 these objectives, GAO selected the 25 major IT business programs DOD reported in its FY 2023 submission to the Federal IT Dashboard (a public website with information on the performance of IT investments). GAO analyzed the Dashboard data to examine DOD's planned expenditures for these programs and for its standard IT infrastructure (the supporting hardware, software, and services that a business system requires to operate) from FY 2021 through FY 2023. GAO compared programs' operational performance data to OMB guidance. GAO also met with DOD OCIO officials to determine reasons for differences between how metrics data were reported and reporting guidance.

What GAO Found

According to the Department of Defense's (DOD) fiscal year (FY) 2023 submission to the Federal IT Dashboard, DOD planned to spend about $9 billion on its portfolio of 25 major IT business programs and about $31 billion on its 723 standard IT infrastructure investments from FY 2021 through FY 2023. These two areas accounted for 30 percent of total planned spending on the department's unclassified IT portfolio (see figure).

The Department of Defense's Major IT Programs and IT Infrastructure Accounted for 30% of Total Planned Spending on Its Unclassified IT for Fiscal Years 2021–2023
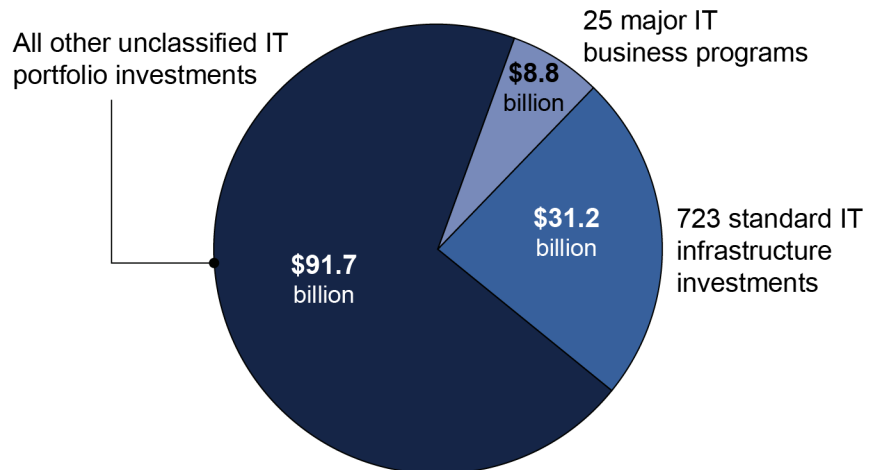
Source: GAO analysis of FY 2023 Department of Defense budget data. | GAO 23-106117

Sixteen of the 25 major IT business programs reported cost or schedule changes since January 2021, including 12 that had cost increases ranging from $43 thousand to $194 million (a median of $4.6 million); 12 had schedule delays ranging from 3 to 33 months (a median of 24 months). Program officials attributed the changes to factors such as new requirements and unanticipated technical complexities.

Programs also reported performance data. As of January 2023, 22 of the 25 programs identified at least the minimum required number of operational performance metrics, consistent with Office of Management and Budget (OMB) guidance. However, the other three programs did not identify the minimum required metrics, including two that did not identify any metrics data. Additionally, eight programs did not fully report on the extent to which they achieved their targets. By not ensuring that programs fully identify and report required performance metrics, DOD limits program accountability and its own ability to effectively oversee performance.

As of February 2023, officials for the eight programs that we identified as actively developing software reported using recommended iterative development approaches and practices that can limit risks of adverse cost and schedule outcomes. In addition, five of the eight programs reported delivering software functionality every 6 months or less as called for in OMB guidance (see table).

—— **United States Government Accountability Office**

In addition, GAO administered a questionnaire to the 25 program offices to obtain information about cost and schedule changes that the programs had experienced since January 2021. The questionnaire also sought information about software development and cybersecurity practices used by the programs, including whether users were involved during the development process. GAO compared the responses to relevant guidance and leading practices to identify gaps and risks. For programs that did not demonstrate having plans, strategies, or other comparable documents, GAO followed up with DOD officials for clarification.

Further, GAO reviewed actions DOD has taken to implement its plans for addressing previously identified legislative and policy changes that could affect its IT acquisitions. This included reviewing policy, plans, and guidance associated with the department's efforts to (1) reorganize former CMO responsibilities and (2) implement changes associated with its defense business systems investment management guidance and business enterprise architecture. GAO met with DOD officials to discuss each of the topics addressed in this report.

What GAO Recommends

GAO is making two recommendations to DOD to ensure programs (1) identify operational performance metrics data, as appropriate, in its reporting to the Federal IT Dashboard and (2) develop plans that address conducting user training and deployment, as appropriate. GAO also reiterates the need for DOD to address previous recommendations focused on improving major IT programs.

DOD agreed with the content of GAO's report, but did not concur with the recommendations because the department believes it has already taken actions to address them. However, the department did not provide sufficient evidence indicating it had done so. As a result, GAO continues to believe the recommendations are appropriate.

Department of Defense 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
Uses an iterative development approach	8 of 8
Uses Agile as an approach	6 of 8
Delivery of minimum viable product	7 of 8
Delivery of software at least every 6 months	5 of 8

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023.| GAO-23-160117

Moreover, recognizing the importance of user involvement throughout the software development process, officials for all eight programs in active development reported involving users through collecting feedback during requirements development and refinement. In addition, most of the 25 major IT business programs in various stages reported involving users through testing and surveying them about customer experience (see table).

Department of Defense Major IT Business Programs in Various Stages of Development Reported Conducting Activities to Involve Users

User involvement activity	Number of programs that reported conducting each activity
Collecting user feedback during development	8 of 8
Involving users in testing	23 of 25
Surveying users about customer experience	20 of 25

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023. | GAO-23-160117

However, as of February 2023, 11 of the 25 programs did not demonstrate having approved plans for conducting user training and deployment as required by DOD. Program officials provided various reasons for not having the plans, including the system nearing retirement or predating the requirement. However, DOD officials acknowledged that programs should have user training and deployment plans and stated that they will follow up with the programs that did not have them. Without such plans, the department is at increased risk of programs not achieving required organizational changes and delivering business systems that do not meet their users' needs and are not widely adopted by users.

Further, while program officials reported conducting cybersecurity assessments and tests, six programs did not demonstrate having an approved cybersecurity strategy as required. In June 2022, GAO reported that 10 of DOD's major IT business programs did not have approved strategies and recommended the DOD Chief Information Officer (CIO) ensure programs develop them. The department concurred with the recommendation and, as of March 2023, officials stated that they were following up with the programs that did not have one. Until the department ensures that all programs develop strategies, it lacks assurance that programs are positioned to effectively manage cybersecurity risks and mitigate threats. As a result, DOD programs are at increased risk of adverse cost, schedule, and performance impacts.

Regarding legislative and policy changes, DOD has taken actions to implement the National Defense Authorization Act (NDAA) for FY 2021, which eliminated the DOD Chief Management Officer (CMO) position. This position previously had broad oversight responsibilities for the department's business systems. In September 2021, the Deputy Secretary of Defense directed an extensive realignment of the responsibilities previously assigned to the CMO. In March 2023, GAO reported on DOD's oversight of its business systems and recommended that DOD update guidance for addressing statutory requirements for initially approving and annually certifying business systems and maintain complete and accurate data for its systems, among other things. The department has efforts underway to implement changes, including plans to issue revised business systems investment management guidance. GAO will continue to monitor DOD's efforts to redistribute the roles and responsibilities formerly assigned to the CMO and to improve how the department manages its IT investments.

Contents

Figures

Abbreviations

A&S	Acquisition and Sustainment
ACWS	Army Contract Writing System
AFIPPS	Air Force Integrated Personnel and Pay System
ATP	authority to proceed
CIO	Chief Information Officer
CMO	Chief Management Officer
COTS	commercial off-the-shelf
DAI	Defense Agencies Initiative
DEAMS	Defense Enterprise Accounting and Management System-Increment 1
DevOps	development and operations
DevSecOps	development, security, and operations
DHMSM	Department of Defense Healthcare Management System Modernization
DME	development, modernization, and enhancement
DOD	Department of Defense
DSS	Distributed Standard System
FY	fiscal year
GCSS-A	Global Combat Support System-Army
MIP	Military Health System Information Platform
MROI	Maintenance Repair and Overhaul Initiative
Navy EPS	Navy Electronic Procurement System
Navy ERP	Navy Enterprise Resource Planning
NDAA	National Defense Authorization Act
O&S	operations and sustainment
OMB	Office of Management and Budget
USD(C)	Under Secretary of Defense (Comptroller)/Chief Financial Officer

June 13, 2023

Congressional Committees

The Department of Defense (DOD) is one of the largest and most complex organizations in the world. To protect the security of our nation and deter war, DOD relies heavily on the use of IT. For fiscal year (FY) 2023, the department requested approximately $45.2 billion for its unclassified IT investments.[1]

Collectively, these investments encompass essential infrastructure, communications, and business systems that support DOD processes and services and provide department officials with information used to plan, direct, and monitor mission operations. This includes DOD's major IT programs, which are intended to help sustain key business operations (e.g., contracting, logistics, human resources, and financial management).

The John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 included a provision for GAO to conduct annual assessments of selected DOD IT programs, which was recently extended through March 2026.[2] This report presents the results of our fourth annual assessment. Our specific objectives for this assessment were to (1)

---

[1]Department of Defense (DOD)*, Information Technology and Cyberspace Activities Budget Overview: Fiscal Year (FY) 2023 Budget Request* (May 2022). This figure does not reflect all funding requested for DOD's IT systems. For example, classified systems are not included. In addition, not all DOD IT expenditures are reported separately from their respective programs if those programs are developing more than software and hardware to support the software. 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: Challenges to Fielding Capabilities Faster Persist,* GAO-22-105230 (Washington, D.C.: June 8, 2022).

[2]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 and amended by Pub. L. No.116–283 (William M. [Mac] Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021), §§ 813, 1807(g)(1), 134 Stat. 3388, 3749 and 4159 (Jan. 1, 2021). Under this provision, we are to report on these assessments no later than March 30 of each year from 2020 through 2023. 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-22-105230. Congress and the President recently extended this mandate through 2026 in Section 812 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, 136 Stat. 2395, 2706 (Dec. 23, 2022).

examine how DOD's portfolio of major IT business programs has performed, (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, we selected the 25 business programs that DOD listed as major IT investments in its FY 2023 submission to the Federal IT Dashboard (Dashboard).[3] We analyzed Dashboard data to examine how much the department reported planning to spend on these 25 major IT business programs from FY 2021 through FY 2023. Additionally, we compared DOD's planned spending on the four largest business programs during the 3-year period to its total planned spending for the full portfolio of 25.

We also analyzed responses to a questionnaire we developed and administered to all 25 programs in October 2022. Programs provided their responses between October 2022 and December 2022, and we followed up with programs about their responses through February 2023. The questionnaire included questions about whether programs had experienced cost or schedule changes since January 1, 2021, and whether programs had rebaselined or expect to rebaseline as a result of the changes.[4]

In addition to the 25 major IT business programs, we analyzed the Dashboard data to determine how much DOD reported planning to spend on its 723 standard IT infrastructure investments from FY 2021 through

---

[3]The Federal IT Dashboard is a public, government website previously operated by the Office of Management and Budget (OMB) and currently by the General Services Administration (GSA) at https://itdashboard.gov. It includes streamlined data to enable agencies and Congress to understand and manage federal IT portfolios and make better IT planning decisions and includes information on the performance of major IT investments. We initially considered 28 business programs that DOD listed as major IT investments at the start of our review in June 2022 and excluded three programs based on the department no longer considering them to be major investments. We determined the number of major IT business programs to be the remaining 25.

[4]OMB 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.

FY 2023.[5] We also used the department's FY 2023 budget data to compare its planned spending on the business programs and infrastructure investments during the 3-year period to its total planned spending for the unclassified IT portfolio.[6]

Further, for the 25 business programs, we analyzed programs' FY 2023 performance data as of January 2023 and compared the data to the Office of Management and Budget (OMB) guidance.[7] We also met with officials within DOD's Office of the Chief Information Officer (CIO) to determine reasons for differences between how operational performance metrics data were reported and guidance for such reporting.

For the second objective, we sought information on the software development and cybersecurity practices used by the 25 major IT business programs via our questionnaire, including eight programs that we identified as actively developing software.[8] We collected and analyzed key information and supporting documents related to each of the 25 programs' software development and cybersecurity practices, including information about involving users throughout the development process, capability implementation plans, and cybersecurity strategies. For programs that did not demonstrate having plans, strategies, or other comparable documents, we followed up with officials within DOD CIO and the Office of the Under Secretary of Defense for Acquisition and Sustainment (A&S) for clarification.

We aggregated the program office responses to our questionnaire and compared the information to relevant guidance and leading practices (e.g., Defense Innovation Board and Defense Science Board reports,

---

[5]IT infrastructure is the supporting hardware, software, communication, and information security services that a business system requires to operate, but that can be shared by multiple business systems for scalability.

[6]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year (FY) 2023 Budget Request* (May 2022).

[7]DOD collected the FY 2023 performance metrics data and reported it to GSA; however, it did not get posted publically to the Dashboard as it has in previous years. DOD sent us the data in August 2022 and we confirmed that it was still current in January 2023. Office of Management and Budget, *FY 2022 IT Budget—Capital Planning Guidance* (Washington, D.C.: Nov. 16, 2020).

[8]For the purposes of this assessment, we considered programs to be actively developing software if program officials reported they were actively developing new software functionality or if they had not yet reached full deployment authority to proceed.

DOD instructions, and OMB guidance) to identify where there were gaps.[9] In doing so, we identified key challenges associated with software development and cybersecurity and risks associated with not following guidance and leading practices that may affect acquisition outcomes relative to cost, schedule, and performance.

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.[10] The objective focused on DOD's efforts to reorganize former Chief Management Officer (CMO) responsibilities and planned improvements to the department's IT portfolio management (i.e., updates to its investment management guidance and business enterprise architecture). To assess the potential 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 examining major defense acquisition programs that was conducted under this same provision of the NDAA for FY 2019.[11] Appendix I provides a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from June 2022 to June 2023 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.

---

[9]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense*, Test and Evaluation*, DOD Instruction 5000.89 (Nov. 19, 2020); Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense, *Business Systems Requirements and Acquisition*, DOD Instruction 5000.75, Incorporating Change 2, Jan. 24, 2020 (Washington, D.C.: Feb. 2, 2017); Office of Management and Budget, *FY 2022 IT Budget—Capital Planning Guidance* (Washington, D.C.: Nov. 16, 2020).

[10]The previously identified legislative and policy changes are discussed in previous quick look and related reports. For example, see GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, GAO-22-105330 (Washington, D.C.: June 14, 2022).

[11]GAO-22-105230.

Background

In support of its military operations, DOD manages many IT investments encompassing critical infrastructure, communications, command and control, and business systems. According to DOD's FY 2023 budget request, the department requested approximately $57.9 billion for its total FY 2023 IT and cyber activities, including $45.2 billion for its unclassified IT investments. In addition, DOD planned to spend $131.7 billion on these unclassified investments from FY 2021 through FY 2023. These investments include DOD's major IT business programs, which are intended to help the department sustain key business operations (e.g., contracting, logistics, human capital, health care, and financial management). They also include its standard IT infrastructure investments, which are supporting hardware, software, communication, and information security services that a business system requires to operate.[12]

As part of DOD's budget submissions, investment expenditures are broken down into two main categories: (1) development, modernization, and enhancement (DME) costs and (2) operations and sustainment (O&S) costs.[13] These categories represent the two higher-level phases of the system life cycle, also referred to as development and sustainment.

Development generally starts at the capability need–identification stage and includes all of the activities associated with developing new functionality or enhancements, including the delivery of limited and full deployments. A limited deployment is any deployment before the full deployment authority to proceed (ATP) that provides a set of functionality to a set of users of the business system. The functional sponsor and program manager recommend the functionality and number of users. Limited deployments are approved at a limited deployment ATP. This is 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] Multiple limited deployments may be authorized at the same decision point or at other points. Full deployment is the delivery of full functionality to all planned users of the

---

[12]These IT infrastructure services can be shared by multiple business systems for scalability.

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

[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.

business system in accordance with the full deployment ATP. This is a decision point where the milestone decision authority considers the results of limited deployment(s) and operational testing and approves deployment to the entire user community.

Sustainment generally starts during the capability support stage and includes all of the activities associated with maintaining fully deployed, existing functionality. Capability support is a phase where the functional sponsor manages and governs the business capability. In this phase, the program manager oversees the technical implementation and configuration of the business 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).

DOD's Policy and Framework for Managing Major IT Acquisitions

In January 2020, DOD updated its acquisition policy to create a framework to enable flexible and responsive acquisitions. The reissued DOD Instruction 5000.02 established the new adaptive acquisition framework, provided high-level policy for the framework, and assigned roles and responsibilities to acquisition officials.[15] The department subsequently issued new policies to continue replacing the old approach. In addition, DOD Instruction 5000.02 was also 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) defense business systems acquisition, (5) software acquisition, and (6) defense acquisition of services. Additionally, the framework calls for program managers to continuously address cybersecurity throughout the program life cycle and establish a risk-management program.

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.

---

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

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

In January 2020, DOD updated the instruction for the 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.[16] While maintaining the general structure of the defense business systems pathway, the 2020 update removed certain oversight requirements and encouraged a tailored approach to each program. The 2020 update also enabled and encouraged acquisition officials to delegate decision-making down to the "lowest practical level."

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

- align the program with commercial best practices;

- minimize the need for customization of commercial products to the maximum 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 or incremental software development processes to the greatest extent practical.

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

---

[16]Department of Defense, *Business Systems Requirements and Acquisition, Instruction 5000.75* (incorporating change 2 [Jan. 24, 2020]) (Washington, D.C.: Feb. 2, 2017).

Figure 1: The Department of Defense's Business Capability Acquisition Cycle
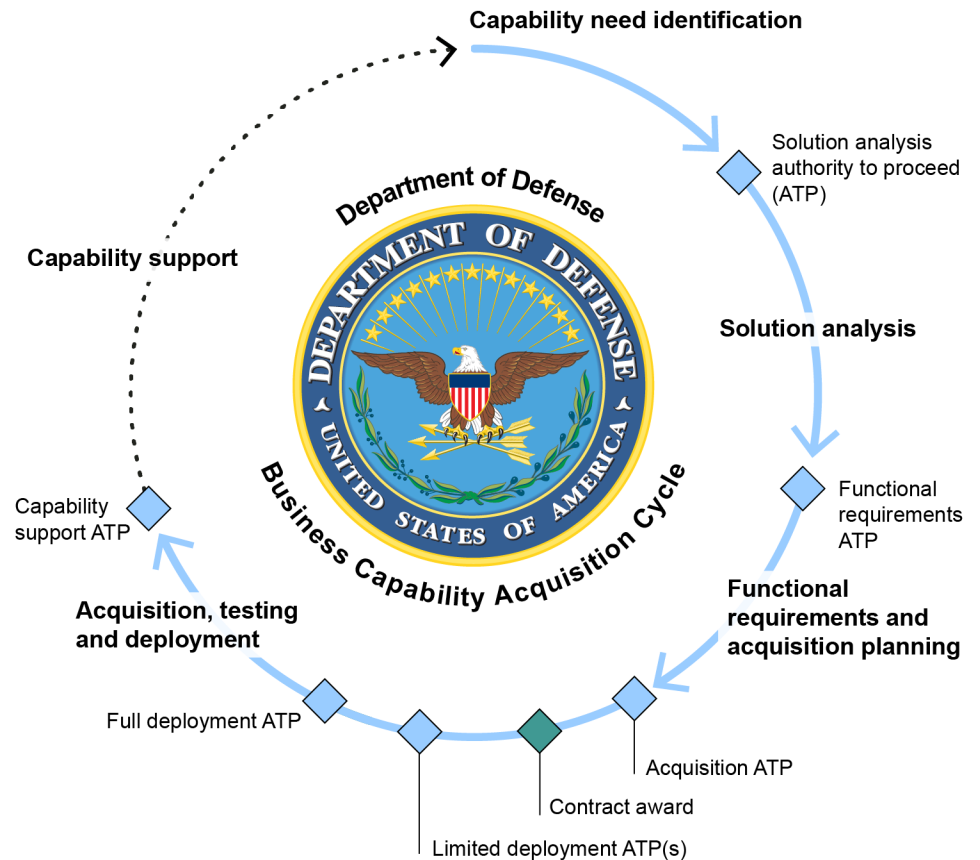
Source: Department of Defense Instruction 5000.75 (January 2020). | GAO-23-106117

Software Acquisition Pathway

Section 800 of the NDAA for FY 2020 mandated that DOD develop the software acquisition pathway.[17] In October 2020, the department issued guidance titled Operation of the Software Acquisition Pathway, Instruction 5000.87.[18] According to this Instruction, the purpose of the pathway is to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software.

