



# IT SYSTEMS ANNUAL ASSESSMENT

## DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps

Report to Congressional Committees

July 2024  
GAO-24-106912  
United States Government Accountability Office

Accessible Version

# GAO Highlights

View [GAO-24-106912](#). For more information, contact Vijay D'Souza at (202) 512-7650 or [dsouzav@gao.gov](mailto:dsouzav@gao.gov).  
Highlights of [GAO-24-106912](#), a report to congressional committees

July 2024

## IT SYSTEMS ANNUAL ASSESSMENT

### **DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps**

#### **Why GAO Did This Study**

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

The National Defense Authorization Act for FY 2019, as amended, includes a provision for GAO to conduct assessments of selected DOD IT programs annually through March 2026. GAO's objectives for this fifth such review were to (1) examine the cost, schedule, and performance of selected DOD IT business programs, (2) assess the extent to which DOD has implemented key software development and cybersecurity practices for selected programs, and (3) describe DOD actions to implement legislative and policy changes that could affect its IT acquisitions.

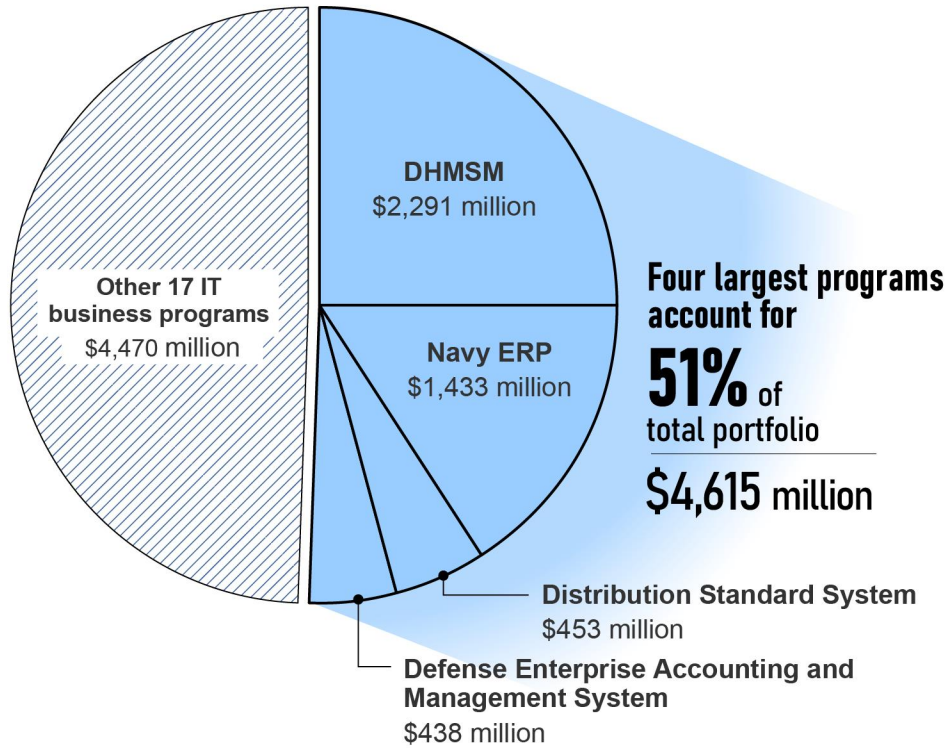
To address the first objective, GAO selected 21 DOD IT business programs, including (1) 20 business programs listed as major IT investments in the department's FY 2024 submission to the Federal IT Dashboard and (2) an additional business program that had been previously designated as major and continued to have high annual costs. In analyzing the FY 2024 Dashboard data, GAO examined DOD's planned expenditures for these programs from FY 2022 through FY 2024.

GAO also administered a questionnaire to the 21 program offices to obtain and analyze information about cost and schedule changes that the programs reported experiencing since January 2022.

#### **What GAO Found**

According to the Department of Defense's (DOD) fiscal year (FY) 2024 Federal IT Dashboard data, DOD's planned expenditures for 21 selected IT business programs amounted to \$9.1 billion from FY 2022 through FY 2024. The four largest programs accounted for just over half of the planned cost of the portfolio (see figure).

**The Department of Defense's (DOD) Planned Costs for the Four Largest IT Business Programs Compared to the Remaining 17 Selected Programs from Fiscal Year (FY) 2022–FY 2024**



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

Source: GAO analysis of DOD's FY 2024 Federal IT Dashboard data. | GAO-24-106912

For the 21 programs, 70 percent (\$6.4 billion) of the total reported cost across the 3 years was for operating and maintaining the systems and 30 percent (\$2.7 billion) was for development and modernization.

Officials from 15 of the 21 IT business programs reported cost and/or schedule changes since January 2022 (see figure).

Further, GAO compared programs' performance metrics data reported on the Dashboard to OMB guidance and met with DOD CIO officials to understand differences in how the data were reported.

To address the second objective, the questionnaire also sought information about the programs' software development and cybersecurity practices, including their use and documentation of Agile metrics and development of cybersecurity strategies. GAO compared the responses and documentation against relevant guidance and best practices (e.g. DOD guidance and GAO's Agile Guide) to identify gaps and risks associated with not following the guidance. For programs that did not follow the guidance or demonstrate having documentation, GAO followed up with DOD officials for clarification on reasons why the programs did not do so.

For the third objective, GAO reviewed policy, plans, and guidance associated with the department's efforts to reorganize former CMO responsibilities; implement changes to its defense business systems investment management guidance and business enterprise architecture; and adopt zero trust cybersecurity principles. GAO also met with DOD CIO officials to discuss the department's efforts in these areas.







### **What GAO Recommends**

GAO is making one recommendation to DOD to ensure that IT business programs developing software are using Agile metrics and management tools required by DOD and consistent with GAO's Agile Guide. DOD concurred with GAO's recommendation and described actions it planned to take to address it. In its prior annual assessment reviews, GAO made three recommendations related to performance reporting and cybersecurity strategies. Although DOD described actions it planned to take to address the recommendations, they have not yet been implemented. Doing so would help ensure that the issues GAO identified are addressed.