---

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

[18]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).

According to DOD Instruction 5000.02, the software acquisition pathway is intended to integrate modern software development practices such as Agile; development, security, and operations (DevSecOps); and lean practices.[19] 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.

---

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

Figure 2: The Department of Defense's Software Acquisition Pathway
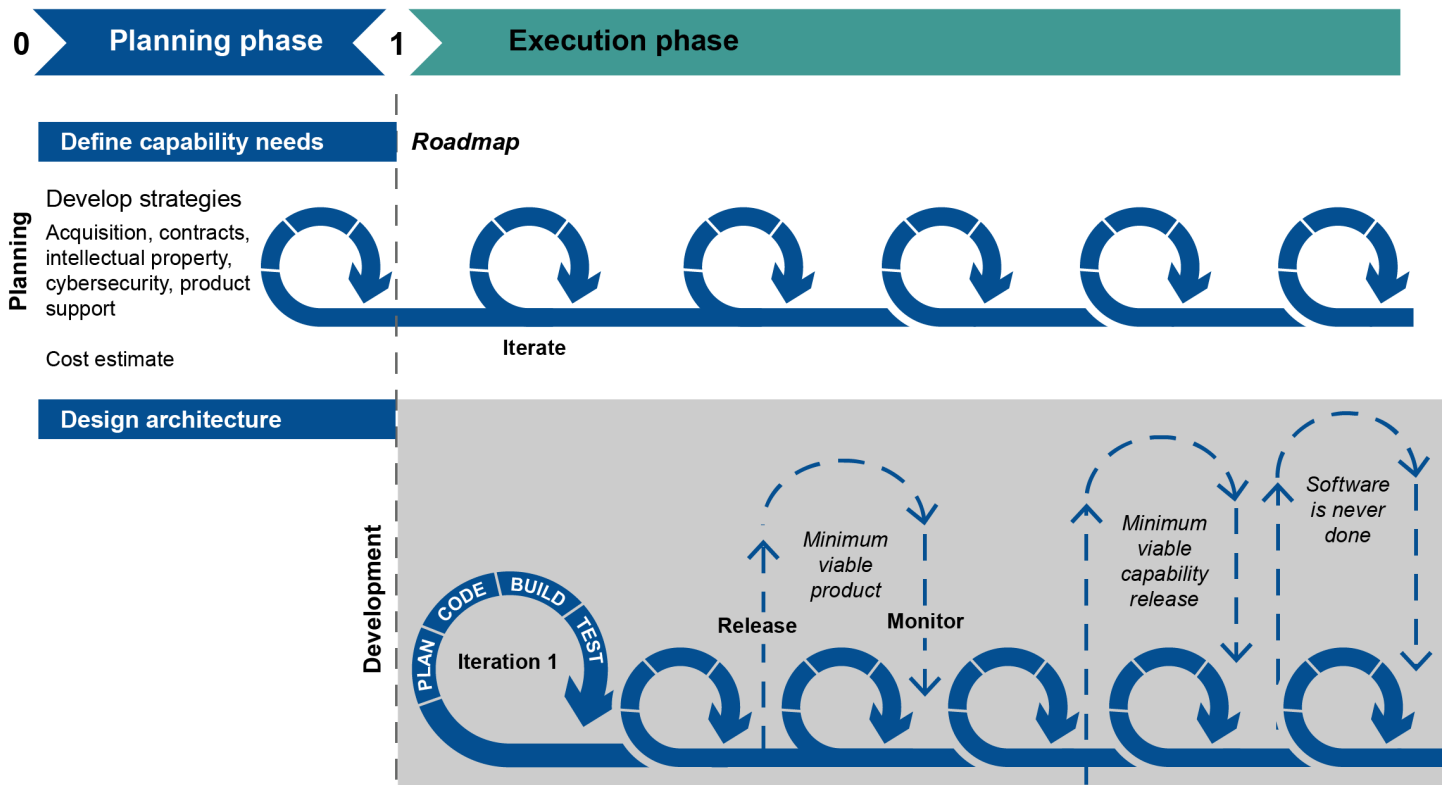
Source: Department of Defense Instruction 5000.87 (October 2020). | GAO-23-106117

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

DOD's Initial Implementation of Agile Software Development

Consistent with studies recommending DOD's transition toward Agile software development,[20] and to implement statutory mandates to help enable its transition, the department has begun implementing Agile as

---

[20]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington, D.C.: Feb. 18, 2018). Defense Innovation Board, *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Washington, D.C.: May 3, 2019).

part of its software modernization initiatives.[21] 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 allows program staff to catch errors quickly and continuously, integrate new code with ease, and obtain user feedback throughout the process.

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 capability acquisition cycle can be similar to a minimum viable product in Agile development methodology, and the program team is expected to iteratively release functionality. In addition, the software acquisition pathway requires the use of iterative and Agile practices.

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.[22] 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 is to continue through FY 2023.

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

---

[21]Sections 873 and 874 of the National Defense Authorization Act for Fiscal Year 2018 established two Agile pilot programs, Pub. L. No. 115-91, §§ 873-874, 131 Stat. 1283, 1498-1503 (Dec. 12, 2017). Section 800 of the National Defense Authorization Act for Fiscal Year 2020 established a software acquisition pathway that, according to DOD Instruction 5000.02, is to include support for Agile practices. 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-22-105230.

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

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

transforming processes and developing personnel. The strategy has three goals:

1. Accelerate development of the DOD enterprise cloud environment
2. Establish a department-wide software factory environment
3. 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 CIO; Under Secretary of Defense for Acquisition & Sustainment (A&S); Under Secretary of Defense for Research and Engineering; Under Secretary of Defense for Intelligence & Security; Director, Operational Test and Evaluation; and Director, Cost Assessment and Program Evaluation, as well as the military departments and services, Joint Chiefs of Staff, and the Defense Information Systems Agency.

DOD's Cybersecurity Guidance

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

Additionally, DOD Instruction 8510.01 documents specific guidance for IT risk management.[25] Under this instruction, all DOD IT systems must be categorized in accordance with Committee on National Security Systems Instruction 1253[26] and implement a corresponding set of security controls and assessments from National Institute of Standards and Technology

---

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

[25]Department of Defense, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, Instruction 8510.01 (incorporating change 3 [Dec. 29, 2020]) (Washington, D.C.: Mar. 12, 2014).

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

Special Publication 800-53.[27] The guidance requires officials responsible for IT systems to identify resources needed to implement DOD's risk management framework, develop and maintain milestones and a plan of action to address known vulnerabilities, and designate an official responsible for authorizing the system's operation based on its risk posture. The instruction also clarifies that the risk management framework will inform acquisition processes for requirements development, procurement, and developmental and operational testing and evaluation.

DOD's Chief Management Officer Position Repealed by Statute

The NDAA for FY 2018 codified the position of Chief Management Officer (CMO).[28] Additional responsibilities and functions for the CMO were enacted in the NDAA for FY 2019.[29] The CMO's responsibilities included managing DOD's enterprise business operations and exercising authority, direction, and control over the department's shared business services. The CMO was also responsible for overseeing efforts associated with the business system acquisition pathway.

In January 2021, section 901 of the William M. (Mac) Thornberry NDAA for FY 2021 repealed the position of CMO within DOD.[30] The NDAA also mandated that within one year the department transfer the responsibilities, personnel, functions, and assets of the CMO to other organizations within DOD and provide a report to Congress with any associated recommendations for legislative action by January 2022. In response to this requirement, in September 2021 the Deputy Secretary of Defense issued a memorandum directing realignments of the responsibilities previously assigned to the CMO.

The Federal IT Dashboard

The Director of the Office of Management and Budget (OMB) is required by statute to make information on major federal IT investments of covered agencies (including DOD) publicly available, in accordance with detailed

---

[27]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).

[28]Pub. L. No. 115-91, § 910, 131 Stat. 1283, 1516-1519 (Dec. 12, 2017).

[29]Pub. L. No. 115-232, § 921, 132 Stat. 1636, 1926-1929 (Aug. 13, 2018).

[30]Pub. L. No. 116-283 § 901, 134 Stat. 3388, 3794-3795 (Jan. 1, 2021).

OMB guidance.[31] This information is displayed on the Federal IT Dashboard, a public, government website that includes streamlined data and information on the performance of major IT investments. The Dashboard is intended to enable agencies and Congress to better understand and manage federal IT portfolios and make better IT planning decisions. In March 2022, the Dashboard's management responsibilities—including collecting, analyzing, and displaying IT budget and performance data—transitioned from OMB to the General Services Administration's (GSA) Office of Government-wide Policy;[32] however, OMB guidance continues to dictate many aspects of the reporting.[33] While OMB guidance provides a general definition of a major IT investment, it gives each covered agency the flexibility to establish specific criteria.

According to officials from the office of the DOD CIO and DOD guidance,[34] the department's major IT investments include: (1) major defense acquisition programs[35] determined to be IT investments by the DOD CIO; (2) IT programs with a budget greater than $43 million for FY 2022 or greater than $569.2 million greater across the future years

---

[31]Subtitle D of Title VIII of the 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).

[32]DOD's FY 2023 data was available on the Dashboard at the start of our review in June 2022 and remained available until November 2022; however, due to a technical issue, the data is not currently displayed publically. DOD officials stated that they are working with GSA to resolve the issue and expect the data to be publically available again for DOD's FY 2024 submission.

[33]FY 2023 reporting requirements for IT investments are contained in section 55 of OMB's Circular A-11 guidance. Office of Management and Budget, *Circular No. A-11, Preparation, Submission, and Execution of the Budget* (Washington, D.C.: Aug. 6, 2021). OMB's FY 2022 capital planning guidance was the most current guidance for reporting performance data at the time of DOD's FY 2023 submission to the Dashboard and the guidance has been updated in OMB's Circular A-11 guidance for FY 2024. Office of Management and Budget, *FY 2022 IT Budget—Capital Planning Guidance* (Washington, D.C.: Nov. 16, 2020). For subsequent years, GSA has issued guidance as well.

[34]Department of Defense, *FY 2023 Information Technology/Cyberspace Activities Budget Guidance* (Washington, D.C.: July 15, 2021).

[35]DOD defines a major defense acquisition program as a program where the dollar value for all increments of the program is estimated by the defense acquisition executive to require an eventual total expenditure for (1) research, development, and test and evaluation of more than $525 million in FY 2020 constant dollars; (2) procurement of more than $3.065 billion in FY 2020 constant dollars; or (3) a program designated as special interest by the milestone decision authority.

defense plan;[36] and (3) IT investments designated as major by department leadership.

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 outcomes. We have issued a series of reports that noted both the significant steps that OMB had previously taken to enhance the oversight, transparency, and accountability of federal IT investments by creating the Dashboard. These reports also addressed issues with the accuracy and reliability of the Dashboard's data.[37] Accordingly, we made recommendations to OMB to address these issues, which it implemented.

GAO's Recent Reviews of DOD IT Systems

In 2020 and 2021, GAO reported on DOD's portfolio of major IT business systems and DOD's efforts to modify how it collects and reports acquisition program data.[38] Among other things, our 2021 report addressed the program risk ratings that DOD reported to the Federal IT Dashboard. In June 2021, GAO made recommendations aimed at improving how DOD approaches both of these efforts.

---

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

[37]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).

[38]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); and *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, GAO-21-182 (Washington, D.C.: Dec. 23, 2020).

OMB requires that each federal agency CIO rate the risk of its major IT investments on a scale of 1 to 5, with 1 reflecting more risk and 5 reflecting less risk. These ratings are to be reported on the Dashboard. In June 2021, GAO reported that some DOD IT programs could be underreporting risks.[39]

For example, our assessments of program risk found that, of 22 programs that were actively using a risk register to manage program risks, 10 programs reflected greater risk than reported by DOD. Among other things, DOD CIO officials stated that different approaches for assessing program risks was likely a factor in the difference between the DOD CIO's and our risk ratings. Nevertheless, our assessments showed that some programs could be underreporting program risks.

We recommended that, for the next submission to the Federal IT Dashboard, the DOD CIO revisit risk ratings for the programs where their ratings indicated less risk than GAO's assessment. DOD concurred with our recommendation. In January 2022, officials from the office of the DOD CIO stated that they asked the programs with CIO risk ratings lower than GAO's ratings to reassess their ratings for their next submission. As of March 2023, the recommendation has not been implemented, and we will revisit the status of the recommendation after updates to program risk ratings are publicly available on the Dashboard.

In addition, our June 2021 report discussed steps DOD was taking to collect and report acquisition program data. Specifically, the report noted that, since June 2020, DOD had issued a series of policies, memos, and plans intended to improve the sharing and transparency of data it uses to monitor its acquisitions. For example, according to a November 2020 proposal from the Office of the Under Secretary of Defense for A&S, DOD officials were to develop data strategies and metrics to assess performance for the department's acquisition pathways. However, as of February 2021, DOD had not developed data strategies and had not finalized metrics for the business systems and software pathways. We also reported that officials said they were working with DOD programs and components to finalize initial pathway metrics.

We recommended that, in consultation with appropriate stakeholders, DOD ensure the data strategies and data collection efforts for the business system and software acquisition pathways define, collect,

---

[39]GAO-21-351 described our detailed approach for assessing program risk.

automate, and share, with the appropriate level of visibility, the metrics that are (1) necessary for stakeholders to monitor acquisitions and (2) critical to the department's ability to assess acquisition performance. DOD concurred with our recommendation. In October 2021, an official from DOD's Washington Headquarters Services provided a corrective action plan intended to help address the recommendation. This included establishing a data collection strategy and reporting template for the software pathway and collecting data in October 2021 and April 2022. In addition, the plan stated that DOD would identify reporting thresholds and metrics for the business systems pathway by the third quarter of FY 2022 and document required data elements by the fourth quarter of FY 2022. As of March 2023, DOD has not yet demonstrated that it completed these tasks and the recommendation has not yet been implemented.[40]

In addition, in June 2021, GAO reported on cybersecurity at the Defense Logistics Agency in which we assessed critical DOD IT systems to determine whether they had fully addressed steps for cybersecurity risk management and made one recommendation aimed at ensuring systems had approved cybersecurity strategies.[41] As of March 2023, DOD has not yet demonstrated that it completed these tasks and the recommendation remains open.

Further, our June 2022 report included three recommendations related to DOD ensuring programs (1) report operational performance data to the Federal IT Dashboard, (2) develop cybersecurity strategies, and (3) develop supply chain risk management plans that address information and communications technology considerations, as appropriate.[42] DOD concurred with GAO's recommendations and described actions it was taking and planned to take to address them. As of March 2023, the recommendations had not yet been implemented.

In March 2023, we reported on DOD's financial management systems and found that the department's guidance for addressing business system modernization statutory requirements for initially approving and

---

[40]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-22-104687. As of March 2023, the two recommendations from that report are also still open.

[41]GAO, *Defense Cybersecurity: Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Systems*, GAO-21-278 (Washington, D.C.: June 21, 2021).

[42]GAO-22-105330.

annually certifying business systems did not fully address key requirements, such as addressing DOD's auditability requirements.[43] In addition, we found that DOD does not apply key requirements to systems in sustainment, even though the statute does not provide for such an exclusion. We made nine recommendations, including that DOD and the military departments update guidance for initial approvals and annual certifications of business and financial systems to substantiate and document compliance with requirements. In addition, we recommended that the department ensure that the data collected on the extent of business and financial system compliance with statutory requirements are reliable. Further, we recommended that the department implement a strategic approach to workforce planning that, among other things, analyzes gaps in capabilities between existing staff and future needs, and formulates strategies to fill expected gaps. DOD concurred with seven of the recommendations and partially concurred with the remaining two.

In addition, DOD's business systems modernization efforts have been on GAO's High-Risk List since 1995, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments, including for its major IT programs.[44] The list focuses attention on government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement or that are in need of transformation to address economy, efficiency, or effectiveness challenges. As we reported in March 2021, DOD has only partially met the leadership commitment criterion of our High-Risk List.

In December 2022, officials from DOD's Offices of the Chief Information Officer (CIO) and the Director of Administration and Management described efforts underway to address the DOD business systems modernization high-risk area. An official from DOD CIO indicated that the department intends to develop an action plan that would include tasks and associated milestones for its efforts to update its business enterprise

---

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

[44]For example, see GAO, *High-Risk Series*, GAO-HR-95-1 (Washington, D.C.: Feb. 1, 1995) and additional work such as GAO-21-119SP and GAO-19-157SP.

architecture.[45] GAO reiterates the need for DOD to address previous recommendations focused on improving major IT programs.

Major DOD IT Programs Reported Cost and Schedule Changes, but Not All Reported Required Performance Data

According to DOD's FY 2023 Federal IT Dashboard data, the department planned to spend just under $9 billion on its portfolio of 25 major IT business programs from FY 2021 through FY 2023, with the four largest of these programs accounting for nearly 50 percent of its total planned spending on the full portfolio.[46] Based on questionnaire responses, 16 of the 25 business programs reported experiencing cost or schedule changes since January 2021, including cost increases ranging from $43 thousand to $194 million (a median of $4.6 million) and schedule delays ranging from 3 months to 33 months (a median of 24 months). Seven programs also reported rebaselining or expecting to rebaseline as a result of the cost and schedule changes and provided a variety of reasons for the changes, including new requirements, contractor issues, and unanticipated technical complexities.[47]

In addition to the 25 major IT business programs, DOD reported planning to spend about $31 billion on its 723 standard IT infrastructure investments (i.e., supporting hardware, software, communication, and information security services that a business system requires to operate) from FY 2021 through FY 2023. These two areas accounted for 30 percent of total planned spending on its unclassified IT portfolio during the 3-year period.[48]

Programs also reported operational performance data. As of January 2023, 22 of the 25 major IT business programs identified at least the minimum required number of operational performance metrics in each of

---

[45]As of January 2023, there are 14 recommendations that DOD has not yet implemented associated with this high-risk area. These do not include the nine recommendations that we made in our March 2023 report on DOD's financial management systems.

[46]In June 2022, we released the 2022 "DOD IT Quick Look" report (GAO-22-105330), which discussed 25 major IT business programs that DOD reported as part of its FY 2022 submission to the Federal IT Dashboard. As a result of program retirements and reclassifications, two programs from last year's review were not included in this review and two were added.

[47]The Office of Management and Budget states that agencies and contractors should establish a performance measurement baseline to track progress and report cost and schedule variance. Changes, or rebaselines, should be reviewed and approved according to agency governance processes.

[48]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year (FY) 2023 Budget Request* (May 2022).

the required categories and, in total, reported 141 operational performance metrics consistent with OMB's guidance. However, the other three programs did not identify the minimum required number of metrics. In addition, eight of the 25 programs did not fully report progress relative to these metrics, including two that did not report any data.[49]

DOD Planned to Spend Almost $9 Billion on Its 25 Major IT Business Programs from FY 2021 through FY 2023

From FY 2021 through FY 2023, DOD budgeted just under $9 billion for its 25 major IT business programs, with the four largest of these programs accounting for nearly 50 percent of its total planned spending on the full portfolio. Specifically, based on our analysis of DOD's FY 2023 Dashboard data, the department reported spending almost $3 billion on the 25 business programs in FY 2021.[50] In addition, the department reported that it planned to spend $5.8 billion on these programs between FY 2022 and FY 2023. Table 1 shows DOD's actual and planned expenditures during the 3-year period for the 25 major IT business programs.

Table 1: Actual and Planned Expenditures for the Department of Defense's (DOD) 25 Major IT Business Programs from Fiscal Year (FY) 2021 through FY 2023

Program	Dollars in millions			
	FY 2021 (actual)	FY 2022 (projected)	FY 2023 (requested)	3-year total
DOD Healthcare Management System Modernization	663	941	812	**2,416**
Navy Enterprise Resource Planning	381	232	248	**861**
Global Combat Support System-Army	293	218	131	**642**
Defense Enterprise Accounting and Management System-Increment 1	119	143	143	**405**
Distribution Standard System	104	138	158	**400**
General Fund Enterprise Business System	148	137	112	**397**
Enterprise Business System	80	139	126	**345**
Navy Maritime Maintenance Enterprise Solution	110	110	114	**334**
Maintenance Repair and Overhaul initiative	241	43	43	**327**

[49]In our 2022 DOD IT Quick Look report (GAO-22-105330), we found that 19 of 25 major IT business programs had not fully reported data indicating progress they were making toward their operational performance goals and recommended that the DOD Chief Information Officer (CIO) ensure these programs report performance measures, as appropriate, in the department's submission to the Federal IT Dashboard.

[50]According to DOD's Federal IT Dashboard data, the department last updated the data it submitted to the Dashboard on November 18, 2022. GAO obtained the latest data on November 22, 2022 and, as of January 2023, the November 2022 data were the most current data publicly available on the Dashboard.

Program	Dollars in millions			
	FY 2021 (actual)	FY 2022 (projected)	FY 2023 (requested)	3-year total
Defense Agencies Initiative	87	104	107	**298**
Joint Operational Medicine Information Systems	84	88	112	**284**
Defense Enrollment Eligibility Reporting System	104	76	78	**258**
Real-Time Automated Personnel Identification System and Common Access Card	77	62	89	**228**
Global Combat Support System-Marine Corps / Logistics Chain Management	62	69	69	**200**
Military Health System Information Platform	48	55	95	**198**
Defense Medical Logistics-Enterprise Solution	58	73	58	**189**
Naval Tactical Command Support System	46	47	45	**138**
Navy Standard Integrated Personnel System	35	48	47	**129**
Standard Procurement System	42	32	47	**121**
Air Force Integrated Personnel and Pay System	32	40	47	**119**
Defense Travel System	30	43	39	**111**
Military Entrance Processing Command Integrated Resource System	45	42	24	**111**
Army Contract Writing System	33	49	11	**93**
Defense Civilian Personnel Data System	32	33	26	**91**
Navy Electronic Procurement System	30	27	27	**84**
Total	**2,985**	**2,987**	**2,807**	**8,779**

Notes: Numbers do not always add due to rounding.

The four largest major IT business programs—the DOD Healthcare Management System Modernization (DHMSM), Navy Enterprise Resource Planning (ERP), Global Combat Support System-Army (GCSS-A), and Defense Enterprise Accounting and Management System-Increment 1 (DEAMS)—accounted for $4.3 billion (49.3 percent) of the department's $8.8 billion in total planned spending on the full portfolio of 25 from FY 2021 through FY 2023.[51] Figure 3 shows DOD's planned spending on its four largest business programs during the 3-year period compared to the full portfolio of 25.

[51]Numbers do not add due to rounding.

Figure 3: The Department of Defense's (DOD) Planned Spending on Its Four Largest Major IT Business Programs Compared to the Full Portfolio of 25 from Fiscal Year (FY) 2021 through FY 2023
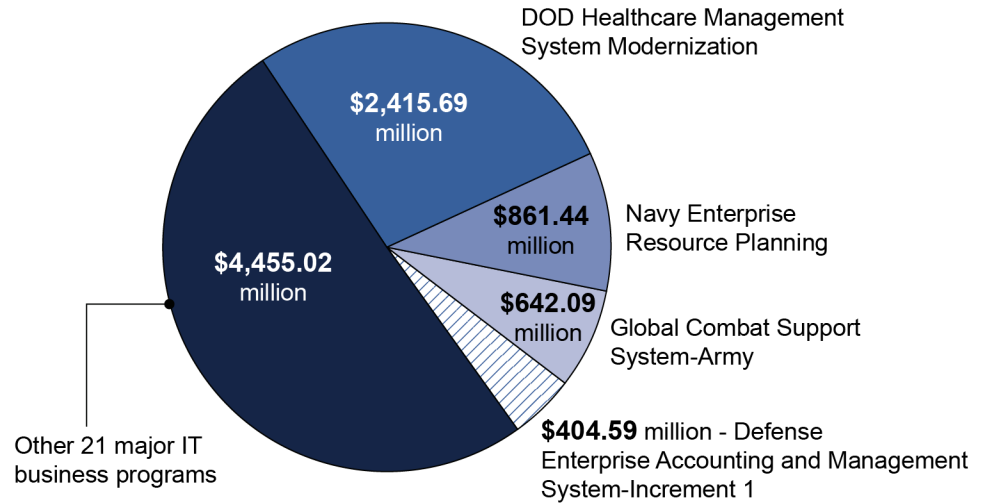
Source: GAO analysis of FY 2023 DOD data reported to the Federal IT Dashboard. | GAO-23-106117

Based on program officials' responses to our questionnaire, these four programs are collectively in more mature stages of their program life cycles. Navy ERP and GCSS-A officials reported that their programs are in sustainment.[52] DHMSM and DEAMS officials reported being in later stages of development and, more specifically, that their next program acquisition milestones were full deployment ATP and capability support ATP.

Sixteen Major IT Business Programs Reported Cost or Schedule Changes

As of February 2023, 16 of the 25 major IT business programs reported that they had experienced cost or schedule changes since January 1, 2021 and provided the extent of the changes. Figure 4 shows the programs that reported cost or schedule changes and the direction of the changes.

---

[52]Navy Enterprise Resource Planning (ERP) and Global Combat Support System-Army (GCSS-A) officials reported most recently achieving full deployment authority to proceed (ATP) and capability support ATP and currently being in sustainment. Full deployment ATP is a decision point where the milestone decision authority, with the support of the functional sponsor, considers the results of limited deployment(s) and operational testing and approves deployment to the entire user community. Capability support ATP is a decision point where the milestone decision authority accepts full deployment of the system and approves transition to capability support.

Figure 4: The Department of Defense's (DOD) Major IT Business Programs Reported Cost and Schedule Changes Since January 2021

Cost/schedule direction change

Cost	Schedule	Program
Cost increase	Schedule delay	Defense Civilian Personnel Data System
Cost increase	Schedule delay	Military Health System Information Platform
Cost increase	Schedule delay	Air Force Integrated Personnel and Pay System
Cost increase	Schedule delay	Military Entrance Processing Command Integrated Resource System
Cost increase	Schedule delay	Defense Agencies Initiative
Cost increase	Schedule delay	Defense Medical Logistics-Enterprise Solution
Cost increase	Schedule delay	Distribution Standard System
Cost increase	Schedule delay	Global Combat Support System-Army
Cost increase	Schedule delay	Standard Procurement System
Cost increase	Schedule delay	Maintenance Repair and Overhaul initiative
Cost increase	No schedule change	Naval Tactical Command Support System
Cost increase	No schedule change	Real-Time Automated Personnel Identification System and Common Access Card
Cost decrease	Schedule delay	Navy Enterprise Resource Planning
Cost decrease	Schedule delay	Navy Electronic Procurement System
Cost decrease	Schedule improvement	Army Contract Writing System
Cost decrease	No schedule change	Global Combat Support System-Marine Corps / Logistics Chain Management
No cost change	No schedule change	Defense Enrollment Eligibility Reporting System
No cost change	No schedule change	Navy Standard Integrated Personnel System
No cost change	No schedule change	Defense Enterprise Accounting and Management System-Increment 1
No cost change	No schedule change	DOD Healthcare Management System Modernization
No cost change	No schedule change	General Fund Enterprise Business System
No cost change	No schedule change	Navy Maritime Maintenance Enterprise Solution
No cost change	No schedule change	Joint Operational Medicine Information Systems
No cost change	No schedule change	Defense Travel System
No cost change	No schedule change	Enterprise Business System

Legend:
- Cost increase
- Cost decrease
- Schedule delay
- Schedule improvement
- No cost change
- No schedule change

Source: GAO analysis of DOD program questionnaire responses, as of February 2023. | GAO-23-106117

Officials for 16 programs reported cost changes, including 12 that reported cost increases. Eleven of these programs provided the specific dollar values associated with the increases, which ranged from $43

thousand to $194 million (a median of $4.6 million).[53] The other four programs reported cost decreases, including three that provided the specific dollar values associated with the decreases, which ranged from $18.1 million to $80 million.[54]

Thirteen programs reported schedule changes, including 12 that reported delays. Eleven of these programs provided the amount of time associated with the delays, which ranged from 3 months to 33 months (a median of 24 months).[55] The remaining program reported expecting a shortened schedule of 18 to 24 months.[56]

Officials for two of the largest four programs mentioned earlier, Navy ERP and GCSS-A, each reported changes to their planned costs and schedules since January 1, 2021. Regarding these programs:

- Navy ERP officials reported a 24-month schedule delay and a reduction in overall users, in part due to the delay, as well as an associated cost decrease. Program officials could not quantify the specific cost decrease associated with the delay but reported a total decrease of $1.04 billion for the program from FY 2023 to FY 2032.[57] Officials attributed the changes to significant volatility in the program's requirements and unplanned changes to technical strategies and contract awards. In addition, several migration efforts were postponed to 2024 and beyond due to lack of funding in 2022.

- GCSS-A officials reported a cost increase of $37 million and an associated schedule delay of a yet-to-be-determined amount of

---

[53]One program reported a cost increase, but could not quantify the amount associated with the increase.

[54]One of the programs reported a cost decrease of $80 million; however, this was due to the program terminating a contract and changing acquisition strategies. Another program reported a cost decrease; however, it was as a result of a reduction in overall users, in part due to a schedule delay, and the program could not quantify the decrease associated with the delay.

[55]One program that reported a schedule delay did not provide information quantifying the delay.

[56]One program reported expecting a shortened schedule; however, the program's estimate was based on the time it would have taken to continue the program's original path and product with a terminated vendor to achieve a deployable product and subsequent deliveries of required capability would have slipped comparatively.

[57]Navy ERP officials stated that the cost decrease associated with the 24 month schedule delay was not directly traceable in the program's cost estimate.

time.[58] Program officials attributed the changes to a contractor's inability to complete migration activities as required, increasing cloud costs. This led to the program terminating the contract in October 2022 and working to re-plan the work with new supporting contractors.

Seven Programs Rebaselined or Expect to Rebaseline

Officials for four of the 16 major IT business programs that reported cost or schedule changes reported rebaselining as a result of the changes. In addition, officials for three of the 16 programs indicated that they expect to rebaseline. Repeated rebaselines may indicate that programs are not appropriately managing cost, schedule, or performance expectations or that they are experiencing other issues.[59] For example, repeated rebaselines might indicate other challenges, such as unexpected technical complexity or issues with program contractors. Specifically, the four programs that rebaselined reported the following:

- **Defense Agencies Initiative (DAI).** A DAI official reported that the changes in the program's baseline were driven by the addition of new client organizations and a change in the program's hosting solution. Specifically, the OSD (Comptroller) directed the extension and restructuring of DAI's deployment timeline, including the addition of the Naval Special Warfare Command, a shift back for the Defense Information Systems Agency Defense Working Capital Fund, and the migration of DAI to commercial cloud hosting. These changes increased the program's cost by $27 million and extended the program's schedule by 24 months.

- **Distributed Standard System (DSS).** A DSS program official reported rebaselining to accommodate a bid protest and the impacts of COVID-19 restrictions. The rebaseline moved DSS's achievement of limited deployment to the third quarter of FY 2022 and expected achievement of full deployment to the first quarter of FY 2026.[60]

---

[58]GCSS-A officials reported experiencing a schedule delay but were not able to quantify the amount of time associated with the delay due to efforts being halted and the program working to re-plan the work.

[59]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.

[60]A limited deployment is any deployment before the full deployment ATP that provides a set of functionality to a set of users of the business system. The functional sponsor and program manager recommend the functionality and number of users. Full deployment is the delivery of full functionality to all planned users of the business system in accordance with the full deployment ATP.

These changes increased the program's cost by a yet-to-be-determined amount and delayed its schedule by 8 months.[61]

- **Maintenance Repair and Overhaul Initiative (MROI).** An MROI program official reported rebaselining due to the expansion of the initiative's scope. Specifically, the Air Force expanded implementation of MROI to additional maintenance organizations (i.e., aircraft, software, and maintenance) to support standard processes and allow the Air Force to retire additional systems. Additionally, as part of integration associated with the expansion, the program identified capabilities requiring additional efforts, which increased workload and development capacity. The milestone decision authority approved the rebaseline in February 2022, which reflects a delay of MROI's full deployment date from April 2025 to July 2025. These changes increased the program's cost by $35.2 million and delayed its schedule by 3 months.

- **Military Health System Information Platform (MIP).** An MIP program official reported rebaselining due to the addition of several high priority COVID-19 related projects. The prioritization of these projects delayed other planned releases. These changes increased the program's cost by $10.4 million and delayed its schedule by 6 to 12 months.

In addition, the three programs that anticipated a rebaseline reported the following:

- **Air Force Integrated Personnel and Pay System (AFIPPS).** An AFIPPS official reported that the planned changes to the program's baseline were related to the extension of its deployment date. Specifically, developmental test and evaluation integration challenges, new requirements, and other issues and risks delayed the program's limited deployment date from June 2022 to January 2025. Additionally, the program official reported awaiting approval of a new release and test strategy. The cost changes are reflected in AFIPPS's July 2022 cost estimate. These changes are expected to increase the program's cost by $194.1 million and delay its schedule by 31 months.

- **Army Contract Writing System (ACWS).** An ACWS program official reported planning to rebaseline based on an April 2022 Army decision

---

[61]Distributed Standard System officials reported a cost increase but could not quantify the amount as they are competing a follow-on contract to complete the work that was not completed under the current contract. They stated that they would not be able to quantity the cost increase until the new contract is awarded.

to change strategies after poor test and evaluation results. The new strategy is to use different and pre-existing contract writing solutions. In September 2022, the ACWS program office presented the new acquisition approach and estimated cost to support the new schedule. The program official reported that ACWS will transition from Waterfall development to an Agile approach for software delivery and establish a new baseline in the first quarter of FY 2023. The program's planned changes include achieving deployment with a minimum viable product in FY 2023, with additional deployments from FY 2024 to FY 2026 to provide capabilities, and full deployment slated for FY 2026.[62] These changes are expected to decrease the program's cost by $80 million and shorten its schedule by 18 to 24 months.[63]

- **Navy Electronic Procurement System (EPS).** A Navy EPS official reported that the planned changes to the program's baseline were related to greater technical complexity in development than anticipated. The Navy EPS contract was originally awarded in March 2019 and the program experienced two major baseline changes that delayed its deployment. The program management office issued a stop work order in June 2021 and allowed the contract to expire in October 2021. Navy EPS then transitioned to an Agile approach in the fourth quarter of FY 2021. The official reported that the program expects to rebaseline once its new contract is awarded. These changes are expected to decrease the program's cost by $18.09 million and delay its schedule by 32 months.[64]

Program officials provided a variety of reasons for the cost and schedule changes and rebaselines, including:

- **New and unplanned requirements.** Officials from 10 programs reported cost or schedule changes due to new or unplanned

---

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

[63]As previously mentioned, the cost decrease reported by Army Contract Writing System (ACWS) officials was due to the program terminating a vendor's contract and changing acquisition strategies. The original program would have had an increased cost based on what would have been another shift in schedule and required fixes and changes to the software. The program did not estimate the cost of continuing the original path and product with the terminated vendor. Similarly, the shortened schedule reflected in the program's estimate was based on the required time it would have taken to continue the original path and product to achieve a deployable product and subsequent deliveries of required capability would have slipped comparatively.

[64]Navy Electronic Procurement System officials reported that its cost estimate had decreased due to the program changing to an Agile approach that leverages pre-existing solutions.

requirements. This included changes related to new statutory requirements, audibility requirements, and requirements for sustainment of new capabilities.

- **Cloud migration and modernization developments.** Officials from 10 programs reported cost or schedule changes due to cloud migration and modernization effort developments. This included changes related to migration to commercial cloud hosting and migration of legacy applications, changes to support needed for cloud efforts and applications, and adjustments to support one program's modernization roadmap.

- **Workforce and contract issues.** Officials from nine programs reported cost or schedule changes due to workforce and contract issues. This included changes related to a delay in getting IT talent due to high industry demand and increased labor costs necessary to support existing applications and consolidation of legacy capabilities, issues related to the delivery of a solution by a contractor and a bid protest, and one program terminating its contract with a vendor and changing strategies due to poor test results.

- **Unanticipated technical complexities.** Officials from six programs reported cost or schedule changes due to greater technical complexities than anticipated. This included changes related to technical strategies, one program experiencing data conversion issues, and another program identifying capabilities requiring additional efforts related to integration.

- **Cybersecurity.** Officials from four programs reported cost or schedule changes due to cybersecurity issues. This included changes related to supporting DOD CIO's Zero Trust cybersecurity requirement, increasing cybersecurity control activities, and addressing an industry-wide cybersecurity issue impacting software used by one of the programs.[65]

- **COVID-19 impacts.** Officials from four programs reported cost and schedule changes due to impacts of COVID-19. This included changes related to COVID-19 restrictions, COVID-19 impacts shifting schedules, and the addition of several high priority COVID-19 related projects to one program's portfolio.

---

[65]Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

DOD's Major IT Programs and Infrastructure Investments Were 30 Percent of Total Planned Unclassified IT Spending

In addition to the 25 major IT business programs discussed above, DOD's FY 2023 Dashboard data included its 723 standard IT infrastructure investments (i.e., supporting hardware, software, communication, and information security services that a business system requires to operate). These two areas are included in the department's unclassified IT portfolio.[66] From FY 2021 through FY 2023, DOD budgeted about $31 billion for these standard IT infrastructure investments, including just over $17 billion on the 25 largest infrastructure investments. Specifically, based on our analysis of the Dashboard data, the department reported spending $9.1 billion on its standard IT infrastructure in FY 2021 and planning to spend $22.2 billion for these investments between FY 2022 and 2023. This included spending $4.6 billion on the 25 largest infrastructure investments in FY 2021 and planning to spend $12.4 billion on these 25 investments between FY 2022 and FY 2023. Table 2 shows DOD's actual and planned expenditures for the 25 largest standard IT infrastructure investments during the 3-year period.