## Selected Department of Defense (DOD) IT Business Programs Reported Cost and Schedule Changes Since January 2022

| Cost  | Schedule                                  |  |
|-------|---|--|
| Red   | Diagonal lines (top-left to bottom-right) | Air Force Integrated Personnel and Pay System                              |
| Red   | Diagonal lines (top-left to bottom-right) | Defense Enterprise Accounting and Management System                        |
| Red   | Diagonal lines (top-left to bottom-right) | Defense Travel System  |
| Red   | Diagonal lines (top-left to bottom-right) | Navy Maritime Maintenance Enterprise Solution                              |
| Red   | Diagonal lines (top-left to bottom-right) | Naval-Maintenance, Repair, and Overhaul                                    |
| Red   | Diagonal lines (top-left to bottom-right) | Navy Personnel and Pay   |
| Red   | Diagonal lines (top-left to bottom-right) | Navy Electronic Procurement System   |
| Red   | Diagonal lines (bottom-left to top-right) | Global Combat Support System-Marine Corps/Logistics Chain Management       |
| Red   | Diagonal lines (bottom-left to top-right) | General Fund Enterprise Business System                                    |
| Red   | Diagonal lines (bottom-left to top-right) | Joint Operational Medicine Information Systems                             |
| Red   | Diagonal lines (bottom-left to top-right) | Naval Air Systems Command Aviation Logistics Environment                   |
| Red   | Diagonal lines (bottom-left to top-right) | Navy Enterprise Resource Planning  |
| Red   | Diagonal lines (bottom-left to top-right) | Real-Time Automated Personnel Identification System and Common Access Card |
| Green | Diagonal lines (bottom-left to top-right) | Distribution Standard System   |
| Green | Diagonal lines (bottom-left to top-right) | Global Combat Support System-Army  |
| White | Diagonal lines (bottom-left to top-right) | Defense Agencies Initiative  |
| White | Diagonal lines (bottom-left to top-right) | Defense Enrollment Eligibility Reporting System                            |
| White | Diagonal lines (bottom-left to top-right) | DOD Healthcare Management System Modernization                             |
| White | Diagonal lines (bottom-left to top-right) | Enterprise Business System   |
| White | Diagonal lines (bottom-left to top-right) | Military Health System Information Platform                                |
| White | Diagonal lines (bottom-left to top-right) | Theater Medical Information Program-Joint Increment 2                      |

|                 |  |   |   |
|-----------------|--|---|---|
| <b>Cost</b>     |  Increase |  Decrease    |  No change |
| <b>Schedule</b> |  Delay    |  Improvement |  No change |

Source: GAO analysis of DOD program questionnaire responses as of February 2024. | GAO-24-106912

This included 13 programs that reported cost increases ranging from \$0.5 million to \$1.3 billion (a median of \$163.3 million) and seven that reported schedule delays ranging from 15 months to 36 months (a median of 24 months).

Programs reported mixed progress on performance. Programs are required to identify and track a minimum of five metrics covering customer satisfaction, business results, financial performance, and innovation. Of the 21 programs, four reported meeting all performance targets, 10 reported meeting at least one, and one reported meeting none. The remaining six programs did not report. GAO has previously recommended that DOD ensure that such reporting occur.

The 10 DOD IT business programs actively developing software reported using recommended Agile and iterative approaches. However, in areas related to tracking customer satisfaction and progress of software development, four of the 10 programs did not use metrics and management tools required by DOD and consistent with GAO's Agile Assessment Guide. As a result, the department risks not having sound information on its Agile software development efforts.

Further, while program officials for all 21 programs reported conducting cybersecurity testing and assessments, several programs did not have an approved cybersecurity strategy. In June 2022, GAO had recommended that DOD's Chief Information Officer (CIO) ensure that programs each develop such a strategy. The department concurred with the recommendation and officials stated that they were continuing to follow up with programs that did not have a strategy.

Regarding legislative and policy changes, DOD is revising its business systems investment management guidance, modernizing its business enterprise architecture, and adopting zero trust cybersecurity principles. GAO will continue

to monitor DOD's efforts to redistribute roles and responsibilities, improve department management of IT investments, and adopt zero trust cybersecurity.

# Contents

|   |  |
|---|--|
| GAO Highlights  | ii   |
| <b>Why GAO Did This Study</b>   | ii   |
| <b>What GAO Found</b>   | ii   |
| <b>What GAO Recommends</b>  | iv   |
| <hr/>   |  |
| Letter  | 1  |
| Background  | 3  |
| Selected Business Programs Reported Cost and Schedule Changes and Mixed Progress on Performance                           | 14   |
| Selected Programs Reported Using Software Development and Cybersecurity Practices, but Some Lacked Metrics and Strategies | 23   |
| DOD Continues to Implement Legislative and Policy Changes   | 32   |
| Conclusions   | 34   |
| Recommendation for Executive Action   | 34   |
| Agency Comments   | 34   |
| <hr/>   |  |
| Appendix I  | Objectives, Scope, and Methodology 37  |
| Appendix II   | Program Summaries 40   |
| Appendix III  | Comments from the Department of Defense 68   |
| Accessible Text for Appendix III  | Comments from the Department of Defense 69   |
| Appendix IV   | GAO Contact and Staff Acknowledgments 70   |
| <hr/>   |  |
| Tables  |  |
| Table 1:  | The Department of Defense’s (DOD) Actual and Planned Costs for 21 Selected IT Business Programs from Fiscal Year (FY) 2022 through FY 2024 15          |
| Table 2:  | Iterative Software Development Approaches Recommended by the Defense Science Board 25  |
| Table 3:  | The Selected Department of Defense (DOD) IT Business Programs Actively Developing Software Reported Using Recommended Iterative Practices 26           |
| Table 4:  | The Selected Department of Defense (DOD) IT Business Programs Reported Using Metrics Identified in GAO’s <i>Agile Assessment Guide</i> 27              |
| Table 5:  | The Selected Department of Defense (DOD) IT Business Programs Demonstrated Using Management Tools Identified in GAO’s <i>Agile Assessment Guide</i> 28 |
| Table 6:  | The Selected Department of Defense (DOD) IT Business Programs Reported Conducting Developmental and Operational Cybersecurity Testing 29               |

Table 7: The Selected Department of Defense (DOD) IT Business Programs Reported Key Software Development and Cybersecurity Challenges and Actions to Address Them 31

Table 8: Air Force Integrated Personnel and Pay System’s (AFIPPS) Reported Software Development Approaches and Practices 41

Table 9: Defense Agencies Initiative’s (DAI) Reported Software Development Approaches and Practices 43

Table 10: Defense Enrollment Eligibility Reporting System’s (DEERS) Reported Software Development Approaches and Practices 44

Table 11: Defense Enterprise Accounting and Management System’s (DEAMS) Reported Software Development Approaches and Practices 45

Table 12: Defense Travel System’s (DTS) Reported Software Development Approaches and Practices 46

Table 13: Distribution Standard System’s (DSS) Reported Software Development Approaches and Practices 47

Table 14: Department of Defense Healthcare Management System Modernization’s (DHMSM) Reported Software Development Approaches and Practices 50

Table 15: Enterprise Business System’s (EBS) Reported Software Development Approaches and Practices 52

Table 16: General Fund Enterprise Business System’s (GFEBS) Reported Software Development Approaches and Practices 52

Table 17: Global Combat Support System-Army’s (GCSS-A) Reported Software Development Approaches and Practices 53

Table 18: Global Combat Support System-Marine Corps/Logistics Chain Management’s (GCSS-MC/LCM) Reported Software Development Approaches and Practices 54

Table 19: Joint Operational Medicine Information Systems’ (JOMIS) Reported Software Development Approaches and Practices 55

Table 20: Military Health System Information Platform’s (MIP) Reported Software Development Approaches and Practices 56

Table 21: Naval-Maintenance, Repair, and Overhaul’s (N-MRO) Reported Software Development Approaches and Practices 58

Table 22: Naval Air Systems Command Aviation Logistics Environment’s (NAVAIR ALE) Reported Software Development Approaches and Practices 58

Table 23: Navy Electronic Procurement System’s (Navy EPS) Reported Software Development Approaches and Practices 60

Table 24: Navy Enterprise Resource Planning’s (Navy ERP) Reported Software Development Approaches and Practices 61

Table 25: Navy Maritime Maintenance Enterprise Solution’s (NMMES) Reported Software Development Approaches and Practices 62

Table 26: Navy Personnel and Pay’s (NP2) Reported Software Development Approaches and Practices 64



|  |    |
|--|----|
| Table 27: Real-Time Automated Personnel Identification System and Common Access Card's (RAPIDS) Reported Software Development Approaches and Practices | 66 |
| Table 28: Theater Medical Information Program-Joint Increment 2's (TMIP-J) Reported Software Development Approaches and Practices                      | 66 |

---

**Figures**

|   |     |
|---|-----|
| The Department of Defense's (DOD) Planned Costs for the Four Largest IT Business Programs Compared to the Remaining 17 Selected Programs from Fiscal Year (FY) 2022–FY 2024                   | iii |
| Selected Department of Defense (DOD) IT Business Programs Reported Cost and Schedule Changes Since January 2022   | v   |
| Figure 1: The Department of Defense's (DOD) Business Capability Acquisition Cycle   | 5   |
| Figure 2: The Department of Defense's Software Acquisition Pathway  | 7   |
| Figure 3: The Department of Defense's (DOD) Planned Costs for the Four Largest IT Business Programs Compared to the Remaining 17 Selected Programs from Fiscal Year (FY) 2022 through FY 2024 | 16  |
| Figure 4: Selected Department of Defense (DOD) IT Business Programs Reported Cost and Schedule Changes Since January 2022   | 18  |
| Figure 5: Selected Department of Defense (DOD) IT Business Programs' Performance Measures   | 22  |
| Accessible Data for Figure 5: Selected Department of Defense (DOD) IT Business Programs' Performance Measures   | 22  |

---

**Abbreviations**

|           |   |
|-----------|---|
| A&S       | Acquisition and Sustainment   |
| AFIPPS    | Air Force Integrated Personnel and Pay System                       |
| ATP       | authority to proceed  |
| BEA       | business enterprise architecture                                    |
| CIO       | Chief Information Officer   |
| CMO       | Chief Management Officer  |
| DBC       | Defense Business Council  |
| DEAMS     | Defense Enterprise Accounting and Management System                 |
| DevOps    | Development and Operations  |
| DevSecOps | Development, Security, and Operations                               |
| DHA       | Defense Health Agency   |
| DHMSM     | Department of Defense Healthcare Management System<br>Modernization |
| DLA       | Defense Logistics Agency  |
| DME       | development, modernization, and enhancement                         |
| DOD       | Department of Defense   |
| DSS       | Distributed Standard System   |
| DTS       | Defense Travel System   |
| FY        | fiscal year   |
| GSA       | General Services Administration                                     |
| Navy EPS  | Navy Electronic Procurement System                                  |
| Navy ERP  | Navy Enterprise Resource Planning                                   |
| NDAA      | National Defense Authorization Act                                  |
| N-MRO     | Naval-Maintenance, Repair, and Overhaul                             |
| O&S       | operations and sustainment  |
| OMB       | Office of Management and Budget                                     |

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



July 11, 2024

## Congressional Committees

The Department of Defense (DOD) is one of the largest and most complex organizations in the world. To meet its mission to protect the security of our nation and deter war, DOD relies heavily on the use of IT for ensuring the success of its major business functions. These functions include such areas as health care, human capital, financial management, logistics, and contracting. The John S. McCain National Defense Authorization Act (NDAA) for fiscal year (FY) 2019 includes a provision as amended for GAO to conduct annual assessments of selected DOD IT programs through March 2026.<sup>1</sup>

This report presents the results of our fifth annual assessment. Our specific objectives for this assessment were to (1) examine the cost, schedule, and performance of selected DOD IT business programs, (2) assess the extent to which DOD has implemented key software development and cybersecurity practices for selected programs, and (3) describe DOD actions to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, we selected 21 IT business programs for review,<sup>2</sup> including 20 business programs that DOD listed as major IT investments in its FY 2024 Federal IT Dashboard (Dashboard) data<sup>3</sup> We added an additional business program that, among other things, had been previously designated as major and continued to have high annual costs.<sup>4</sup>

We analyzed the Dashboard data to examine DOD's planned costs for the 21 business programs from FY 2022 through FY 2024, including a breakdown of the costs for operating and maintaining the systems compared to development and modernization. We also analyzed program officials' responses to a

---

<sup>1</sup>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 section 3072 and amended by Pub. L. No. 116-283 (William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021), § 813, 1807(g)(1), 134 Stat. 3388, 3749 and 4159 (Jan. 1, 2021). Under this provision, we were to report on these assessments no later than March 30 of each year from 2020 through 2023. 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, § 812(a), 136 Stat. 2395, 2706 (Dec. 23, 2022). Our assessment of the performance of DOD's weapon programs is included in a separate report, which we also prepared in response to this legislative mandate. See GAO, *Weapon Systems Annual Assessment: DOD Is Not Yet Well-Positioned to Field Systems with Speed*, [GAO-24-106831](#) (Washington, D.C.: June 17, 2024).