Table 2: Actual and Planned Expenditures for the Department of Defense's (DOD) 25 Largest Standard IT Infrastructure Investments from Fiscal Year (FY) 2021 through FY 2023

Investment	Dollars in millions			
	FY 2021 (actual)	FY 2022 (projected)	FY 2023 (requested)	3-year total
Enterprise Information Technology as a Service-1	602	1,071	1,529	**3,202**
Non-Defense Information System Network Telecomm	726	740	757	**2,223**
Defense Logistics Agency Computing Infrastructure	499	546	641	**1,687**
Military Health System Desktop to Datacenter	427	501	479	**1,407**
Microsoft Enterprise License Agreement	147	319	313	**779**
Installation Information Infrastructure Modernization Program	304	220	207	**731**
Military Treatment Facility Operations	183	201	293	**677**
Other Payments to Defense Information Systems Agency-Navy	217	205	213	**635**
Cisco Joint Enterprise License Agreement	55	244	251	**550**
Base Communications Office	148	182	121	**452**
B-52 Defense Research and Engineering Network-Tinker	135	135	135	**406**
Information Technology Services Management-Command, Control, Communications, Computers, and Information Management	95	122	167	**384**
Navy Continuous Training Environment	128	140	104	**372**
Command Post Computing Environment-Project EJ4	113	135	121	**369**

[66]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year (FY) 2023 Budget Request* (May 2022).

Investment	Dollars in millions			
	FY 2021 (actual)	FY 2022 (projected)	FY 2023 (requested)	3-year total
CNP Chief Information Officers Support	86	97	147	**331**
Cloud Army	77	140	110	**328**
Defense Logistics Agency Communications Infrastructure	114	106	104	**324**
Microsoft Joint Enterprise License Agreement	30	134	145	**308**
DOD Air Force 365	63	125	111	**300**
Solution Delivery Division Virtual Hosting	81	111	97	**289**
Nett Warrior (Ground Soldier System)	137	150	0	**288**
Proponent / Mission Information Technology-Military Construction Army / Physical Relocation	0	177	83	**260**
Command Post Integrated Infrastructure	67	100	90	**257**
DOD Chief Information Officer Programs	85	86	83	**253**
Naval Computer and Telecommunications Area Master Station / Naval Computer and Telecommunication Station Pacific Mission Ops	96	74	72	**243**
Total	**4,615**	**6,063**	**6,374**	**17,053**

Source: GAO analysis of FY 2023 DOD data reported to the Federal IT Dashboard. | GAO-23-106117

Note: Numbers do not always add due to rounding.

Further, DOD's 25 major IT business programs and 723 standard IT infrastructure investments accounted for 30 percent in total planned spending on its unclassified IT portfolio. Specifically, the department's major IT business programs accounted for $8.8 billion (6.7 percent), and its standard IT infrastructure accounted for $31.2 billion (23.7 percent) of $131.7 billion in total planned spending on the department's unclassified IT portfolio from FY 2021 through FY 2023. We have previously reported on DOD's IT portfolio management, and the department has planned improvements for how it manages its IT investments, which are discussed later in the report.[67] Figure 5 shows DOD's planned spending on its major IT business programs and standard IT infrastructure investments during the 3-year period compared to its total unclassified IT portfolio.

[67]GAO-22-105330.

Figure 5: The Department of Defense's Planned Spending on Its Major IT Programs and IT Infrastructure Compared to Its Unclassified IT Portfolio from Fiscal Year (FY) 2021 through FY 2023

All other unclassified IT portfolio investments

$91.7 billion

25 major IT business programs

$8.8 billion

$31.2 billion

723 standard IT infrastructure investments
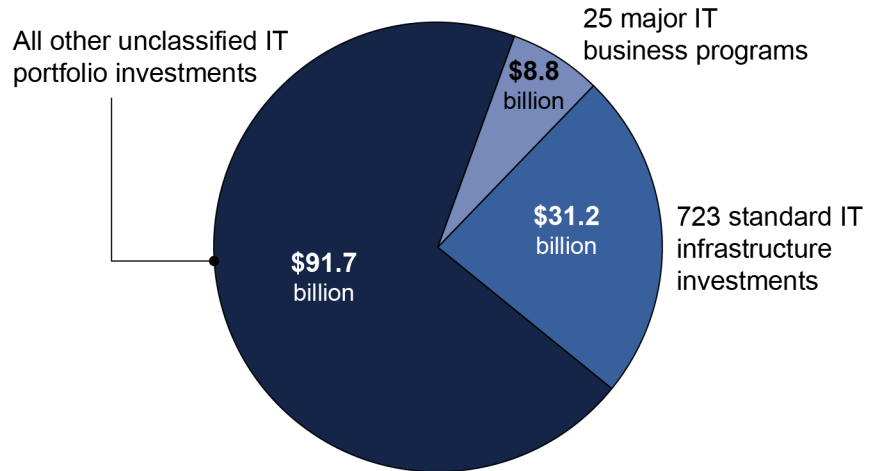
Source: GAO analysis of FY 2023 Department of Defense budget data. | GAO 23-106117

Not All Programs Fully Identified and Reported Required Performance Metrics Data

OMB requires IT programs to submit current information on program operational performance to the Federal IT Dashboard. According to OMB's capital planning guidance, programs must identify and report on a minimum of five operational performance metrics consistent with the following four categories:[68]

- **Customer satisfaction.** These metrics are intended to measure an investment's ability to deliver its goods or services. Programs must report a minimum of one metric under this category.

- **Strategic and business results.** These metrics are intended to measure an investment's effectiveness or its contribution to the organization's achievement of strategic goals, fulfillment of its mission, and meeting service level agreements with its customers. Programs must report a minimum of three metrics under this category.

[68]Office of Management and Budget, *FY 2022 IT Budget—Capital Planning Guidance* (Washington, D.C.: Nov. 16, 2020). OMB's FY 2022 capital planning guidance was the most current guidance for reporting performance data at the time of DOD's FY 2023 submission to the Dashboard.

Additionally, at least one metric must contribute to a strategic objective[69] or agency priority goal.[70]

- **Financial performance.** These metrics are intended to compare an investment's current performance with a pre-established cost baseline. The metric also supports periodic reviews for reasonableness compared to benchmarks or similar investments. Programs are not required to report a metric under this category.

- **Innovation.** These metrics are intended to measure an investment's means of maintaining or improving performance in terms of customer satisfaction, strategic and business results, and financial performance. Programs are not required to report a metric under this category.

As of January 2023, 22 of the 25 programs identified at least the minimum required number of operational performance metrics in each of the required categories and, in total, reported 141 operational performance metrics (an average of 5.6 metrics per program) consistent with OMB's guidance.[71] However, the other three programs did not identify the minimum required number of operational performance metrics. This included ACWS, which identified four of the five required metrics, and Joint Operational Medicine Information Systems and MROI, which did not identify any metrics data. These shortfalls and their impact on progress reporting are discussed below.

Programs Reported Mixed Progress on Operational Performance Metrics with Eight Not Fully Reporting Progress on Metrics

OMB's guidance further calls for programs to use the performance metrics they have identified to track progress toward achieving operational performance goals. Additionally, OMB's guidance states program submissions must include operational performance targets for the current fiscal year and a measurement condition.[72]

---

[69]Strategic objectives are to reflect the outcome or management impact the agency is trying to achieve to make progress on its mission and provide services to customers.

[70]Agency priority goals are to reflect near-term results or achievements that leadership wants to accomplish in support of broader strategic objectives or goals in the agency's strategic plan.

[71]DOD sent us the performance data in August 2022 and we confirmed that it was still current as of January 2023.

[72]The measurement condition is to indicate whether a desired result would be "over target," indicating that the trend should maintain or increase, or "under target," indicating that the trend should maintain or decrease. For example, if a program reported an operational performance metric with a target of 90 percent and a metric condition of "under target," any value less than or equal to 90 percent would mean the program had achieved that operational performance metric.

Of the 25 major IT business programs, eight programs did not fully report on the extent to which they achieved their operational performance targets.[73] Specifically, six programs reported incomplete data, and two did not report any data.[74] Of the 17 programs that fully reported the extent to which they achieved their operational performance metrics, eight programs reported achieving all targets and nine programs reported achieving some of their targets. We previously determined that major IT business programs had not fully reported data indicating progress they were making toward their operational performance goals. As a result, we recommended that the DOD CIO ensure these programs report performance measures, as appropriate, in the department's submission to the Federal IT Dashboard. Figure 6 shows a breakdown of programs' reported operational performance metrics and their progress toward achieving their targets.

---

[73]GAO-22-105330.

[74]Although ACWS reported progress against all of their metrics, we counted the program as reporting incomplete data because they had not identified the minimum required amount of metrics.

Figure 6: Department of Defense (DOD) Major IT Business Programs' Reported Performance Measurements as of January 2023

Number of reported metrics

Minimum number of metrics programs are to report

Program	Value
Navy Enterprise Resource Planning	10
Military Entrance Processing Integrated Resource System	8
Navy Standard Integrated Personnel System	6
Defense Agencies Initiative	5
DOD Healthcare Management System Modernization	5
Defense Medical Logistics-Enterprise Solution	5
Distribution Standard System	5
Enterprise Business System	5
Real-Time Automated Personnel Identification System and Common Access Card	4, 1
Air Force Integrated Personnel and Pay System	8
Navy Electronic Procurement System	6
Defense Enterprise Accounting and Management System-Increment 1	5
Defense Civilian Personnel Data System	9, 1, 5
Defense Enrollment Eligibility Reporting System	4, 3
Global Combat Support System-Army	4, 1
Military Health System Information Platform	3, 4
Defense Travel System	3, 2
Global Combat Support System-Marine Corps/Logistics Chain Management	3, 2
Navy Tactical Command Support System	3, 2
Standard Procurements System	3, 2
Navy Maritime Maintenance Enterprise Solution	2, 3
General Fund Enterprise Business System	1, 4
Army Contract Writing System	4
Joint Operational Medicine Information Systems	0
Maintenance Repair and Overhaul Initiative	0

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Legend:
- Reported progress and achieved target
- Reported progress and did not achieve target
- Did not report progress

Source: GAO analysis of DOD's fiscal year 2023 Federal IT Dashboard data.

As noted above, three of DOD's 25 major IT business programs did not identify operational performance metrics consistent with OMB guidance, including two programs that did not identify any metrics data. DOD CIO officials acknowledged that the programs should be identifying and reporting the required performance metrics. The officials stated that DOD CIO put checks in place that should improve program reporting and make sure the data are up to date with programs' operational performance metrics data, but that some programs still had incomplete reporting because those checks had been made incrementally and had only been partially implemented. The officials stated that they expect the checks to be fully implemented before the department's next Dashboard submission for FY 2024 in June 2023. However, as of March 2023, DOD was unable to confirm that the checks were currently in place to ensure that all programs identify and report complete operational performance metrics for their FY 2024 submission.

By not ensuring that programs identify and report these required metrics, the department limits program accountability and its own ability to effectively oversee program performance. Additionally, DOD limits the availability of information needed to understand how programs are performing for stakeholders, federal agencies, and the public and impedes the ability of Congress to conduct effective oversight.

Major IT Programs Reported Using Software Development and Cybersecurity Practices, but Not All Had Required Plans and Strategies

As of February 2023, officials for all eight major IT business programs that we identified as actively developing software reported using approaches and practices that may help limit risks to cost and schedule outcomes.[75] For example, all eight programs reported using iterative development approaches, as recommended by the Defense Science Board, including six programs that reported using Agile. In addition, seven programs reported delivering a minimum viable product. Five of the eight programs also reported delivering software functionality every 6 months or less, as called for in OMB guidance.[76]

Further, recognizing the importance of user involvement throughout the software development process, officials for all eight programs actively

[75]For the purposes of this assessment, we considered programs to be actively developing software if program officials reported they were actively developing new software functionality or if they had not yet reached full deployment ATP.

[76]OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (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.

developing software reported collecting some form of user feedback during requirements development and refinement. However, officials for nearly half of the full set of 25 major IT business programs that were in various stages did not demonstrate having approved plans for user training and deployment as required by DOD.[77] Additionally, while programs reported conducting cybersecurity assessments and tests, six of the 25 programs did not demonstrate having an approved cybersecurity strategy as required.[78]

Program officials reported facing a variety of key challenges related to software development and cybersecurity, including budget constraints, changing customer requirements, and updated cybersecurity requirements.

Major IT Business Programs Actively Developing Software Reported Using Recommended Software Development Approaches and Practices

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).[79] An iterative development approach is a way of breaking down the development of large applications into smaller pieces or increments. The board assessed that the iterative approach to software development is applicable to DOD and should be adopted as quickly as possible. Table 3 describes the recommended iterative software development approaches.

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

Development 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	This approach combines "development" and "operations", emphasizing communication, collaboration, and continuous integration between both software developers and users.
DevSecOps	This model combines "development," "security," and "operations," and emphasizes communication, collaboration, and continuous integration between software developers and users.

[77]Department of Defense, *Business Systems Requirements and Acquisition*, DOD Instruction 5000.75, Incorporating Change 2, Jan. 24, 2020 (Washington, D.C.: Feb. 2, 2017)

[78]Department of Defense, *Test and Evaluation*, DOD Instruction 5000.89 (Nov. 19, 2020).

[79]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.

Development approach	Description
Other incremental	This includes incremental approaches other than Agile, DevOps, or DevSecOps. Incremental approaches set high-level requirements early in the effort and functionality is delivered in stages or increments. Multiple increments each deliver part of the overall required program capability. Several builds and deployments are typically necessary to satisfy approved requirements.

Source: GAO analysis of the Defense Science Board's February 2018 report on design and acquisition of software for defense systems. | GAO-23-106117

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 is in contrast 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.[80]

As of February 2023, officials for all eight major IT business programs that we identified as actively developing software reported using at least one of, or a mix of, the recommended software development approaches that support continuous, iterative development and could result in cost or schedule benefits. For example, six of these programs reported using Agile as an approach. Officials for two of the eight programs reported using Waterfall; however, they reported using a mixed approach that also included an iterative development approach.

All Eight Programs Reported Using a Variety of Iterative Development Practices

The Defense Science Board also recommended that DOD implement certain practices that support continuous, iterative software development. Officials for each of the eight programs reported using a variety of the recommended iterative development practices. For example, seven of the eight 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). Additionally, six of the eight programs reported providing software documentation at each production milestone, which can help program staff more effectively assess progress and inform decisions to move forward in the development process. Table

---

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

4 describes the iterative development practices that programs reported using.

Table 4: Department of Defense Major IT Business Programs Actively Developing Software Reported Using Iterative Development Practices

Development practice	Description	Number of programs that reported using each practice
Delivery of minimum viable product, followed by successive next viable product[a]	A development technique in which a new product is delivered with sufficient features to satisfy early adopters.	7 of 8
Software documentation provided at each production milestone	Written text or illustration that accompanies computer software or is embedded in the source code.	6 of 8
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.	5 of 8
Use of a software factory for development	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 tempo.	1 of 8
Establishing the creation of a software factory as a key evaluation criterion in the source selection process	Development of a software factory as a factor in evaluating proposals for a potential government contractor.	1 of 8

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

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

Five of the Eight Programs in Active Development 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. OMB defines incremental development as planned and actual delivery of new or modified technical functionality to users at least every 6 months.[81] 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

---

[81]OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (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.

opportunities to obtain information from users and may face challenges adjusting requirements to meet customer needs.

Officials for five of the eight programs actively developing software reported delivering software functionality every 6 months or less, as called for in OMB's guidance. The remaining three programs reported not delivering functionality every 6 months or less. Officials for two of the three programs reported that the average length of time between software releases was greater than 6 months. The third program reported that they did not know the average number of months between releases because the program is still refining its new strategy.

Major IT Programs Reported Involving Users in Development, but Many Lacked Required Training and Deployment Plans

DOD instruction 5000.75 calls for involving users throughout the entire system life cycle, including from development through deployments and sustainment. An important part of modern software development is releasing functionality and enhancements to users incrementally and involving users early and often throughout the process to obtain feedback. This includes collecting user feedback during development, involving users in testing, and surveying users about customer experience. This also includes involving users in training and deployment activities and planning for these activities. These types of activities enable DOD to acquire and deliver business systems that work as intended, meet users' needs and increase adoption.

Programs Reported Collecting User Feedback during Requirements Development, Involving Users in Testing, and Surveying Users about Customer Experience

Officials for all eight programs actively developing software reported collecting some form of user feedback during requirements development and refinement.[82] Six of the programs reported collecting the feedback on a daily, weekly, biweekly, monthly, or quarterly basis, or with a mix of these frequencies. The remaining two programs reported other frequencies for collecting this type of feedback, such as during the annual development release process, during biweekly working group meetings, and between meetings via email.

Additionally, officials for 23 of the 25 major IT business programs reported involving users in testing.[83] Seventeen of the 23 programs reported involving users in testing on a daily, weekly, biweekly, monthly, or

---

[82]Requirements development is an activity more likely associated with programs in active development, so we focused on the eight programs actively developing software for this activity.

[83]Testing is an activity that can be associated with programs in various stages of development so we looked at all 25 programs for this activity.

quarterly basis, or with a mix of these frequencies. The remaining six programs reported other frequencies for doing so, such as during incremental release efforts and during the initial operational test phase. Two of the 25 programs responded that this practice was either not applicable to their program or that they did not know.

Officials for 20 of the 25 programs reported surveying users about customer experience.[84] Eight of the 20 programs reported surveying users on a daily, weekly, biweekly, monthly, or quarterly basis, or with a mix of these frequencies. The remaining twelve programs reported other frequencies for doing so, such as at least annually via surveys, after conducting user training, and within their call center system on an ad-hoc basis. Five of the 25 programs responded that they had not yet conducted this practice, that it was not applicable to their program, or that they did not know.[85] Table 5 describes the types and frequencies of user feedback reported by the programs.

Table 5: Department of Defense Major IT Business Programs in Various Stages of Development Reported Frequencies of Conducting Activities to Involve Users

User involvement activity	Frequency	Number of programs that reported conducting each activity and frequency[a]
Collecting user feedback during requirements development and refinement		8 of 8
	Daily, weekly, or biweekly	4 of 8
	Monthly or quarterly	2 of 8
	Other	2[b] of 8
	Never, N/A, or don't know	0 of 8
Involving users in program testing		23 of 25
	Daily, weekly, or biweekly	12 of 25
	Monthly or quarterly	5 of 25
	Other	6[c] of 25
	Never, N/A, or don't know	2 of 25
Surveying users about customer experience		20 of 25

[84]Surveying customers is an activity that can be associated with programs in various stages of development so we looked at all 25 programs for this activity.

[85]Officials for one program reported that the program had not surveyed customers because the system was not yet operational.

User involvement activity	Frequency	Number of programs that reported conducting each activity and frequency[a]
	Daily, weekly, or biweekly	5 of 25
	Monthly or quarterly	3 of 25
	Other	12[d] of 25
	Never, N/A, or don't know	5 of 25

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

[a]Some programs reported more than one type of frequency (e.g. a mix of daily, weekly, biweekly, monthly, quarterly, or other).

[b]Two programs reported other frequencies related to collecting user feedback during requirements development and refinement. For example, one program reported that they collect feedback during the annual development release process. The other program reported that they collected user feedback during biweekly working group meetings and between meetings via email.

[c]Six programs reported other frequencies related to involving users in program testing. For example, programs reported involving users in testing during incremental release efforts and during the initial operational test phase.

[d]Twelve programs reported other frequencies related to surveying users about customer experience. For example, programs reported surveying users about customer service at least annually via surveys, after conducting user training, and within their call center system on an ad-hoc basis.

Eleven Programs Did Not Have Required User Training and Deployment Plans

A capability implementation plan outlines how a program implements new system functionality and enhancements. The plan is a compilation of the content the program office needs to prepare for and manage the delivery of the capability. The plan also describes required actions that must occur before the business system can be acquired. Instruction 5000.75 requires programs to develop capability implementation plans that address conducting user training and deployment in support of the business system.[86] These training- and deployment-related activities are intended to achieve required organizational changes and delivery of supporting business systems that meet their users' needs and are widely adopted by users.

As of February 2023, officials for 14 of the 25 major IT business programs demonstrated that they had an approved capability implementation plan or other program plans that address user training and deployment.[87] However, the remaining 11 programs did not demonstrate having such plans. The 11 programs reported various reasons for not having the plans. Specifically, two of the 11 programs reported that they are

[86]This instruction defines users as the end-user community of the business system and a deployment as either introducing a new release into the production environment or expanding the user base of existing functionality. Deployment includes training and business systems operations activities such as help desk support.

[87]User training and deployment planning can be associated with programs in various stages of development. As a result, we considered all 25 programs for this activity.

developing the plans or that plans are in the process of being approved and one program reported not yet having a timeframe for developing them. The other eight programs reported that their systems had entered a late stage of development, were nearing retirement, or predated the requirement. However, these type of user training and deployment activities can be important for systems in various stages.

Officials with DOD CIO and A&S acknowledged that programs should have plans that address user training and deployment and stated that they will follow up with the programs that did not have such plans to ensure they develop them, as appropriate. Nonetheless, without such plans, the department is at increased risk of programs not achieving required organizational changes and delivering business systems that do not meet their users' needs and are not widely adopted by users.

Programs Reported Conducting Cybersecurity Assessments and Tests, but Not All Had an Approved Strategy

DOD Instructions 5000.75[88] and 5000.90[89] require major IT program staff to conduct cybersecurity assessments. Assessments for potential cybersecurity vulnerabilities are included in programs' cybersecurity testing and assessment processes. These assessments include full system assessments, assessments during development testing, and tabletop exercises; however, program staff may also conduct other types of assessments.[90]

According to DOD's Test and Evaluation Guidebook, cybersecurity testing and evaluation is intended to identify and mitigate exploitable system vulnerabilities.[91] The guidebook notes that early discovery of system vulnerabilities can facilitate remediation and reduce the impact on program cost, schedule, and performance.

---

[88]Department of Defense, *Business System Requirements and Acquisition,* Instruction 5000.75 [incorporating change 2 (Jan. 24, 2020)] (Washington, D.C.: Feb. 2, 2017).

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

[90]Department of Defense, *Operation of the Defense Acquisition System,* Instruction 5000.02T change 9 (Washington D.C.: November 2020).

[91]Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1 (Washington, D.C., February 10, 2020).

Officials from 22 of the 25 major IT business programs reported conducting some form of cybersecurity assessment, while officials for the other three programs reported not conducting any assessments. Officials for two of the three programs reported that they had not yet conducted any assessments but that they have plans to do so. An official for the remaining program stated that the requirement did not apply to their program because it was not included in the program's approved risk management framework posture. Table 6 summarizes the cybersecurity assessments that the programs reported conducting.

Table 6: Department of Defense Major IT Business Programs Reported Conducting Cybersecurity Assessments

Cybersecurity assessment	Description	Number of programs that reported conducting each assessment
Reported conducting cybersecurity assessments		22[a] of 25
Full-system assessment	An assessment performed on a complete system to evaluate its compliance with specified requirements	19 of 25
Cooperative assessment	Assessments by independent assessors in which program office representatives, including developer support, are encouraged to observe and characterize vulnerabilities, potential exploits, and follow-on fixes that may be needed. These assessments may involve any number of cybersecurity test events, such as system and network scans, vulnerability validation, penetration tests, access control checks, physical inspection, personal interviews, and reviews of system architecture and components.	14 of 25
Table top exercise	An activity in which key personnel are gathered to discuss how they would respond to various simulated emergency or rapid response situations, often involving small collaborative teams that prepare briefings on potential threat scenarios. Based on those results, officials can create a path forward for addressing those scenarios, which could include administering additional testing and training, conducting follow-on analysis, or accepting the risk posed by the potential threat.	17 of 25
Component assessment	An assessment of individual hardware and software components or groups of related components.	13 of 25
Penetration test	An assessment methodology in which independent assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. A penetration test may or may not be conducted as part of a cooperative assessment.	14 of 25
Other		5[b] of 25

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

[a]One program reported no for all cybersecurity assessments types.

[b]Officials from five programs reported conducting other types of assessments including a source code cybersecurity vulnerabilities assessment, an ad hoc risk and security impact assessments, and privacy impact assessments.

Programs Reported Conducting Developmental and Operational Cybersecurity Testing	DOD Instruction 5000.89[92] requires that DOD major IT program staff complete both developmental and operational cybersecurity testing.[93] Developmental cybersecurity testing and evaluation is intended to identify cybersecurity vulnerabilities before program deployment to help remediate cybersecurity vulnerabilities and reduce the risk of a negative impact on cost, schedule, or performance. Cybersecurity operational testing evaluates operational programs for effectiveness, suitability, and survivability. However, program staff can perform other developmental and operational cybersecurity assessments.

Officials from 21 of the 25 programs reported conducting developmental cybersecurity testing, operational cybersecurity testing, or both. Specifically, 18 of the 21 programs reported conducting developmental testing and 17 of the 21 programs reported conducting operational testing. Officials for the four remaining programs reported conducting neither developmental nor operational testing. Programs may have conducted certain types of cybersecurity testing and not conducted other types due, in part, to being in different life cycle phases. For example, systems in an earlier life cycle phase may conduct developmental testing, but may not be mature enough to conduct operational testing. Table 7 summarizes the types of developmental and operational cybersecurity tests that the programs reported conducting.

Table 7: Department of Defense Major IT Business Programs Reported Conducting Developmental and Operational Cybersecurity Testing

Testing phase	Testing conducted	Description	Number of programs that reported conducting each test
Developmental testing, operational testing, or both			**21 of 25**
Developmental testing			**18[a] of 25**

[92]Department of Defense, *Test and Evaluation*, Instruction 5000.89 (Nov. 19, 2020).

[93]According to DOD's *Cybersecurity Testing and Evaluation Guidebook*, operational cybersecurity testing provides information that helps to resolve operational cybersecurity issues, identify vulnerabilities in a mission context, and describe operational effects of discovered vulnerabilities. Developmental testing identifies cybersecurity issues and vulnerabilities prior to early in system life cycle in order to facilitate the remediation and reduction of impact on cost, schedule and performance. Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1 (Washington, D.C., Feb. 10, 2020).

Testing phase	Testing conducted	Description	Number of programs that reported conducting each test
	Cooperative vulnerability and identification	A cybersecurity developmental test and evaluation activity that collects data needed to identify vulnerabilities and plan the means to mitigate or resolve them, including system scans, analysis, and architectural reviews.	10 of 25
	Adversarial assessment	An adversarial test during development that uses realistic threat exploitation techniques in representative operating environments.	6 of 25
	Other kind of testing		9[b] of 25
	No testing or N/A		8 of 25
Operational testing			**17[c] of 25**
	Cooperative vulnerability and identification	A cooperative vulnerability and penetration test that examines a system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities.	11 of 25
	Adversarial assessment	An operational adversarial test that assesses the ability of a system to support its mission while withstanding cyber threat activity representative of an actual adversary.	7 of 25
	Other kind of testing		6[d] of 25
	No testing or N/A		8 of 25

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

[a]Officials for some programs reported conducting multiple assessments for developmental testing.

[b]Officials for nine programs reported conducting other types of developmental assessments including tabletop exercises, code scans, peer review and security analysis, and developmental test penetration.

[c]Officials for some programs reported conducting multiple assessments for operational testing.

[d]Officials for six programs reported conducting other types of operational assessments including vulnerability scans and cyber readiness inspections.

Six Programs Did Not Have an Approved Cybersecurity Strategy

DOD Instruction 8500.01, Cybersecurity, and DOD Instruction 5000.89 require that DOD major IT program officials use approved cybersecurity strategies.[94] These strategies are 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.

As of February 2023, officials from 19 of the 25 major IT business programs demonstrated that they had an approved cybersecurity

[94]Department of Defense, *Cybersecurity*, Instruction 8500.01 (Washington, D.C.: Mar. 14, 2014; rev. Oct. 7, 2019), Department of Defense, *Test and Evaluation*, DOD Instruction 5000.89 (Nov. 19, 2020).

strategy.[95] However, the other six programs did not demonstrate having such strategies. Officials for five of the programs reported planning to develop an approved strategy, while the remaining program did not report having plans to do so. In our June 2022 report, we found that 10 of DOD's major IT business programs had not demonstrated having approved cybersecurity strategies and recommended that the DOD CIO ensure these programs develop strategies, as appropriate.[96] DOD officials concurred with our recommendation and, as of March 2023, stated that they were continuing to take actions to address the recommendation by following up with the programs that did not provide an approved strategy to ensure that they develop one.

Although DOD has shown improvement, until the department ensures that all of the programs develop approved cybersecurity strategies, it lacks assurance that programs are positioned to effectively manage cybersecurity risks and mitigate threats. As a result, DOD programs are at increased risk of adverse impacts on cost, schedule, and performance.

Programs Reported Key Challenges Associated with Software Development and Cybersecurity

As of February 2023, officials for major IT business programs included in our review reported facing a number of key challenges associated with software development and cybersecurity. For example:

- Officials for 13 of the 25 programs reported challenges related to budget constraints. For example, an official from one program stated that budget constraints were due to increases in customer and cybersecurity demands without accompanying increases in budget or staff to address aging hardware or software development.

- Program officials for nine programs reported challenges related to changing customer requirements. For example, an official from one program reported that capabilities were expanding without clearly defined requirements.

- Officials for nine programs reported challenges related to keeping up with the DOD's rapidly evolving cybersecurity requirements. For instance, an official from one program reported that changing cybersecurity requirements impacted development and sustainment resources.

- Officials for seven programs reported challenges related to software development and commercial off-the-shelf software issues. For

---

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

[96]GAO-22-105330.

example, an official from one program reported that the program pursued a commercial off-the-shelf solution for about two years, ultimately pivoting to a different solution as the initial solution failed user acceptance testing.

- Officials for six programs reported challenges related to leadership and staff turnover issues. For example, an official from one program stated that leadership and staff turnover was a challenge due to knowledge being lost as people retire.

Additionally, officials for five programs reported other challenges including one program official who stated that an acquisition framework that they were using did not provide instructions on how to manage a portfolio of programs. An official for another program reported having to address contract delays.

For additional information on DOD's 25 major IT business programs, including information related to their reported software development approaches and practices, see appendix II, which contains detailed summaries for each program.

DOD Continues Actions to Implement Legislative and Policy Changes and Improve How It Manages IT Investments

As noted earlier in this report, the NDAA for FY 2021 eliminated the DOD CMO position, which previously had broad oversight responsibilities for DOD business systems. In September 2021, the Deputy Secretary of Defense directed an extensive realignment of the responsibilities previously assigned to the CMO.[97] These changes included the reassignment of the following responsibilities:

- Establishing a Defense Business Council (DBC), previously chaired by the CMO and the DOD CIO, to provide advice to the Secretary of Defense on (1) developing the DOD business enterprise architecture, (2) reengineering department business processes, (3) developing and deploying defense business systems, and (4) developing requirements for defense business systems. This council is to be tri-chaired by the Director of Administration and Management, the Undersecretary of Defense (Comptroller) (USD[C]), and the DOD CIO.

---

[97]Department of Defense, *Disestablishment of the Chief Management Officer, Realignment of Functions and Responsibilities, and Related Issues* (Washington, D.C.: Sept. 1, 2021).

- Developing and maintaining the DOD business enterprise architecture to guide the development of integrated department business processes to the DOD CIO.

- Issuing supporting guidance (along with the Under Secretary of Defense for Acquisition and Sustainment, DOD CIO, and military department CMOs) within respective areas of responsibility for the coordination of, and decision making for, the planning, programming, and control of investments in covered defense business systems to the USD(C) and DOD CIO.

Subsequent to this reassignment of responsibilities, DOD finalized the updated DBC charter in January 2022. In addition, DOD officials stated that the department has identified a permanent DBC subcommittee to guide defense business systems and has finalized the charter for this subcommittee.

In addition, the NDAA for FY 2023, which the President signed in December 2022, included provisions to formally shift certain roles and responsibilities from the former CMO position to other DOD entities. For example, according to the new statute, the DOD CIO is to develop and maintain the business enterprise architecture, chair the DBC, and serve as the approval official for priority defense business systems.

| DOD Officials Described FY 2023 Efforts to Implement Legislative and Policy Changes Affecting IT Acquisitions | Officials from DOD's Offices of the Director of Administration and Management and CIO described continued efforts underway in the department to implement changes associated with its defense business systems investment management guidance and the DOD business enterprise architecture. Specifically, those efforts include the following: |

Defense Business Systems Investment Management Guidance. In December 2022, DOD reported that DOD CIO plans to issue a revised investment management guide that will incorporate the results of a portfolio manager survey to improve the department's business process re-engineering efforts by May 31, 2023. In addition, in March 2023, we reported on our evaluation of the department's existing guidance on how business systems are to address statutory requirements.[98] Our evaluation showed that current DOD guidance does not fully address initial investment approval or describe expectations for documenting or substantiating compliance with statutory requirements for annual certifications. Specifically, the guidance discusses the requirements but

---

[98]Our March 2023 report, GAO-23-104539, focuses on DOD financial management systems and discusses guidance for business systems.

does not describe how systems are to demonstrate or how decision makers are to substantiate system compliance. Subsequently, officials from the office of DOD CIO stated that they recognize the guidance can be improved and noted that they would address the identified gaps.

Business Enterprise Architecture. In December 2022, DOD CIO indicated that the department plans to publish a business enterprise architecture modernization strategy and a new business enterprise architecture by June 30, 2023.

In addition, on March 2023, officials from DOD CIO indicated that they are in the process of aligning strategies to improve how the department manages its IT investments. The officials added that they are making progress, but the strategies have yet to be finalized. 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 (mandated under the FY 2021 NDAA).[99] Additionally, we will monitor DOD's efforts associated with the business systems modernization and approach to business transformation high-risk areas.

Conclusions

DOD relies heavily on the use of IT to protect our nation. Since 1995, we have identified DOD's efforts to modernize its business systems, including its major IT programs, as high risk, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments.

Regarding DOD's major IT business programs, more than half of the programs fully reported performance data and reported mixed progress on achieving their operational performance goals. However, the remaining programs did not fully identify and report required performance metrics data, including a few that did not identify the minimum required number of metrics. By not ensuring that programs identify and report required metrics to the Federal IT Dashboard, DOD limits program accountability and its own ability to effectively oversee performance. Those data also help stakeholders, federal agencies, and the public understand how programs are performing and helps Congress conduct external oversight. As a result, DOD limits the availability of this

---

[99]Pub. L. No. 116-283, § 911, 134 Stat. 3388, 3801-3802 (Jan. 1, 2021) also directed a GAO review of DOD's framework for these reforms. That review is ongoing.

information and this may impede the ability of Congress to conduct effective oversight.

Officials for major IT business programs reported using software development approaches and practices that can limit risks to cost and schedule, and the department is taking steps to address reported challenges. These efforts have the potential to improve how DOD acquires and manages its IT systems. In addition, program officials reported involving users throughout the development process, including through collecting feedback during development, involving users in testing, and surveying about customer experience. However, almost half of the major IT programs did not have required plans for conducting user training and deployment. As a result, the department risks programs not achieving required organizational changes and delivering business systems that do not meet their users' needs and are not widely adopted by users.

Further, although officials for major IT business programs reported conducting a variety of cybersecurity assessments and tests, not all programs had approved cybersecurity strategies as required. We have previously made a recommendation to DOD to address these issues.

As DOD continues to implement its numerous reform efforts, it has multiple opportunities to improve the performance of its IT systems, implement efficient and tailored oversight and management processes, and reduce risk across its systems.

Recommendations for Executive Action

We are making the following two recommendations to the Department of Defense:

The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs identify at least the minimum required amount of operational performance metrics, as appropriate, in the department's submission to the Federal IT Dashboard. (Recommendation 1)

The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs develop capability implementation plans or other program plans that address conducting user training and deployment, as appropriate. (Recommendation 2)
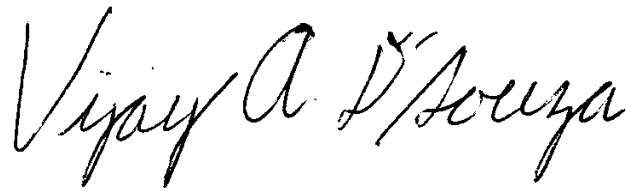
Agency Comments and Our Evaluation

DOD provided written comments on a draft of this report, which are reproduced in Appendix III. In its comments, the department agreed with the overall content of the report, but it did not concur with our recommendations. Regarding our first recommendation to ensure the department identified at least the minimum required amount of operational performance metrics, the department stated that, as of April 2023, it had implemented an audit check as part of its budget collection process to ensure major IT investments report operational metrics in accordance with OMB requirements. However, DOD did not provide evidence that the three programs that did not previously identify the minimum required metrics have done so as part of their next submission to the Federal IT Dashboard for FY 2024. Until DOD demonstrates that its major IT business programs have identified at least the minimum required amount of operational performance metrics on the Federal IT Dashboard, it limits the availability of information needed to understand how programs are performing. As a result, the department will be challenged to effectively oversee program performance and to ensure program accountability.

Regarding our second recommendation to ensure that major IT business programs develop capability implementation plans, the department stated that the requirement to develop capability implementation plans is codified within DOD 5000.75. It further agreed that, as a defense business system progresses through the system lifecycle, the department is required to mature its user training and deployment plans at each decision point. DOD added that the milestone decision authority has the ability to review the user training and deployment plans prior to progressing into the capability support phase. However, we identified 11 programs that did not have capability implementation plans that address conducting user training and deployment, and the department did not provide evidence that such plans had been developed. Until DOD demonstrates that it has developed plans that address conducting user training and deployment for these programs, it risks programs not achieving required organizational changes. Furthermore, the department risks delivering business systems that do not meet its users' needs and are not widely adopted by users. As a result, we continue to believe that both of our recommendations are warranted. We will follow-up with DOD for an update on actions taken in response to these recommendations.

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 have any questions about this report, please contact me at (202) 512-7650 or 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.

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

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

The Honorable Jon Tester
Chair
The Honorable Susan Collins
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
Chair
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 how DOD's portfolio of major IT business programs has performed, (2) determine the extent to which DOD has implemented key software development and cybersecurity practices for selected programs, and (3) describe what actions DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, we initially considered the 28 business programs that DOD reported as major IT investments as part of its FY 2023 submission to the Federal IT Dashboard at the start of our review in June 2022. We then excluded three of these programs based on the department no longer considering them major IT investments.[1] We determined the number of major IT business programs to be the remaining 25.

To determine how much DOD reported spending on the 25 major IT business programs in FY 2021 and planned to spend on the programs between FY 2022 and FY 2023, we analyzed the department's FY 2023 Dashboard data.[2] Based on these data, we calculated the total planned expenditures for the programs during the 3-year period. In addition, we compared DOD's planned spending on the four largest business programs to its total planned spending on the full portfolio of 25 for FY 2021 through FY 2023.

We also collected and analyzed program office responses to a GAO questionnaire we developed and administered to all 25 major IT business programs in October 2022. Programs provided their responses between October 2022 and December 2022, and we followed up with programs about their responses through February 2023. The questionnaire included questions about whether programs had experienced cost or schedule changes since January 1, 2021 and whether programs had rebaselined or

---

[1]The department planned to retire one of the programs in FY 2022, and the Dashboard reflected $0 in planned FY 2022 and FY 2023 expenditures; a portion of one of the program's capabilities were transitioned to a new program; and the remaining program's capabilities were split into three separate programs.