<sup>2</sup>DOD classifies these programs as defense business systems.

<sup>3</sup>The Federal IT Dashboard (Dashboard) is a public, government website operated by the General Services Administration (GSA) at <https://itdashboard.gov/>. It includes streamlined data on IT investments to enable agencies and Congress to better understand and manage federal IT portfolios. In all, we selected 20 of the 21 programs that DOD listed as major investments in its FY 2024 Dashboard data. We excluded the one program due to the department reporting no planned expenditures for it in FY 2024, planning to retire the system, and no longer considering it to be a major investment.

<sup>4</sup>The Defense Travel System (DTS) was selected because it was listed by DOD as a major investment the previous year, has a high annual cost (e.g., the total requested amount exceeded \$30 million), and has an important role in the department's mission, consistent with Office of Management and Budget (OMB) guidance for designating major investments. We also selected the program because officials reported changes to its plans, including DOD extending its use of the system an additional 5 years as a result of the department canceling the intended new system known as MyTravel. GAO, *Defense Management: DOD Challenges with Travel Programs and Business Process Reforms*, [GAO-23-106945](#) (Washington, D.C.: July 26, 2023).

questionnaire we developed and administered to all 21 programs in September 2023. Officials provided their responses, and we followed up with programs through February 2024. The questionnaire addressed such issues as whether (1) programs had experienced cost or schedule changes since January 1, 2022, and (2) programs had rebaselined or expected to rebaseline as a result of the changes.<sup>5</sup>

Further, we analyzed programs' performance metrics data included in DOD's FY 2024 reporting to the Dashboard and compared the data to Office of Management and Budget (OMB) guidance.<sup>6</sup> We also met with officials within the department's Office of the Chief Information Officer (CIO) to determine reasons for differences between how the performance 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 21 programs via our questionnaire, including 10 programs that we identified as actively developing software.<sup>7</sup> We aggregated the program office responses to our questionnaire and compared the information to relevant guidance and best practices (e.g., Defense Science Board and Defense Innovation Board reports, DOD instructions, and OMB guidance) to identify where there were gaps.<sup>8</sup> In addition, we collected and analyzed key information and supporting documents related to the programs' reported practices, including their use of metrics and management tools identified in GAO's *Agile Assessment Guide (Agile Guide)* and development of approved cybersecurity strategies, and compared it to DOD's guidance.<sup>9</sup> In doing so, we identified risks associated with not following the guidance and practices that may affect acquisition outcomes relative to cost, schedule, and performance. For programs that did not follow the guidance or demonstrate having such documentation, we followed up with program officials and officials within the Office of the CIO and the Office of the Under Secretary of Defense for Acquisition and Sustainment (A&S) for reasons why they did not do so.

Further, we obtained information from program officials about key challenges the programs were facing related to software development and cybersecurity and actions these officials reported taking to mitigate them. We

---

<sup>5</sup>OMB's guidance states that agencies and contractors should establish a performance measurement baseline to track progress and report cost and schedule variance. Rebaselines are any revision to the investment's baseline and should be reviewed and approved according to agency governance processes.

<sup>6</sup>Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (Washington, D.C.: Aug. 15, 2022). FY 2024 reporting requirements for IT investments are contained in Section 55 of OMB's Circular No. A-11 guidance and in GSA's supporting guidance for complying with OMB's submission requirements. General Services Administration, *BY 2024 IT Collect Submission Overview* (Washington, D.C.: Jan. 27, 2023).

<sup>7</sup>For the purposes of this assessment, we considered programs to be actively developing software if officials reported that they were actively developing new software functionality. Officials for the other 11 programs reported either that their software development efforts were to sustain existing functionality, involved minor enhancements, or that they were not actively developing software.

<sup>8</sup>Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75, Incorporating Change 2, Jan. 24, 2020 (Washington, D.C.: Feb. 2, 2017); Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense, *Test and Evaluation*, Instruction 5000.89 (Nov. 19, 2020); OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

<sup>9</sup>Department of Defense, *DevSecOps Fundamentals Guidebook: DevSecOps Activities and Tools*, Version 2.2 (Washington, D.C.: May 25, 2023); GAO, *Agile Assessment Guide: Best Practices for Adoption and Implementation*, [GAO-24-105506](#) (Washington, D.C.: Dec. 15, 2023).

also obtained information from DOD's Office of the CIO and A&S officials about actions the department was taking to address the challenges.

To address the third objective, we reviewed DOD actions to implement previously identified legislative and policy changes that could affect its IT acquisitions.<sup>10</sup> In addition, we reviewed DOD actions to implement recent legislative requirements (i.e., its efforts to adopt zero trust cybersecurity).<sup>11</sup> To assess the actions DOD has taken toward implementing 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 weapon system acquisition programs.<sup>12</sup> Appendix I provides a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from June 2023 to July 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

In support of its military operations, DOD manages many IT investments encompassing communications, command and control, and business systems that support the department's operations. For FY 2024, the department requested approximately \$43.3 billion for its unclassified IT investments, including its major IT and other business programs which are intended to help the department sustain its key business operations (e.g., health care, human capital, financial management, logistics, and contracting).<sup>13</sup>

---

### DOD's Policy and Framework for Managing 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.<sup>14</sup> 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.

---

<sup>10</sup>The previously identified legislative and policy changes are discussed in GAO, *IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Development Planning*, [GAO-23-106117](#) (Washington, D.C.: June 13, 2023).

<sup>11</sup>Zero trust is a set of cybersecurity principles that are founded on the concept that no actor, system, network, or service operating outside of or within an organization's security perimeter should be trusted. Instead, the principles suggest that organizations must verify anything and everything that attempts to establish access to their systems, services, and networks.

<sup>12</sup>[GAO-24-106831](#).

<sup>13</sup>These unclassified IT investments also include non-major programs and supporting infrastructure.

<sup>14</sup>Department of Defense, *Operation of the Adaptive Acquisition Framework*, Instruction 5000.02 (Washington, D.C.: Jan. 23, 2020).

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

While the instruction established an overarching policy for acquisition programs, separate instructions specify the roles, responsibilities, and procedures for each pathway. Of the six pathways, two deal primarily with the acquisition of IT: business systems and software.

### Business Systems Acquisition Pathway

According to DOD Instruction 5000.02, the purpose of the business systems pathway is to acquire information systems that support DOD's business operations. The pathway can also be used to acquire non-developmental, software-intensive programs that are not business systems. Under this pathway, DOD is to assess the business 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.<sup>15</sup> While maintaining the general structure of the defense business systems pathway, the 2020 update removed certain oversight requirements and encouraged a tailored approach to each program. The 2020 update also enabled and encouraged acquisition officials to delegate decision-making down to the "lowest practical level."

Under the pathway, business system acquisition program officials are to

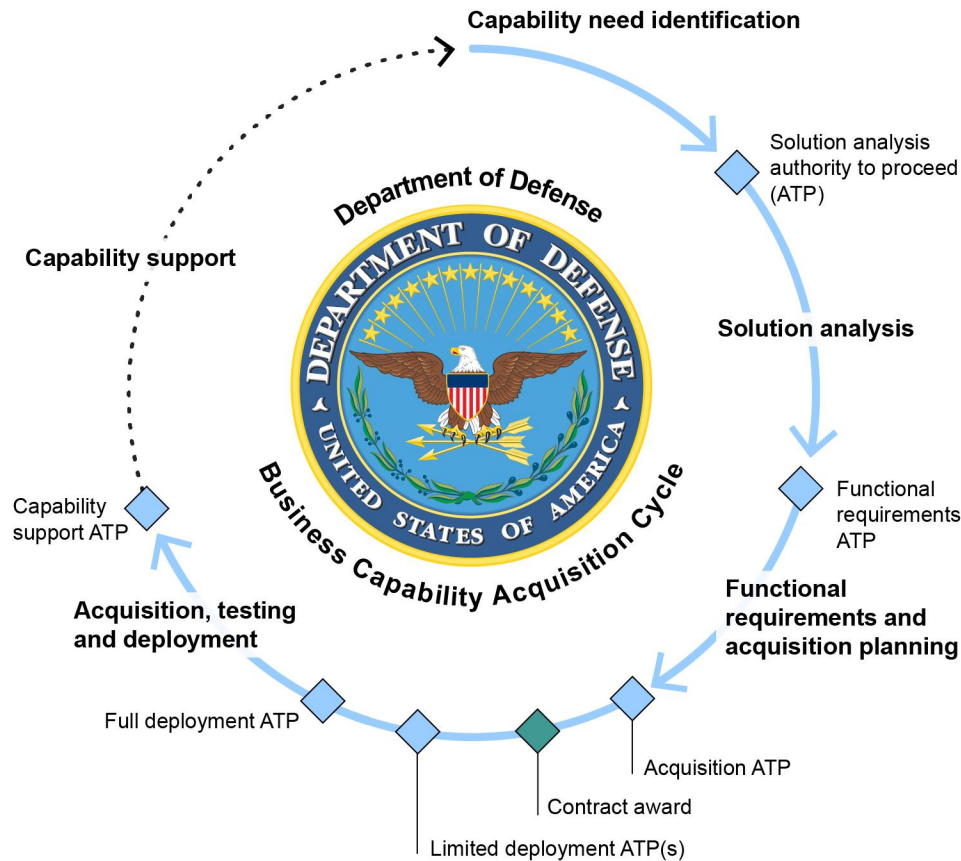
- align the program with commercial best practices;
- minimize the need for customization of commercial products to the greatest extent possible;
- conduct thorough industry analysis and market research of both process and IT solutions using commercial off-the-shelf and government off-the-shelf software;
- tailor and delegate authority to proceed (ATP) 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.

---

<sup>15</sup>Department of Defense, *Instruction 5000.75*.

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



Source: GAO presentation of DOD information; DOD (logo). | GAO-24-106912

These milestones fall under the two higher-level phases of the system life cycle, referred to as development and sustainment.

Development is associated with the activities and milestones starting at the beginning of the system life cycle, at the capability need–identification stage, and includes the development and delivery of new functionality or enhancements through limited and full deployments. A limited deployment is any deployment before the full deployment ATP that provides a set of functionalities to a set of users of the business system. Limited deployments are approved at a limited deployment ATP, a decision point where the milestone decision authority considers the results of testing and approves the deployment of the release to limited portions of the end user community.<sup>16</sup> Full deployment is the delivery of full functionality to all planned users of the business system in accordance with the full deployment ATP. This is a decision point where the milestone decision authority considers the results of limited deployment(s) and operational testing and approves deployment to the entire user community.

<sup>16</sup>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.

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

### Software Acquisition Pathway

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

According to DOD Instruction 5000.02, the software acquisition pathway is intended to integrate modern software development practices such as Agile; Development, Security, and Operations (DevSecOps); and lean practices.<sup>19</sup> 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.