[2]According to DOD's Federal IT Dashboard data, the department last updated the data on November 18, 2022. GAO obtained DOD's Dashboard data on November 22, 2022 and, as of March 2023, the November 2022 data were the most current data publicly available on the Dashboard.

expect to rebaseline as a result of the changes.[3] Additionally, we
collected and analyzed supporting documentation, including key program
documents, reports, and artifacts pertaining to each program's life cycle
cost, schedule estimates, and baselines (e.g., acquisition program
baseline reports).

In addition to the 25 major IT programs, we analyzed DOD's FY 2023
Dashboard data to determine how much the department reported
spending on its 723 standard IT infrastructure programs in FY 2021 and
planned to spend on these programs between FY 2022 and FY 2023.
Based on these data, we calculated the total planned expenditures for the
programs during the 3-year period, including for the 25 largest
infrastructure programs. We also used DOD's FY 2023 budget data to
compare the department's planned spending on the 25 major IT business
programs and 723 standard IT infrastructure programs to the total
planned spending on its unclassified IT portfolio for FY 2021 through FY
2023.[4]

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 the programs to identify any
obvious inconsistencies. In addition, we prepared and sent program
summaries to the 25 major IT business programs and asked program
staff to review the summaries and confirm their accuracy. The 25 program
summaries are included in appendix II. We also met with officials within
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.

Regarding the data collected via our questionnaire, including for
information associated with subsequent objectives, we took steps to
reduce measurement error and non-response error. Specifically, we
conducted pretests of the questionnaire with two programs (one in
development and one in sustainment) to ensure that the questions were
clear, unbiased, and consistently interpreted. The pretests allowed us to
obtain initial program feedback and helped ensure that officials within

---

[3]The Office of Management and Budget 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.

[4]Department of Defense, *Information Technology and Cyberspace Activities Budget
Overview: Fiscal Year (FY) 2023 Budget Request* (May 2022).

each program understood the questions. We also corroborated selected
responses to our questionnaire with supporting documentation and
interviews with program officials. We determined that the data were
reliable for the purposes of this report.

Further, we obtained and analyzed programs' performance metrics data
as of January 2023 and compared the data to Office of Management and
Budget (OMB) guidance.[5] We also met with DOD CIO officials to
determine reasons for differences between how operational performance
metrics 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 identity any obvious inconsistencies. We
also met with DOD CIO officials to determine whether programs
submitted data in accordance with DOD instructions. We determined that
the performance data were sufficiently reliable for our reporting purposes.

For the second objective, we sought information on the software
development and cybersecurity approaches and practices used by the 25
major IT programs via our questionnaire. Our identification of risks
associated with and review of reported software development approaches
and practices focused on the responses to the questionnaire from the
eight programs that we identified as actively developing software. For the
purposes of this assessment, we considered programs to be actively
developing software if program officials reported they were actively
developing new software functionality or if they had not yet reached full
deployment authority to proceed.[6] In addition, we collected and analyzed
key information and documents pertaining to each of the 25 programs'

---

[5]DOD collected the FY 2023 performance metrics data and reported it to GSA; however,
the data did not get posted publically to the Dashboard as they had been in previous
years. DOD sent us the data in August 2022, and we confirmed that they were still current
in January 2023. Office of Management and Budget, *FY 2022 IT Budget—Capital
Planning Guidance* (Washington, D.C.: Nov. 16, 2020).

[6]Of the eight programs that we considered to be actively developing software, officials for
five programs reported that they were actively developing new software functionality, and
three programs reported being in a life cycle stage before full deployment authority to
proceed (ATP). Officials for the other 17 programs reported that their software
development efforts were intended to sustain existing functionality, involved minor
enhancements to a program currently in sustainment, or reported that their program had
reached or proceeded past full deployment ATP or an equivalent milestone. The eight
programs we identified were the ones we expected to most likely be using the more
modern approaches to software development discussed in the related section of the
report.

software development and cybersecurity practices, including information on involving users throughout the development process, capability implementation plans, and cybersecurity strategies. For programs that did not demonstrate having plans, strategies, or other comparable documents, we followed up with officials within DOD CIO and the Office of the Under Secretary of Defense for Acquisition and Sustainment (A&S) for clarification. We selected the topics of software development and cybersecurity to help ensure consistency with companion work that focuses on DOD weapon programs.[7]

We aggregated program office responses and compared the aggregated information from our questionnaires to relevant guidance and leading practices (e.g., Defense Innovation Board and Defense Science Board reports, DOD instructions, and OMB guidance) to identify where there were gaps.[8] In doing so, we identified possible challenges associated with software development and cybersecurity and risks associated with not following guidance and leading practices that may affect acquisition outcomes relative to cost, schedule, and performance.

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.

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.[9] Specifically, we reviewed information previously provided by DOD about the department's plans to implement these

---

[7]GAO, *Weapon Systems Annual Assessment: Programs Are Not Consistently Implementing Practices That Can Help Accelerate Acquisitions*, GAO-23-106059 (Washington, D.C.: June 8, 2023).

[8]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, *Test and Evaluation*, DOD Instruction 5000.89 (Nov. 19, 2020); Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense, *Business Systems Requirements and Acquisition*, DOD Instruction 5000.75, [Incorporating Change 2, (Jan. 24, 2020)] (Washington, D.C.: Feb. 2, 2017); Office of Management and Budget, *FY 2022 IT Budget—Capital Planning Guidance* (Washington, D.C.: Nov. 16, 2020).

[9]The previously identified legislative and policy changes are discussed in GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, GAO-22-105330 (Washington, D.C.: June 14, 2022).

changes and requested status updates, including on DOD's efforts to finalize strategies for its business system and software acquisition pathways; to implement modern approaches to software development such as transitioning to Agile; and to reorganize former CMO responsibilities throughout the department. The objective focused on DOD's efforts to reorganize former CMO responsibilities and planned improvements to how the department manages its IT portfolio (e.g., updates to its investment management guidance and business enterprise architecture), while updates to other efforts are addressed either in the report background or will be addressed in ongoing GAO assessments.

To understand and assess the potential implementation of these changes, we reviewed policies, plans, and guidance provided by DOD; reports that the department submitted to Congress; and internal program documentation. In addition, we interviewed officials within DOD's offices of the CIO, Director of Administration and Management, and Under Secretary of Defense for A&S. We also coordinated with the GAO team conducting a companion assessment examining major defense acquisition programs that was conducted under this same provision of the NDAA for FY 2019.[10]

We conducted this performance audit from June 2022 to June 2023 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 objective.

---

[10]GAO-23-106059.

Appendix II: Program Summaries

This appendix provides summaries of the 25 Department of Defense (DOD) major IT business programs included in our review. Each summary contains a program description and essential information about the program, such as the lead DOD component and acquisition pathway. Each summary also includes a breakdown of the program's actual and planned expenditures over the 3-year period discussed in the report, reported software development practices, and user involvement activities. Programs are listed in order of largest to smallest total planned expenditures. These programs are:

- DOD Healthcare Management System Modernization
- Navy Enterprise Resource Planning
- Global Combat Support System-Army
- Defense Enterprise Accounting and Management System-Increment 1
- Distribution Standard System
- General Fund Enterprise Business System
- Enterprise Business System
- Navy Maritime Maintenance Enterprise Solution
- Maintenance Repair and Overhaul Initiative
- Defense Agencies Initiative
- Joint Operational Medicine Information Systems
- Defense Enrollment Eligibility Reporting System
- Real-Time Automated Personnel Identification System and Common Access Card
- Global Combat Support System-Marine Corps / Logistics Chain Management
- Military Health System Information Platform
- Defense Medical Logistics-Enterprise Solution
- Naval Tactical Command Support System
- Navy Standard Integrated Personnel System
- Standard Procurement System
- Air Force Integrated Personnel and Pay System
- Defense Travel System
- Military Entrance Processing Command Integrated Resource System

GAO-23-106117 IT Systems Annual Assessment

- Army Contract Writing System
- Defense Civilian Personnel Data System
- Navy Electronic Procurement System

DOD Healthcare Management System Modernization (DHMSM)

Program
Department of Defense Healthcare Management System Modernization (DHMSM)

Software development approaches
Agile, DevSecOps, Waterfall

Average time of software deliveries

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

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M)
$1,073.73 mil

$2,415.7 million

Total development, modernization and enhancement (DME)
$1,341.97 mil

Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: — *No change*

Schedule: — *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

DOD established the Defense Health Agency's DHMSM to acquire and implement a configurable and scalable modernized electronic health record system to replace the department's legacy healthcare systems. DHMSM is to replace these legacy systems with an off-the-shelf electronic health record system intended to enable improved sustainability, flexibility, interoperability, and continuity of care.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Health Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Acquisition decision memorandum for continued fielding

Next planned milestone: Full deployment authority to proceed (ATP) and capability support ATP

Year investment began: 2014

Year investment is estimated to reach the end of its useful life: 2034

Chief Information Officer evaluation rating: 3 - Medium risk

Tables 8-10 provide additional key information about DHMSM, including a breakdown of the program's actual and planned expenditures from fiscal year (FY) 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 8: Department of Defense Healthcare Management System Modernization's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	385.72	277.47	**663.19**
2022 (projected)	566.39	374.51	**940.9**
2023 (requested)	389.86	421.75	**811.61**
3-year total	**1341.97**	**1073.73**	**2415.7**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 9: Department of Defense Healthcare Management System Modernization's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps); Waterfall
Delivery of minimum viable product	Yes
Software releases to date	3,867
Planned releases	30
Average time between releases	4-6 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 10: Department of Defense Healthcare Management System Modernization's Reported Activities to Involve Users

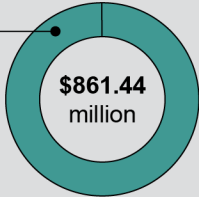| User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Monthly
Frequency of involving users in program testing	Daily, weekly, monthly, quarterly
Frequency of surveying users about customer experience	Lessons learned post wave deployments; annual survey

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Navy Enterprise Resource Planning (ERP)

Program
Navy Enterprise Resource Planning (Navy ERP)

Software development approaches
Agile, DevSecOps, other incremental

Average time of software deliveries

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

Less than one month

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M) **$861.44 mil**

$861.44 million

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

Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬇ *Decrease*

Schedule: ➡ *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

Navy ERP is the Department of the Navy's 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 program officials as of February 2023)

Lead DOD component: Navy, Marine Corps

Program owner: Navy

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Full-rate production (full deployment decision)

Next planned milestone: The program is in sustainment

Year investment began: 2004

Year investment is estimated to reach the end of its useful life: FY 2033

Chief Information Officer evaluation rating: 4 - Low risk

Tables 11-13 provide additional key information about Navy ERP, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 11: Navy Enterprise Resource Planning's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

	Dollars in millions		
FY	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	381.02	381.02
2022 (projected)	0	232.21	232.21
2023 (requested)	0	248.21	248.21
3-year total	**0**	**861.44**	**861.44**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 12: Navy Enterprise Resource Planning's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps); other incremental
Delivery of minimum viable product	Yes
Software releases to date	2,282
Planned releases	Monthly releases with weekly maintenance releases for configuration changes
Average time between releases	1 week
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 13: Navy Enterprise Resource Planning's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Weekly, biweekly, monthly
Frequency of involving users in program testing	Daily
Frequency of surveying users about customer experience	Weekly, monthly

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Global Combat Support System-Army (GCSS-A)

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

Software development approaches
Agile, other incremental

Average time of software deliveries

1-3 months	4-6	7-9	10-12	13+

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME)
$134.11 mil

$642.09 million

Total operations and maintenance (O&M)
$507.98 mil

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Department of the Army's GCSS-A is intended to provide functional services to its 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 program officials as of February 2023)

Lead DOD component: Army

Program owner: Army

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Increment 2 full deployment authority to proceed (ATP)

Next planned milestone: Capability support ATP

Year investment began: 2016

Year investment is estimated to reach the end of its useful life: 2032

Chief Information Officer evaluation rating: 5 - Low risk

Tables 14-16 provide additional key information about GCSS-A, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 14: Global Combat Support System-Army's (GCSS-A) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

	Dollars in millions		
FY	Development, modernization, and enhancement (DME) expenditures[a]	Operations and sustainment (O&S) expenditures[b]	Total expenditures (DME + O&S)
2021 (actual)	73.44	220.01	293.45
2022 (projected)	56.57	161.33	217.90
2023 (requested)	4.10	126.64	130.74
3-year total	**134.11**	**507.98**	**642.09**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]GCSS-A program officials reported updated DME expenditures in February 2023. These values are (in millions of dollars) 54.73, 52.18, and 19.80 for FY 2021, FY 2022, and FY 2023, respectively.

[b]GCSS-A program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 63.65, 58.04, and 63.62 for FY 2021, FY 2022, and FY 2023, respectively.

Table 15: Global Combat Support System-Army's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile, other incremental
Delivery of minimum viable product	Yes
Software releases to date	60
Planned releases	12
Average time between releases	3-6 months
Uses a software factory	Not applicable

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 16: Global Combat Support System-Army's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Every other week
Frequency of involving users in program testing	Quarterly
Frequency of surveying users about customer experience	After each unit that receives training and fielding

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117
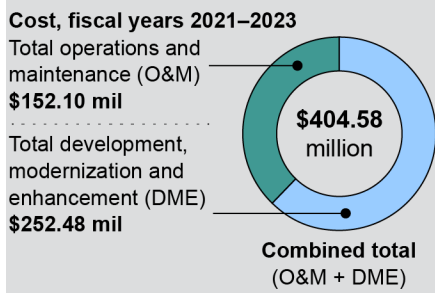
Defense Enterprise Accounting and Management System-Increment 1 (DEAMS)

Program
Defense Enterprise Accounting and Management System-Increment 1 (DEAMS)

Software development approaches
Agile, DevSecOps

Average time of software deliveries

| 0-3 | 4-6 | 7-9 | 10-12 | 13+ |
Less than one month

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M) **$152.10 mil**

$404.58 million

Total development, modernization and enhancement (DME) **$252.48 mil**

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Department of the Air Force's 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 some legacy systems.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Air Force

Program owner: Air Force

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Full deployment authority to proceed (ATP)

Next planned milestone: Capability support ATP

Year investment began: 2003

Year investment is estimated to reach the end of its useful life: No current end date

Chief Information Officer evaluation rating: 4 - Low risk

Tables 17-19 provide additional key information about DEAMS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 17: Defense Enterprise Accounting and Management System-Increment 1's (DEAMS) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

| FY | Dollars in millions | | |
	Development, modernization, and enhancement (DME) expenditures[a]	Operations and sustainment (O&S) expenditures[b]	Total expenditures (DME + O&S)
2021 (actual)	46.25	73	119.25
2022 (projected)	63.44	79.09	142.53
2023 (requested)	142.79	0.01	142.8
3-year total	**252.48**	**152.1**	**404.58**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]DEAMS program officials reported updated DME expenditures in February 2023. These values are (in millions of dollars) 40.43, 54.67, and 49.77 for FY 2021, FY 2022, and FY 2023, respectively.

[b]DEAMS program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 72.91, 80.93, and 84.84 for FY 2021, FY 2022, and FY 2023, respectively.

Table 18: Defense Enterprise Accounting and Management System-Increment 1's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	No
Software development approach	Agile; development, security, and operations (DevSecOps)
Delivery of minimum viable product	Yes
Software releases to date	355
Planned releases	Each project team releases on a 3-week or 12-week iteration until all capability is released into production
Average time between releases	Less than 1 month
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 19: Defense Enterprise Accounting and Management System-Increment 1's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Daily
Frequency of involving users in program testing	Daily
Frequency of surveying users about customer experience	Daily

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Distribution Standard System (DSS)

Program
Distribution Standard System (DSS)

Software development approaches
Agile, other incremental

Average time of software deliveries

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

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME)
$72.56 mil

$399.98 million

Total operations and maintenance (O&M)
$327.42 mil

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *Yes*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

DSS is the Defense Logistics Agency's standard automated system for distributing DOD materiel (i.e., equipment and supplies). The system is intended to provide global service and worldwide support to the warfighter, peacekeepers, and federal and civilian customers.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Logistics Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support authority to proceed

Next planned milestone: The program is in sustainment and plans to continue to support capabilities by conducting technical refresh

Year investment began: 1992

Year investment is estimated to reach the end of its useful life: 2026

Chief Information Officer evaluation rating: 3 – Medium risk

Tables 20-22 provide additional key information about DSS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 20: Distribution Standard System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

| FY | Dollars in millions | | |
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	28.38	75.79	104.17
2022 (projected)	20.40	117.31	137.71
2023 (requested)	23.78	134.32	158.10
3-year total	**72.56**	**327.42**	**399.98**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 21: Distribution Standard System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile, other incremental
Delivery of minimum viable product	Yes
Software releases to date	40
Planned releases	92
Average time between releases	4-6 months
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 22: Distribution Standard System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	User feedback is imbedded in processes
Frequency of involving users in program testing	Users are imbedded in the program's testing cycles
Frequency of surveying users about customer experience	Daily

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

General Fund Enterprise Business System (GFEBS)

Program
General Fund Enterprise Business System (GFEBS)

Software development approaches
Agile, DevOps, other incremental, Waterfall

Average time of software deliveries

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

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME)
$41.72 mil

$396.80 million

Total operations and maintenance (O&M)
$355.08 mil

Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬤ *No change*

Schedule: ⬤ *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

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 program officials as of February 2023)

Lead DOD component: Army

Program owner: Army

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support authority to proceed

Next planned milestone: The program is in sustainment

Year investment began: 2005

Year investment is estimated to reach the end of its useful life: 2032

Chief Information Officer evaluation rating: 5 - Low risk

Tables 23-25 provide additional key information about GFEBS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 23: General Fund Enterprise Business System's (GFEBS) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures[a]	Operations and sustainment (O&S) expenditures[b]	Total expenditures (DME + O&S)
2021 (actual)	16.93	131.06	147.99
2022 (projected)	14.40	122.66	137.06
2023 (requested)	10.39	101.36	111.75
3-year total	**41.72**	**355.08**	**396.80**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]GFEBS program officials reported updated DME expenditures in February 2023. These values are (in millions of dollars) 19.69, 19.77, and 15.77 for FY 2021, FY 2022, and FY 2023, respectively.

[b]GFEBS program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 64.14, 62.13, and 43.04 for FY 2021, FY 2022, and FY 2023, respectively.