---

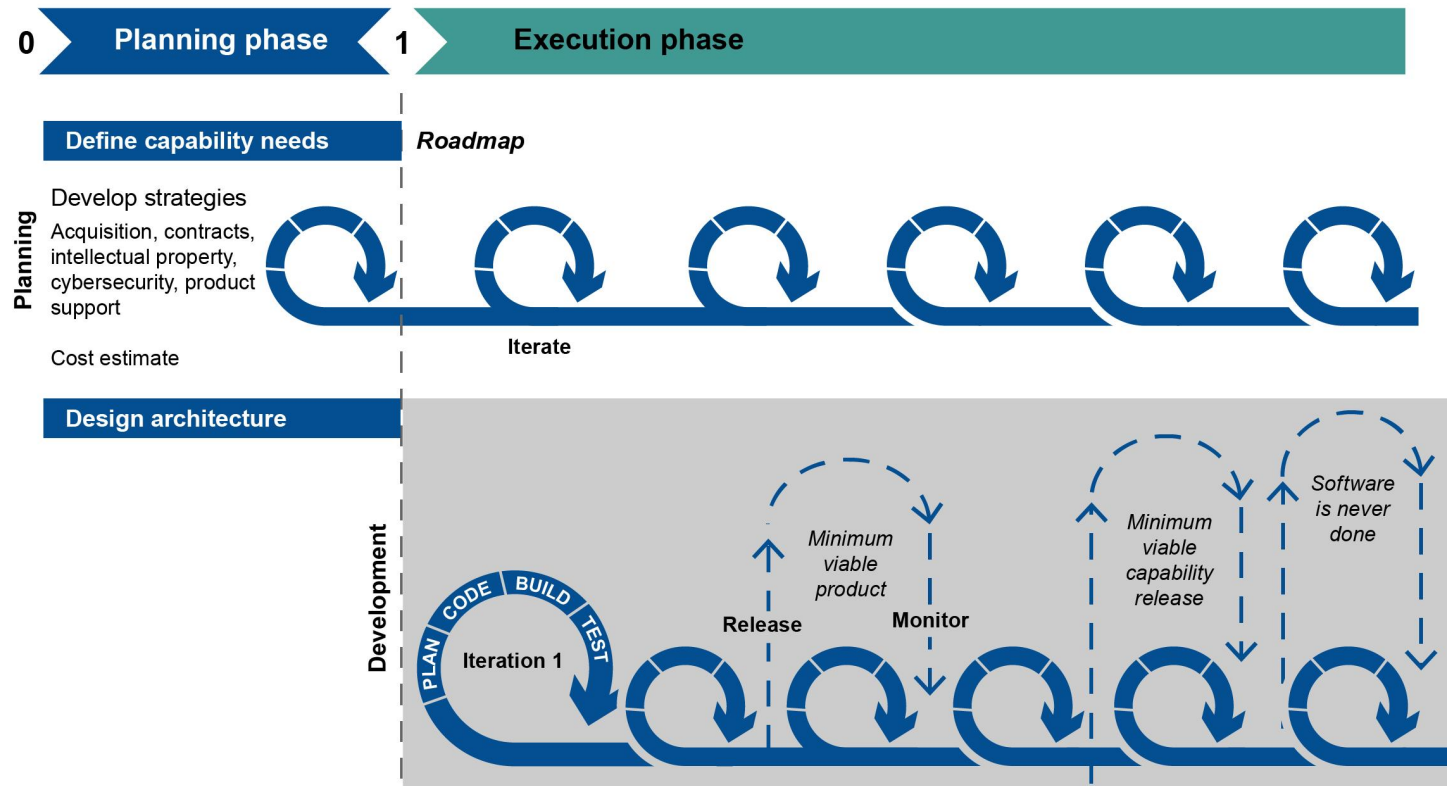
<sup>17</sup>National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 800, 133 Stat 1198, 1478 (Dec. 20, 2019).

<sup>18</sup>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).

<sup>19</sup>Throughout this report, we refer to steps DOD has taken to implement Agile software development. DOD has also developed resources for iterative development methodologies that are consistent with Agile, such as Development, Security, and Operations (DevSecOps), and that are not mutually exclusive. In this report, we discuss these under the category of Agile software development because they also support Agile development.



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



Source: GAO presentation of Department of Defense information. | GAO-24-106912

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

Agile is an iterative development approach in which software is delivered in increments throughout the project but built iteratively by refining or discarding portions as required based on user feedback. This includes delivering a minimum viable product that is an early version of the software to deliver or field basic capabilities to users to evaluate. Iterative development can allow program staff to catch errors quickly and continuously, integrate new code with ease, and obtain user feedback throughout the process. Consistent with studies recommending DOD’s transition toward Agile software development,<sup>20</sup> and to implement statutory mandates to

<sup>20</sup>Defense Science Board, *Design and Acquisition of Software*; Defense Innovation Board, *Software is Never Done*.

help enable its transition, the department has begun implementing Agile as part of its software modernization initiatives.<sup>21</sup>

As previously mentioned, updates to the business systems pathway and the creation of the software acquisition pathway were designed, in part, to enable Agile software development. Both pathways contain provisions that support this type of development. For example, a limited deployment in the business systems pathway can be similar to a minimum viable product in Agile development methodology, and the program team is 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.<sup>22</sup> DOD provided the participating pilot programs with training and tailored Agile guidance. The Section 874 pilot lasted 1 year, and DOD has shared lessons learned from the pilot related to the implementation of these practices. The Section 873 pilot targeted large acquisition programs and continued through FY 2023.

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

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 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.

In addition, DOD's DevSecOps guidance, which is based on Agile software development practices, includes required activities, such as in areas related to tracking customer satisfaction and progress of software development efforts.<sup>24</sup>

---

<sup>21</sup>Section 873 and 874 of the NDAA for FY 2018 established two Agile pilot programs, National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, §§ 873-874, 131 Stat. 1283, 1498-1503 (Dec. 12, 2017). Section 800 of the NDAA for FY 2020 established a software acquisition pathway that, according to DOD Instruction 5000.02, is to include support for Agile practices. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 800, 133 Stat. 1198, 1478 (Dec. 20, 2019). We reported on the implementation status of the section 873 and 874 pilots in [GAO-22-105230](#).

<sup>22</sup>Pub. L. No. 115-91, §§ 873-874, 131 Stat. 1283, 1498-1503 (Dec. 12, 2017).

<sup>23</sup>Department of Defense, *Department of Defense Software Modernization* (Washington, D.C.: Feb. 1, 2022).

<sup>24</sup>Department of Defense, *DevSecOps Fundamentals Guidebook*.

## DOD's Cybersecurity Guidance

DOD Instruction 8500.01 describes cybersecurity requirements for all DOD acquisition programs containing IT.<sup>25</sup> 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.<sup>26</sup> Under this instruction, all DOD IT systems must be categorized in accordance with Committee on National Security Systems Instruction 1253,<sup>27</sup> and implement a corresponding set of security controls and assessments from National Institute of Standards and Technology Special Publication 800-53.<sup>28</sup> 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.

## Requirements for DOD to Adopt Zero Trust Cybersecurity

A May 2021 executive order marked a commitment to, and prioritization of, federal cybersecurity modernization and strategy.<sup>29</sup> Among other policy mandates, the order required that agencies, including DOD, adopt cybersecurity best practices, which included developing a plan to implement a zero trust architecture.

In addition, the NDAA for FY 2022 directed DOD to develop a zero trust strategy, a model architecture, and implementation plans.<sup>30</sup> While the concepts behind zero trust are not new, the implications of shifting away from perimeter-based security are new to most enterprises and many federal agencies, including DOD.<sup>31</sup>

---

<sup>25</sup>Department of Defense, *Cybersecurity*, Instruction 8500.01 (incorporating change 1 [Oct. 7, 2019]) (Washington, D.C.: Mar. 14, 2014).