Table 24: General Fund Enterprise Business System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile, development and operations (DevOps), other incremental, Waterfall
Delivery of minimum viable product	Yes
Software releases to date	221
Planned releases	231
Average time between releases	1-3 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 25: General Fund Enterprise Business System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Daily
Frequency of involving users in program testing	Daily
Frequency of surveying users about customer experience	Weekly

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Enterprise Business System (EBS)

Program
Enterprise Business Systems (EBS)

Software development approaches
Agile, DevOps, DevSecOps, other incremental

Average time of software deliveries

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

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME) **$26.05**

$318.83 million

Total operations and maintenance (O&M) **$318.78 mil**

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: — *No change*

Schedule: — *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Logistics Agency's EBS 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 program officials as February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Logistics Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support authority to proceed (ATP)

Next planned milestone: Capability support ATP

Year investment began: 2001

Year investment is estimated to reach the end of its useful life: 2030

Chief Information Officer evaluation rating: 5 - Low risk

Tables 26-28 provide additional key information about EBS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 26: Enterprise Business System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	6.05	73.79	79.84
2022 (projected)	14	124.94	138.94
2023 (requested)	6	120.05	126.05
3-year total	**26.05**	**318.78**	**344.83**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 27: Enterprise Business System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development and operations (DevOps); development, security, and operations (DevSecOps); other incremental
Delivery of minimum viable product	Yes
Software releases to date	44
Planned releases	91
Average time between releases	4-6 months
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 28: Enterprise Business System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Daily
Frequency of involving users in program testing	User acceptance testing is performed with each release
Frequency of surveying users about customer experience	User feedback is provided during user acceptance testing

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Navy Maritime Maintenance Enterprise Solution (NMMES)

Program
Navy Maritime Maintenance Enterprise Solution (NMMES)

Software development approaches
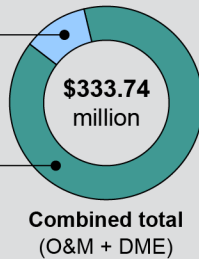Agile, DevOps, DevSecOps, other incremental, Waterfall

Average time of software deliveries

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

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME) **$36.76 mil**

$333.74 million

Total operations and maintenance (O&M) **$296.98 mil**

Combined total (O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

Navy's NMMES is intended to consolidate overlapping application functionality and databases, data centers, and infrastructure for ship and submarine maintenance into a fully integrated enterprise solution resulting in reduced costs.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Navy, Marine Corps

Program owner: Navy

Acquisition pathway: Software acquisition, defense business systems acquisition, defense acquisition of service

Last milestone achieved: Capability support authority to proceed (ATP)

Next planned milestone: Capability support ATP

Year investment began: 2012

Year investment is estimated to reach the end of its useful life: FY 2034

Chief Information Officer evaluation rating: 4 – Low risk

Tables 29-31 provide additional key information about NMMES, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 29: Navy Maritime Maintenance Enterprise Solution's (NMMES) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures[a]	Operations and sustainment (O&S) expenditures[b]	Total expenditures (DME + O&S)
2021 (actual)	13.69	96.55	110.24
2022 (projected)	9.97	100.03	110
2023 (requested)	13.10	100.40	113.50
3-year total	**36.76**	**296.98**	**333.74**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]NMMES program officials reported updated DME expenditures in February 2023. These values are (in millions of dollars) 21.53, 15.93, 17.47 for FY 2021, FY 2022, and FY 2023, respectively.

[b]NMMES program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 96.53, 105.4, and 95.47 for FY 2021, FY 2022, and FY 2023, respectively.

Table 30: Navy Maritime Maintenance Enterprise Solution's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development and operations (DevOps); development, security, and operations (DevSecOps); other incremental; Waterfall
Delivery of minimum viable product	Yes
Software releases to date	Not applicable; unable to track total releases due to the age of some systems
Planned releases	Not applicable; program consists of over 35 applications that have individual release schedules or are included in a batch of releases for multiple updates
Average time between releases	1-3 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 31: Navy Maritime Maintenance Enterprise Solution's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Daily
Frequency of involving users in program testing	Weekly
Frequency of surveying users about customer experience	Program does not have formal surveys; product owners and representatives regularly contact users and obtain feedback

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Maintenance Repair and Overhaul Initiative (MROI)

Program
Maintenance, Repair, and Overhaul Initiative (MROI)

Software development approaches
Agile, DevSecOps, other incremental

Average time of software deliveries

1-3 months   4-6   7-9   10-12   13+

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME)
$326.23 mil

$326.88 million

Total operations and maintenance (O&M)
$.65 mil

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *Yes*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

MROI is intended to provide the Air Force's sustainment center with an integrated capability for planning, scheduling, and executing organic depot maintenance. The initiative supports Agile planning, optimized workload assignment, resource allocation, integrated quality, and maintenance-driven Air Force working capital fund financials for auditability.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Air Force

Program owner: Air Force

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Limited deployment authority to proceed (ATP)

Next planned milestone: Limited deployment ATPs

Year investment began: 2013

Year investment is estimated to reach the end of its useful life: FY 2036

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 32-34 provide additional key information about MROI, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 32: Maintenance Repair and Overhaul Initiative's (MROI) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

| FY | Dollars in millions | | |
	Development, modernization, and enhancement (DME) expenditures[a]	Operations and sustainment (O&S) expenditures[b]	Total expenditures (DME + O&S)
2021 (actual)	240.81	0.23	241.04
2022 (projected)	42.83	0.19	43.02
2023 (requested)	42.59	0.23	42.82
3-year total	**326.23**	**0.65**	**326.88**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]MROI program officials reported updated DME expenditures in February 2023. These values are (in millions of dollars) 28.38, 42.83, and 39.26 for FY 2021, FY 2022, and FY 2023, respectively.

[b]MROI program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 0.23, 0.19, and 0.23 for FY 2021, FY 2022, and FY 2023, respectively.

Table 33: Maintenance Repair and Overhaul Initiative's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps); other incremental
Delivery of minimum viable product	Yes
Software releases to date	1
Planned releases	2 with follow-on minimum viable products under Agile construct
Average time between releases	Develops code in 13-week increments, system not yet implemented
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 34: Maintenance Repair and Overhaul Initiative's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Weekly
Frequency of involving users in program testing	Weekly
Frequency of surveying users about customer experience	Not applicable; the program is still in development.

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Defense Agencies Initiative (DAI)

Program
Defense Agencies Initiative (DAI)
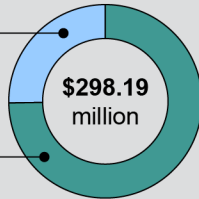
Software development approaches
Other incremental

Average time of software deliveries

1-3   4-6   7-9   10-12   13+
                      months

Cost, fiscal years 2021–2023
Total development, modernization and enhancement (DME) $74.74 mil

$298.19 million

Total operations and maintenance (O&M) $223.45 mil

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: *Increase*

Schedule: *Delay*

Rebaseline: *Yes*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Logistics Agency's DAI is intended to transform the budget, finance, and accounting operations of DOD components in order to achieve accurate and reliable information in support of financial accountability and effective and efficient decision-making. The initiative is a critical part of the department's effort to modernize its financial management capabilities.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Logistics Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Limited deployment authority to proceed (ATP)

Next planned milestone: Limited deployment ATPs

Year investment began: 2017

Year investment is estimated to reach the end of its useful life: FY 2035

Chief Information Officer evaluation rating: 4 – Low risk

Tables 35-37 provide additional key information about DAI, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 35: Defense Agencies Initiative's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	20.43	66.88	87.31
2022 (projected)	31.14	72.52	103.66
2023 (requested)	23.17	84.05	107.22
3-year total	**74.74**	**223.45**	**298.19**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 36: Defense Agencies Initiative's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Other incremental
Delivery of minimum viable product	Yes
Software releases to date	5
Planned releases	7
Average time between releases	10-12 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 37: Defense Agencies Initiative's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Issues with the system are addressed through reports submitted by the users via help desk functionality; requirements development is done collaboratively with users during the release development process
Frequency of involving users in program testing	Users are involved in user acceptance testing for all releases
Frequency of surveying users about customer experience	Surveying occurs through help desk tickets and the program's hosting of the quarterly Executive Steering Group to address customer issues and questions

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

# Joint Operational Medicine Information Systems (JOMIS)

Program
Joint Operational Medicine Information Systems (JOMIS)

Software development approaches
Agile, DevOps, DevSecOps

Average time of software deliveries

| 0-3 | 4-6 | 7-9 | 10-12 | 13+ |
Less than one month

Cost, fiscal years 2021–2023
Total development, modernization and enhancement (DME)
$282.21 mil

$283.68 million

Total operations and maintenance (O&M)
$1.47 mil

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: *No change*

Schedule: *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description
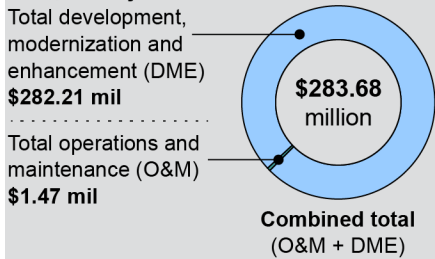
The Defense Health Agency's JOMIS is a collection of systems that will pursue efforts allowing it to sunset costly and difficult-to-maintain legacy systems. The program will acquire solutions for the modernization of operational medicine information systems to provide commanders and medical professionals with integrated, timely, and accurate information to make critical command and control and medical decisions.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Health Agency

Acquisition pathway: Middle tier of acquisition, major capability acquisition, software acquisition

Last milestone achieved: According to the JOMIS acquisition strategy, the program will be managed as a portfolio of products with each managed application to deliver needed capabilities via the most effective and efficient pathway available

Next planned milestone: There are multiple products in the process of development and delivery, each product is in a different phase of the acquisition life cycle

Year investment began: 2016

Year investment is estimated to reach the end of its useful life: 2045

Chief Information Officer evaluation rating: 4 – Low risk

Tables 38-40 provide additional key information about JOMIS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 38: Joint Operational Medicine Information Systems' (JOMIS) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures[a]	Operations and sustainment (O&S) expenditures[b]	Total expenditures (DME + O&S)
2021 (actual)	83.90	0	83.90
2022 (projected)	87.55	0	87.55
2023 (requested)	110.76	1.47	112.23
3-year total	**282.21**	**1.47**	**283.68**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]JOMIS program officials reported updated DME expenditures in February 2023. These values are (in millions of dollars) 67.25, 87.82, and 112.23 for FY 2021, FY 2022, and FY 2023, respectively.

[b]JOMIS program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 0 for FY 2023.

Table 39: Joint Operational Medicine Information Systems' Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development and operations (DevOps); development, security, and operations (DevSecOps)
Delivery of minimum viable product	Yes
Software releases to date	64
Planned releases	Biweekly releases for the full life cycle of the program
Average time between releases	Less than 1 month
Uses a software factory	Not applicable

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 40: Joint Operational Medicine Information Systems' Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Continuous based on capability; working groups were established with biweekly communication via email between scheduled meetings
Frequency of involving users in program testing	The program conducts development and acceptance testing, and operational testing involving the user community
Frequency of surveying users about customer experience	Pre-training, immediately post training, 3 weeks after training

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Defense Enrollment Eligibility Reporting System (DEERS)

Program
Defense Enrollment Eligibility Reporting System (DEERS)

Software development approaches
Agile, Waterfall

Average time of software deliveries

1-3   4-6   7-9   10-12   13+
months

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M)
$257.65 mil

$257.65 million

Total development, modernization and enhancement (DME)
$0

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⊖ *No change*

Schedule: ⊖ *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Health Agency's DEERS is the authoritative data repository for all DOD workforce, personnel benefits, eligibility, and military health care system enrollment information.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Health Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support

Next planned milestone: The program is in sustainment

Year investment began: 1978

Year investment is estimated to reach the end of its useful life: No current end date

Chief Information Officer evaluation rating: 3 - Medium risk

Tables 41-43 provide additional key information about DEERS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 41: Defense Enrollment Eligibility Reporting System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

	Dollars in millions		
FY	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	104.31	104.31
2022 (projected)	0	75.62	75.62
2023 (requested)	0	77.72	77.72
3-year total	**0**	**257.65**	**257.65**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 42: Defense Enrollment Eligibility Reporting System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	No
Software development approach	Agile, Waterfall
Delivery of minimum viable product	No
Software releases to date	There is no specific record due to the age of the program, applications have averaged 4 releases per year in recent years but can vary depending on requirements
Planned releases	Applications plan an average of 4 releases per year
Average time between releases	1-3 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 43: Defense Enrollment Eligibility Reporting System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Daily, weekly, every other week, monthly, and quarterly
Frequency of involving users in program testing	Daily
Frequency of surveying users about customer experience	Never

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

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

Program

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

Software development approaches
DevOps, other

Average time of software deliveries

1-3   4-6   7-9   10-12   13+
    months

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME)
$26.12 mil

$228.29 million

Total operations and maintenance (O&M)
$202.17 mil

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ⊖ *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Human Resources Activity's RAPIDS and Common Access Card is the infrastructure that supports the uniformed services identification card, provides online updates to the Defense Enrollment Eligibility Reporting System, and issues the common access card to service members, civilian employees, and eligible contractors.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Human Resources Activity

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Solution analysis authority to proceed (ATP)

Next planned milestone: Functional requirements ATP

Year investment began: 1997

Year investment is estimated to reach the end of its useful life: No current end date

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 44-46 provide additional key information about RAPIDS and Common Access Card, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 44: Real-Time Automated Personnel Identification System and Common Access Card's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

	Dollars in millions		
FY	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	11.26	66.01	77.27
2022 (projected)	4.69	57.24	61.93
2023 (requested)	10.17	78.92	89.09
3-year total	**26.12**	**202.17**	**228.29**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 45: Real-Time Automated Personnel Identification System and Common Access Card's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Development and operations (DevOps), other
Delivery of minimum viable product	No
Software releases to date	Different systems have delivered a different number of releases so far (approximately 1-3 releases)
Planned releases	8 (4 major and 4 minor releases per program's 12-month contractual period)
Average time between releases	1-3 months, 4-6 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 46: Real-Time Automated Personnel Identification System and Common Access Card's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Quarterly
Frequency of involving users in program testing	Release-specific
Frequency of surveying users about customer experience	Customer feedback is captured on an ad-hoc basis within the system and through the call center

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

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

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

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M) $199.94 mil

Total development, modernization and enhancement (DME) $0

$199.94 million

Combined total (O&M + DME)

Cost and Schedule Changes *(since January 2021)*

Cost: ⬇ *Decrease*

Schedule: ➖ *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

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

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Navy, Marine Corps

Program owner: Navy

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Full deployment for the operations and support acquisition phase.

Next planned milestone: The program is in sustainment

Year investment began: 2004

Year investment is estimated to reach the end of its useful life: FY 2035

Chief Information Officer evaluation rating: 4 – Low risk

Tables 47-49 provide additional key information about GCSS-MC/LCM, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 47: Global Combat Support System-Marine Corps / Logistics Chain Management's (GCSS-MC/LCM) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures[a]	Total expenditures (DME + O&S)
2021 (actual)	0	61.61	61.61
2022 (projected)	0	69.47	69.47
2023 (requested)	0	68.86	68.86
3-year total	**0**	**199.94**	**199.94**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]GCSS-MC/LCM program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 61.22, 69.06, and 68.46 for FY 2021, FY 2022, and FY 2023, respectively.

Table 48: Global Combat Support System-Marine Corps / Logistics Chain Management's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile
Delivery of minimum viable product	Yes
Software releases to date	Software change and security patch releases are conducted monthly
Planned releases	Software changes and security patch releases are conducted monthly
Average time between releases	Monthly
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 49: Global Combat Support System–Marine Corps / Logistics Chain Management's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Product owners lead Agile development efforts providing user requirements during development and refinement
Frequency of involving users in program testing	Product owners test software as sprints or releases are completed
Frequency of surveying users about customer experience	Service desk ticket survey conducted after completion of each trouble ticket, system usability scale survey is approximately every 2-3 years

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Military Health System Information Platform (MIP)

Program
Military Health System Information Platform (MIP)

Software development approaches
Agile, DevSecOps, other incremental

Average time of software deliveries

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

Less than a month

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M) $197.51 mil

$197.51 million

Total development, modernization and enhancement (DME) $0

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆️ *Increase*

Schedule: ➡️ *Delay*

Rebaseline: *Yes*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Health Agency's MIP serves to deliver, connect, and curate data to facilitate informed decision-making in health data integration. The platform also serves as a hub for patient information, clinical decision support tools, medical readiness innovation, clinical research, and centralized, advanced operational and clinical analytics.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Health Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Deliver capabilities

Next planned milestone: Deliver capabilities

Year investment began: 2019

Year investment is estimated to reach the end of its useful life: FY 2032

Chief Information Officer evaluation rating: 4 – Low risk

Tables 50-52 provide additional key information about MIP, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 50: Military Health System Information Platform's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	47.55	47.55
2022 (projected)	0	59.94	59.94
2023 (requested)	0	95.02	95.02
3-year total	**0**	**197.51**	**197.51**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 51: Military Health System Information Platform's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps); other incremental
Delivery of minimum viable product	Yes
Software releases to date	The program has a continuous development release on the user interfaces, releases are variable in size and frequency depending on requirements and priority
Planned releases	The program has a continuous development release on the user interfaces, releases are variable in size and frequency depending on requirements and priority
Average time between releases	The program releases user interface improvements continuously
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 52: Military Health System Information Platform's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Every other week
Frequency of involving users in program testing	Every other Week
Frequency of surveying users about customer experience	Biannually

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Defense Medical Logistics-Enterprise Solution (DML-ES)

Program
Defense Medical Logistics-Enterprise Solution (DML-ES)

Software development approaches
Agile, DevSecOps, other incremental

Average time of software deliveries

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

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M)
$188.93 mil

$188.93 million

Total development, modernization and enhancement (DME)
$0

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Health Agency's DML-ES supports DOD's integration of medical logistics business capabilities.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Health Agency

Acquisition pathway: Defense business system acquisition

Last milestone achieved: Full deployment, technical change for process migrating to cloud hosting capabilities

Next planned milestone: Continued capability delivery and support

Year investment began: 1993

Year investment is estimated to reach the end of its useful life: fiscal year (FY) 2033

Chief Information Officer evaluation rating: 4- Low risk

Tables 53-55 provide additional key information about DML-ES, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 53: Defense Medical Logistics-Enterprise Solution's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	57.78	57.78
2022 (projected)	0	72.97	72.97
2023 (requested)	0	58.18	58.18
3-year total	**0**	**188.93**	**188.93**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 54: Defense Medical Logistics-Enterprise Solution's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps); other incremental
Delivery of minimum viable product	Yes
Software releases to date	68
Planned releases	101
Average time between releases	4-6 months
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 55: Defense Medical Logistics-Enterprise Solution's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Monthly
Frequency of involving users in program testing	Monthly
Frequency of surveying users about customer experience	Quarterly

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117
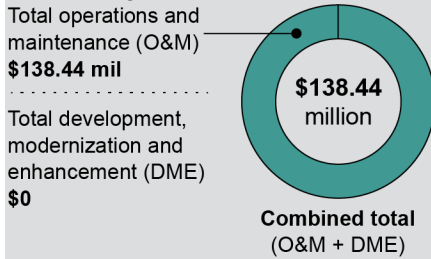
Navy Tactical Command Support System (NTCSS)

Program
Naval Tactical Command Support System (NTCSS)

Software development approaches
DevOps, other incremental, Waterfall

Average time of software deliveries

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

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M)
$138.44 mil

Total development, modernization and enhancement (DME)
$0

$138.44 million

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ⊖ *No change*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

Navy's NTCSS is a suite of applications supporting the Navy and Marine Corps' supply and maintenance activities, both ashore and afloat, in a common computing infrastructure. The system manages non-tactical information resources, including logistics; maintenance; administration; and supply management, to meet the Navy and Marine Corps' force readiness and sustainment requirements.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Navy, Marine Corps

Program owner: Navy

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Fielding decision

Next planned milestone: The program is in sustainment

Year investment began: 2004

Year investment is estimated to reach the end of its useful life: FY 2032

Chief Information Officer evaluation rating: 5 – Low risk

Tables 56-58 provide additional key information about NTCSS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 56: Navy Tactical Command Support System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

	Dollars in millions		
FY	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	46.33	46.33
2022 (projected)	0	47.42	47.42
2023 (requested)	0	44.69	44.69
3-year total	**0**	**138.44**	**138.44**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 57: Navy Tactical Command Support System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	No
Software development approach	Development and operations (DevOps), other incremental, Waterfall
Delivery of minimum viable product	Not applicable
Software releases to date	5
Planned releases	6
Average time between releases	13 or more months
Uses a software factory	Not applicable

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 58: Navy Tactical Command Support System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	The program is in sustainment and does not collect user feedback because it does not have requirements development or refinement
Frequency of involving users in program testing	Not applicable
Frequency of surveying users about customer experience	Not applicable

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Navy Standard Integrated Personnel System (NSIPS)

Program
Navy Standard Integrated Personnel System (NSIPS)

Software development approaches
Waterfall

Average time of software deliveries

1-3 months	4-6	7-9	10-12	13+

Cost, fiscal years 2021–2023

Total operations and maintenance (O&M)
$129.23 mil

Total development, modernization and enhancement (DME)
$0

$129.23 million

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: No change

Schedule: No change

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

NSIPS is the Navy's human resource management system for approximately 400,000 sailors worldwide. The system tracks the personnel record from accession to departure from Navy service.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Navy, Marine Corps

Program owner: Navy

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Full operational capability
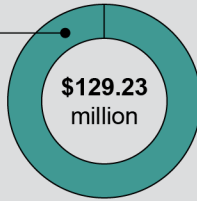
Next planned milestone: Retirement

Year investment began: 1996

Year investment is estimated to reach the end of its useful life: FY 2028

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 59-61 provide additional key information about NSIPS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 59: Navy Standard Integrated Personnel System's (NSIPS) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures[a]	Total expenditures (DME + O&S)
2021 (actual)	0	34.65	34.65
2022 (projected)	0	47.68	47.68
2023 (requested)	0	46.9	46.90
3-year total	**0**	**129.23**	**129.23**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]NSIPS program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 30.72, 32.19, and 42.01 for FY 2021, FY 2022, and FY 2023, respectively.