<sup>26</sup>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).

<sup>27</sup>Committee on National Security Systems, *Security Categorization and Control Selection for National Security Systems*, Instruction 1253 (Washington, D.C.: Mar. 27, 2014).

<sup>28</sup>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).

<sup>29</sup>The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

<sup>30</sup>Pub. L. No. 117-81, § 1528, 135 Stat. 1541, 2044-2048 (Dec. 27, 2021).

<sup>31</sup>Perimeter-based security refers to conventional network security practices in which, once a user is inside of an organization's network, that user is considered trusted and is often given broad access to multiple resources.

---

## DOD's Chief Management Officer Position Repealed by Statute and Responsibilities Reassigned

The NDAA for FY 2018 previously codified the position of Chief Management Officer (CMO) in Title 10 of the U.S. Code.<sup>32</sup> Additional responsibilities and functions for the CMO were enacted in the NDAA for FY 2019.<sup>33</sup> 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. 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, including its broad oversight for DOD's business systems. To address these changes, in September 2021, the Deputy Secretary of Defense directed an extensive realignment of the responsibilities previously assigned to the CMO.<sup>34</sup> These changes included the reassignment of the following responsibilities:

- Establishing the Defense Business Council (DBC), to provide advice to the Secretary of Defense on (1) developing the DOD business enterprise architecture (BEA), (2) reengineering department business processes, (3) developing and deploying defense business systems, and (4) developing requirements for defense business systems. This council, which was previously co-chaired by the CMO and DOD's CIO, is now chaired solely by DOD's CIO.
- Developing and maintaining DOD's BEA, to guide the development of integrated department business processes, is assigned to DOD's CIO.
- Issuing supporting guidance within respective areas of responsibility, for the coordination of and decision making for planning, programming, and control of investments in covered defense business systems, is assigned to the Under Secretary of Defense (Comptroller)/Chief Financial Officer and DOD's CIO, along with the Under Secretary of Defense for Acquisition and Sustainment and military department CMOs.

After 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.

The NDAA for FY 2023, which the President signed in December 2022, also included provisions to formally shift certain roles and responsibilities from the former CMO position to other DOD entities, consistent with the changes above. In addition, according to the new statute, DOD's CIO is to serve as the approval official for

---

<sup>32</sup>Pub. L. No. 115-91, § 910, 131 Stat. 1283, 1516-1519 (Dec. 12, 2017), codified at 10 U.S.C. § 132a.

<sup>33</sup>Pub. L. No. 115-232, § 921, 132 Stat. 1636, 1926-1929 (Aug. 13, 2018).

<sup>34</sup>Department of Defense, *Disestablishment of the Chief Management Officer, Realignment of Functions and Responsibilities, and Related Issues* (Washington, D.C.: Sept. 1, 2021).

priority defense business systems. The NDAA for FY 2024 made further amendments to eliminate the CMO position from relevant DOD requirements or to reassign responsibilities to other DOD officials.<sup>35</sup>

---

## The Federal IT Dashboard

A provision in what is commonly known as the Federal Information Technology Acquisition Reform Act requires that the Director of OMB make information on major federal IT investments of covered agencies (including DOD) publicly available,<sup>36</sup> in accordance with detailed OMB guidance.<sup>37</sup> 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.<sup>38</sup> However, OMB's guidance continues to include, and dictate many aspects of, the reporting requirements for IT investments and GSA provides supporting guidance for complying with the requirements.<sup>39</sup>

Additionally, while OMB provides guidance on designating major IT investments and reserves the right to designate them, it gives each covered agency the flexibility to establish specific criteria. According to officials from DOD's Office of the CIO and the department's guidance,<sup>40</sup> DOD's major IT investments include: (1) defense business systems with a budget greater than \$250 million across the future years defense plan;<sup>41</sup> (2) non-defense business systems with a budget greater than \$569 million across the future years defense plan; (3) IT investments designated as major by the DOD's CIO; and (4) major defense acquisition programs determined to be IT investments by DOD's CIO.<sup>42</sup>

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

---

<sup>35</sup>Pub. L. No. 118-31, § 901, 137 Stat. 136, 354 (Dec. 22, 2023).

<sup>36</sup>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).

<sup>37</sup>Office of Management and Budget, *Circular No. A-11*.

<sup>38</sup>GSA's FY 2019 budget justification included this change.

<sup>39</sup>FY 2024 reporting requirements for IT investments are contained in Section 55 of OMB's Circular No. A-11 guidance and in GSA's supporting guidance for submissions to the Dashboard. General Services Administration, *BY 2024 IT Collect Submission Overview*.

<sup>40</sup>Department of Defense, *FY 2024 IT/CA Budget Guidance Implementation I Guide A*.

<sup>41</sup>DOD's future years defense plan includes planned program costs over a 5-year period.

<sup>42</sup>Major defense acquisition programs generally include programs that are not highly sensitive or classified and DOD defines them as programs that are either (1) designated by the Secretary of Defense or (2) estimated to require, for all planned increments, an eventual total expenditure for research, development, testing, and evaluation of more than \$525 million in FY 2020 constant dollars or procurement of more than \$3.065 billion in FY 2020 constant dollars. See 10 U.S.C. § 4201(a); Department of Defense, *Major Capability Acquisition*, Instruction 5000.85, (Aug. 6, 2020) (Change 1 Effective Nov. 4, 2021) (reflecting statutory cost thresholds in FY 2020 constant dollars).

ratings should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals.

The public display of these data is intended to allow oversight bodies and the general public to hold agencies accountable for mission-related outcomes. We have issued a series of reports that noted the significant steps that OMB had previously taken to enhance the oversight, transparency, and accountability of federal IT investments by creating the Dashboard.<sup>43</sup> These reports also addressed issues with the accuracy and reliability of the Dashboard's data. Accordingly, we made recommendations to OMB to address these issues, which it implemented.

---

### GAO's Agile Assessment Guide

In December 2023, GAO issued its updated *Agile Guide* to help organizations assess their readiness to adopt Agile methods, as well as to enable assessment of an agency's use of these methods.<sup>44</sup> The Guide describes best practices, including metrics and management tools that programs are encouraged to use when pursuing Agile software development. Specifically, metrics are the data about a program's performance to help measure an organization's operations and results, while management tools can be used to help capture the metrics and support decision making.