Table 60: Navy Standard Integrated Personnel System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	No
Software development approach	Waterfall
Delivery of minimum viable product	Not applicable
Software releases to date	0
Planned releases	Program plans for quarterly releases, with more than 50 releases planned since full operating capability
Average time between releases	1-3 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 61: Navy Standard Integrated Personnel System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Quarterly
Frequency of involving users in program testing	Quarterly
Frequency of surveying users about customer experience	Surveys are offered to customers when reaching out to the help desk

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Standard Procurement System (SPS)

Program
Standard Procurement System (SPS)

Software development approaches
Waterfall

Average time of software deliveries

1-3   4-6   7-9   10-12   13+
months

Cost, fiscal years 2021–2023

Total operations and maintenance (O&M)
$121.35 mil

Total development, modernization and enhancement (DME)
$0

$121.35 million

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Logistics Agency's SPS automates the contracting process from procurement request through award and administration to final closeout. The system accomplishes three main functions: contract placement, procurement, and contract administration.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Logistics Agency

Acquisition pathway: System acquisition, defense business systems acquisition

Last milestone achieved: Full-rate production (full deployment decision)

Next planned milestone: Decommissioning, the program has a formal sunset date currently planned to be by the end of FY 2026

Year investment began: 1994

Year investment is estimated to reach the end of its useful life: FY 2026

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 62-64 provide additional key information about SPS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 62: Standard Procurement System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

| FY | Dollars in millions | | |
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	41.76	41.76
2022 (projected)	0	32.22	32.22
2023 (requested)	0	47.37	47.37
3-year total	**0**	**121.35**	**121.35**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 63: Standard Procurement System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	No
Software development approach	Waterfall
Delivery of minimum viable product	Not applicable
Software releases to date	18
Planned releases	19
Average time between releases	10-12 months
Uses a software factory	Not applicable

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 64: Standard Procurement System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Weekly, quarterly
Frequency of involving users in program testing	Quarterly
Frequency of surveying users about customer experience	Weekly

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117
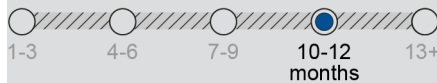
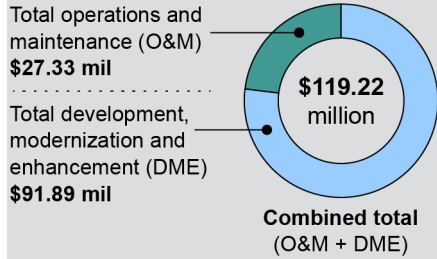# Air Force Integrated Personnel and Pay System (AFIPPS)

Program description

Air Force's 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 program officials as of February 2023)

Lead DOD component: Air Force

Program owner: Air Force

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Acquisition authority to proceed (ATP)

Next planned milestone: Limited deployment ATP

Year investment began: 2009

Year investment is estimated to reach the end of its useful life: 2036

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 65-67 provide additional key information about AFIPPS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Program
Air Force Integrated Personnel and Pay System (AFIPPS)

Software development approaches
Agile, Waterfall

Average time of software deliveries

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

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M)
$27.33 mil

$119.22 million

Total development, modernization and enhancement (DME)
$91.89 mil

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *Expects to*

Table 65: Air Force Integrated Personnel and Pay System's (AFIPPS) Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures[a]	Operations and sustainment (O&S) expenditures[b]	Total expenditures (DME + O&S)
2021 (actual)	26.75	5.52	32.27
2022 (projected)	29.40	10.79	40.19
2023 (requested)	35.74	11.02	46.76
3-year total	**91.89**	**27.33**	**119.22**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

[a]AFIPPS program officials reported updated DME expenditures in February 2023. These values are (in millions of dollars) 31.33, 33.95, and 37.90 for FY 2021, FY 2022, and FY 2023, respectively.

[b]AFIPPS program officials reported updated O&S expenditures in February 2023. These values are (in millions of dollars) 5.41, 5.52, and 5.49 for FY 2021, FY 2022, and FY 2023, respectively.

Table 66: Air Force Integrated Personnel and Pay System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile, Waterfall
Delivery of minimum viable product	Yes
Software releases to date	0
Planned releases	2
Average time between releases	10-12 months
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 67: Air Force Integrated Personnel and Pay System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	Yes
Frequency of collecting user feedback during requirements development and refinement	Daily
Frequency of involving users in program testing	Daily
Frequency of surveying users about customer experience	Not applicable

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Defense Travel System (DTS)

Program
Defense Travel System (DTS)
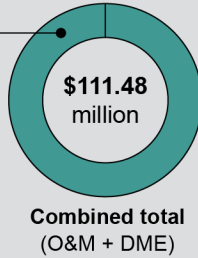
Software development approaches
Agile, DevSecOps

Average time of software deliveries

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

Cost, fiscal years 2021–2023

Total operations and maintenance (O&M)
$111.48 mil

Total development, modernization and enhancement (DME)
$0

$111.48 million

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: No change

Schedule: No change

Rebaseline: No

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Human Resources Activity's DTS is a travel management system that automates DOD's temporary duty travel and allows travelers to create authorizations, prepare reservations, receive approvals, generate travel vouchers, and direct deposit payment to travelers and the government charge card vendor.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Human Resources Activity

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support

Next planned milestone: The program is in sustainment

Year investment began: 2003

Year investment is estimated to reach the end of its useful life: 2027

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 68-70 provide additional key information about DTS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 68: Defense Travel System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	29.52	29.52
2022 (projected)	0	42.72	42.72
2023 (requested)	0	39.24	39.24
3-year total	**0**	**111.48**	**111.48**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 69: Defense Travel System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps)
Delivery of minimum viable product	Yes
Software releases to date	36 major releases issued since the base year
Planned releases	The program is currently in sustainment, government requires at least 4 major releases per year and minor updates as necessary
Average time between releases	1-3 months
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 70: Defense Travel System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Weekly
Frequency of involving users in program testing	Daily
Frequency of surveying users about customer experience	Monthly

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Military Entrance Processing Command Integrated Resource System (MIRS)

Program
Military Entrance Processing Command Integrated Resource System (MIRS)

Software development approaches
Agile, DevOps, DevSecOps

Average time of software deliveries

1-3 months	4-6	7-9	10-12	13+

Cost, fiscal years 2021–2023

Total development, modernization and enhancement (DME) **$22.41 mil**

$110.65 million

Total operations and maintenance (O&M) **$88.24 mil**

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

Army's MIRS provides the automation and communications capability to meet the military's workforce accession mission for the armed services to include collecting and retaining applicant qualification information.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Army

Program owner: Army

Acquisition pathway: The closest pathway description is software acquisition. Portions of the program were reengineered and deployed in a cloud environment in February 2021. The remaining portions are being redesigned for the cloud

Last milestone achieved: The program has been operational in the cloud since February 2021

Next planned milestone: The program is continuing to migrate other applications into the cloud

Year investment began: 1995

Year investment is estimated to reach the end of its useful life: No current end date

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 71-72 provide additional key information about MIRS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.
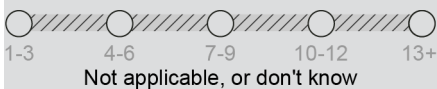
Table 71: Military Entrance Processing Command Integrated Resource System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

	Dollars in millions		
FY	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	11.1	33.56	44.66
2022 (projected)	9.09	32.93	42.02
2023 (requested)	2.22	21.75	23.97
3-year total	**22.41**	**88.24**	**110.65**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 72: Military Entrance Processing Command Integrated Resource System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development and operations (DevOps); development, security, and operations (DevSecOps)
Delivery of minimum viable product	Yes
Software releases to date	45 total releases (delivered 2 production releases for FY 2023, 25 during FY 2022, and 18 since the system's deployments)
Planned releases	Approximately 23 more releases are planned for a total of 68 total releases through the end of FY 2023. The program's roadmap currently extends to FY 2023, has 1 year of additional planned development work with new and refined feature releases at the end of each 2-week sprint. The long-range plan is to continue to have 2-week sprints after FY 2023 throughout the life of the program
Average time between releases	1-3 months
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 73: Military Entrance Processing Command Integrated Resource System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Every other week
Frequency of involving users in program testing	Every other week
Frequency of surveying users about customer experience	Every other week

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Army Contract Writing System (ACWS)

Program description

ACWS is intended to be the Army's single, enterprise-wide, contract writing and management system. The system is also intended to replace existing legacy contract systems and facilitate the standardization of Army's procurement business processes and integration with other DOD systems.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Army

Program owner: Army

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Acquisition authority to proceed (ATP)

Next planned milestone: Limited deployment ATP

Year investment began: 2014

Year investment is estimated to reach the end of its useful life: No current end date

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 74-76 provide additional key information about ACWS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Program
Army Contract Writing System (ACWS)

Software development approaches
Agile, DevSecOps

Average time of software deliveries

1-3   4-6   7-9   10-12   13+
Not applicable, or don't know

Cost, fiscal years 2021–2023

Total operations and maintenance (O&M)
$32.15 mil

$92.55 million

Total development, modernization and enhancement (DME)
$60.4 mil

Combined total
(O&M + DME)
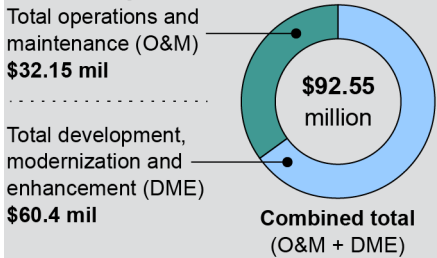
Cost and Schedule Changes
(since January 2021)

Cost: ⬇ *Decrease*

Schedule: ⬅ *Shortened*

Rebaseline: *Expects to*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Table 74: Army Contract Writing System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	24.48	8.70	33.18
2022 (projected)	35.92	12.83	48.75
2023 (requested)	0	10.62	10.62
3-year total	**60.4**	**32.15**	**92.55**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 75: Army Contract Writing System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps)
Delivery of minimum viable product	Yes
Software releases to date	0
Planned releases	4
Average time between releases	Not applicable or don't know; the cadence of software delivery to the user is still being assessed as the program refines its new strategy. The program will either be on a 3-week delivery cycle, 13-week delivery cycle, or a 10-12 month delivery cycle
Uses a software factory	No

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 76: Army Contract Writing System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Weekly
Frequency of involving users in program testing	Currently in planning stage; users will be involved as required by 4-week interval sprints or capability increment
Frequency of surveying users about customer experience	Not applicable; there are no active users at this time. The program is targeting FY 2023 for a minimum viable product delivery

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Defense Civilian Personnel Data System (DCPDS)

Program
Defense Civilian Personnel Data System (DCPDS)

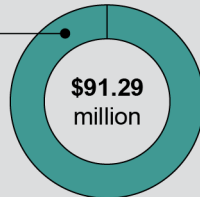**Software development approaches**
Agile, Waterfall

Average time of software deliveries

◉////// ◯////// ◯////// ◯////// ◯
1-3   4-6   7-9   10-12   13+
months

Cost, fiscal years 2021–2023
Total operations and maintenance (O&M)
$91.29 mil

$91.29 million

Total development, modernization and enhancement (DME)
$0

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬆ *Increase*

Schedule: ➡ *Delay*

Rebaseline: *No*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

The Defense Human Resources Activity's DCPDS is DOD's enterprise civilian human resources automated system that supports one-third of the federal workforce. The system's operational activities include processing of all personnel transactions, providing workforce analysis, and reporting for the department and external government agencies.

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Defense-wide

Program owner: Defense Human Resources Activity

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support

Next planned milestone: Decommissioning

Year investment began: 1994

Year investment is estimated to reach the end of its useful life: 2026

Chief Information Officer evaluation rating: 3 – Moderate risk

Tables 77-79 provide additional key information about DCPDS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 77: Defense Civilian Personnel Data System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	0	32.25	32.35
2022 (projected)	0	32.64	32.64
2023 (requested)	0	26.30	26.30
3-year total	**0**	**91.29**	**91.29**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 78: Defense Civilian Personnel Data System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	No
Software development approach	Agile, Waterfall
Delivery of minimum viable product	Yes
Software releases to date	127
Planned releases	Quarterly releases applied to the program since deployment, latest release was version 128
Average time between releases	1-3 months
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 79: Defense Civilian Personnel Data System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	The program is in sustainment; requirements are refined via problem reports to be resolved in the current system
Frequency of involving users in program testing	Every other week
Frequency of surveying users about customer experience	Accomplished previously but the program is no longer collecting this information since it is in sustainment

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Navy Electronic Procurement System (EPS)

Program
Navy Electronic Procurement System (EPS)

Software development approaches
Agile, DevSecOps

Average time of software deliveries

○⁄⁄⁄⁄⁄⁄⁄○⁄⁄⁄⁄⁄⁄⁄○⁄⁄⁄⁄⁄⁄⁄○⁄⁄⁄⁄⁄⁄⁄○
1-3   4-6   7-9   10-12   13+
months

Cost, fiscal years 2021–2023
Total development, modernization and enhancement (DME) **$81.66 mil**
. . . .
Total operations and maintenance (O&M) **$2.78 mil**

$84.44 million

Combined total
(O&M + DME)

Cost and Schedule Changes
(since January 2021)

Cost: ⬇ *Decrease*
. . . .
Schedule: ➡ *Delay*
. . . .
Rebaseline: *Expects to*

Source: GAO analysis of Department of Defense program questionnaire responses, as of February 2023, and fiscal year 2023 data reported to the Federal IT Dashboard. | GAO-23-106117

Program description

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

Program essentials (reported by program officials as of February 2023)

Lead DOD component: Navy, Marine Corps

Program owner: Navy

Acquisition pathway: Software acquisition, defense business system acquisition

Last milestone achieved: Decision authority authorized entry into execution phase

Next planned milestone: Contract award to start minimal capability viability release development

Year investment began: 2013

Year investment is estimated to reach the end of its useful life: No current end date

Chief Information Officer evaluation rating: 2 – High risk

Tables 80-82 provide additional key information about Navy EPS, including a breakdown of the program's actual and planned expenditures from FY 2021 through FY 2023, reported software development approaches and practices, and user involvement activities.

Table 80: Navy Electronic Procurement System's Actual and Planned Expenditures from Fiscal Year (FY) 2021 through FY 2023

FY	Dollars in millions		
	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2021 (actual)	29.42	0.90	30.32
2022 (projected)	25.79	0.92	26.71
2023 (requested)	26.45	0.96	27.41
3-year total	**81.66**	**2.78**	**84.44**

Source: GAO analysis of FY 2023 Department of Defense data reported to the Federal IT Dashboard. | GAO-23-106117

Table 81: Navy Electronic Procurement System's Reported Software Development Approaches and Practices

Development approach or practice	Program response
Uses an iterative development approach	Yes
Software development approach	Agile; development, security, and operations (DevSecOps)
Delivery of minimum viable product	Yes
Software releases to date	0 (the program is authorized to enter the execution phase, but has not yet awarded the development contract)
Planned releases	The program intends quarterly releases. For the 5-year period of performance for the program's contract, there are 18 planned releases
Average time between releases	1-3 months
Uses a software factory	Yes

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Table 82: Navy Electronic Procurement System's Reported Activities to Involve Users

User involvement activity	Program response
Had required user training and deployment plans	No
Frequency of collecting user feedback during requirements development and refinement	Daily
Frequency of involving users in program testing	Users are integrated into scrum teams, and testing is a continuous activity as part of the program's Agile based approach. The program is currently in the planning phase; user acceptance testing and developmental testing will be executed with user participation once in execution
Frequency of surveying users about customer experience	Surveys will be performed with every customer once in execution

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2023. | GAO-23-106117

Appendix III: Comments from the Department of Defense

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

CHIEF INFORMATION OFFICER

MAY 1 1 2023

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-23-106117, "IT SYSTEMS ANNUAL ASSESSMENT: DoD Needs to Improve Performance Reporting and Development Planning," dated March 30, 2023 (GAO Code 106117). The Department is in general agreement with the overall content of the draft audit report; however, we non-concur with both recommendations. Enclosed are detailed comments on the report recommendations.

The Department appreciates the opportunity to review the draft report. My point of contact for this matter is Ms. Lora Muchmore at (703) 981-9666 or lora.h.muchmore.civ@mail.mil.

Sincerely,

John B. Sherman

Enclosure:
As stated

GAO DRAFT REPORT DATED MARCH 30, 2023
GAO-23-106117 (GAO CODE 106117)

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

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The Secretary of Defense should direct the Chief Information
Officer to ensure that major IT business programs identify at least the minimum required amount
of operational performance metrics, as appropriate, in the department's submission to the Federal
IT Dashboard.

DoD RESPONSE: Non-concur. DoD CIO, DCIO(R&A), RPB implemented an audit as part of
the IT/CA budget collection process to ensure major IT investments report operational metrics in
accordance with OMB requirements. A Corrective Action Plan was previously provided to GAO
to close this recommendation is attached. The FY24 PB operational metrics will be visible to
GAO on the Federal IT Dashboard when the DoD submission is complete.

RECOMMENDATION 2: The Secretary of Defense should direct the Chief Information
Officer to ensure that major IT business programs develop capability implementation plans or
other program plans that address conducting user training and deployment, as appropriate.

DoD RESPONSE: Non-concur. The requirement to develop capability implementation plans
has been codified within the DoDI 5000.75. As a Defense Business System (DBS) progresses
through the Business Capability Acquisition Cycle (BCAC) they are required to mature their
user training and deployment plans at each BCAC phase/authority to proceed (ATP) decision
point. Per the DoDI 5000.75, the Milestone Decision Authority (MDA) has the ability to review
the user training and deployment plans prior to progressing into the capability support phase.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact	Vijay A. D'Souza at (202) 512-7650
Staff Acknowledgments	Principal contributors to this report were Eric Trout (Assistant Director), Tyler Mountjoy (Analyst in Charge), Gerard Aflague, Lauri Barnes, Chris Businsky, Anthony Gray, Evan Kreiensieck, Richard Sayoc, and Joseph Suh. Other key contributors included Bea Alff, Amanda Andrade, Margaret Best, Garret Chan, Kara Epperson, Michael Holland, Jennifer Leotta, Lori Martinez, Anne McDonough, Shelby Oakley, Sarah Ong, Scott Pettis, Brandon Sanders, Hai Tran, Walter Vance, Adam Vodraska, Jon Wall, Kevin Walsh, Andrew Weiss, and Marshall Williams.