---

### GAO Has Made Recommendations to Improve Management of DOD IT Systems

GAO has included DOD business systems in its High-Risk list and in a number of reports and has made multiple recommendations to improve the department's management of IT systems.

**DOD's business systems modernization efforts on GAO's High-Risk List.** DOD's business systems modernization efforts have been on GAO's High-Risk List since 1995, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments, including for its major IT programs.<sup>45</sup> GAO uses the High-Risk program to highlight government programs in need of transformation. As we reported in April 2023, DOD's efforts to develop an action plan to address high-risk areas had stalled since 2021. In September 2023, DOD described a revised approach for efforts underway to address the DOD business systems modernization high-risk area. These efforts included an action plan with tasks and associated milestones for updating its BEA. As of March 2024, there were 22 recommendations that DOD had not yet implemented associated with this high-risk area.

---

<sup>43</sup>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).

<sup>44</sup>[GAO-24-105506](#).

<sup>45</sup>For example, see GAO, *High-Risk Series*, [GAO-HR-95-1](#) (Washington, D.C.: Feb. 1, 1995) and additional work such as [GAO-23-106203](#) and [GAO-21-119SP](#).

**GAO reports on DOD's major IT business programs.** As part of our mandated work (which originates from the as amended provision in the NDAA for FY 2019 and is included in our High-Risk oversight area), we began a series of annual reports focused on the performance of DOD's major IT business programs. Three of the four reports included recommendations to DOD.

- **June 2021.** We reported on steps DOD was taking to collect and report acquisition program data.<sup>46</sup> For example, we found that DOD had not developed data strategies and had not finalized metrics for its business system and software acquisition pathways. We recommended that the department improve how it monitors its IT acquisitions by ensuring the data strategies and data collection efforts for the business system and software pathways use appropriate metrics to monitor acquisitions and assess performance. Although DOD provided a corrective action plan intended to help address the recommendation in February 2024, it did not fully demonstrate that the department completed these tasks and the recommendation has not yet been implemented.<sup>47</sup>
- **June 2022.** We reported on the performance reporting and cybersecurity and supply chain planning of DOD's major IT business programs.<sup>48</sup> Specifically, we found that not all of the programs fully reported operational performance measures to the Federal IT Dashboard, had approved cybersecurity strategies, or had supply chain risk management plans that addressed information and communications technology. We made three recommendations that DOD ensure the programs, as appropriate, (1) report operational performance measures in its reporting to the Federal IT Dashboard, (2) develop approved cybersecurity strategies, and (3) develop supply chain risk management plans that address information and communications technology. Although DOD concurred with GAO's recommendations and provided corrective action plans intended to help address the recommendations in September 2023, we determined that the department had not yet demonstrated that it completed all tasks needed to implement the recommendations as of March 2024.
- **June 2023.** We reported on the performance reporting and user training and deployment planning of DOD's major IT business programs.<sup>49</sup> Specifically, we found that not all of the programs identified at least the minimum required operational performance metrics in their reporting to the Federal IT Dashboard or had plans for conducting user training and deployment activities. We made two recommendations to DOD to ensure the programs, as appropriate, (1) identify the required operational performance metrics and (2) develop plans to conduct user training and deployment. Although DOD concurred with GAO's recommendations and provided corrective action plans intended to help address the recommendations in September 2023, we determined that the department had not yet demonstrated that it completed tasks needed to implement the recommendations as of March 2024.

**March 2023 report on DOD's financial management systems.** We reported on issues related to DOD's accounting for its physical assets and spending.<sup>50</sup> This included reporting on DOD's guidance for overseeing

---

<sup>46</sup>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).

<sup>47</sup>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 August 2023, DOD has taken some actions to implement the two recommendations from that report but neither has been implemented yet.

<sup>48</sup>GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, [GAO-22-105330](#) (Washington, D.C.: June 14, 2022).

<sup>49</sup>[GAO-23-106117](#).

<sup>50</sup>GAO, *Financial Management: DOD Needs to Improve System Oversight*, [GAO-23-104539](#) (Washington, D.C.: March 7, 2023).



its business and financial systems, the reliability of the data collected on business and financial system compliance with statutory requirements, and workforce planning. Specifically, we found that the department's guidance for initially approving and annually certifying business systems did not fully address statutory requirements, including auditability requirements. In addition, we found that the data collected on business and financial system compliance with statutory requirements was not reliable and that the department did not have a strategic approach to workforce planning for its financial systems.

We made nine recommendations, including that DOD fully develop guidance for overseeing business and financial systems. In addition, we recommended that the department ensure that the data collected on business and financial system compliance with statutory requirements are reliable and that DOD implement a strategic approach to workforce planning. DOD concurred with seven of the recommendations and partially concurred with the remaining two. As of January 2024, three recommendations had been partially addressed while the remaining six had not yet been implemented. GAO reiterates the need for DOD to address previous recommendations focused on improving IT systems, including business and financial systems.

---

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

According to DOD's FY 2024 Federal IT Dashboard data, the department's planned expenditures for 21 selected IT business programs amounted to \$9.1 billion from FY 2022 through FY 2024, with the four largest programs accounting for just over half of the planned cost of the portfolio. Additionally, 70 percent of the total cost across the 3 years was for operating and maintaining the systems and 30 percent was for development and modernization.

Officials for 15 of the 21 business programs reported experiencing cost or schedule changes since January 2022.<sup>51</sup> This included 13 programs that reported cost increases ranging from \$0.5 million to \$1.3 billion (a median of \$163.3 million) and seven programs that reported schedule delays ranging from 15 months to 36 months (a median of 24 months). Four of these programs also reported rebaselining or expecting to rebase as a result of the changes. The program officials provided a variety of reasons for the changes, including new requirements and unanticipated technical complexities.

In addition, programs reported mixed progress on performance in DOD's FY 2024 Dashboard data. Specifically, four programs reported meeting all performance targets, 10 reported meeting at least one target, and one reported meeting none. However, the other six programs did not report on any targets,<sup>52</sup> as required

---

<sup>51</sup>As part of our previous reviews, we have reported on cost and schedule changes experienced by DOD's major IT business programs prior to January 2022. See [GAO-23-106117](#), [GAO-22-105330](#), and [GAO-21-351](#).

<sup>52</sup>Of these six programs, DOD officials stated that one did not identify any metrics because it was in an earlier stage of the system life cycle and did not yet have operational measures. Performance data for another program was not included in DOD's reporting to the Dashboard because the department did not list it as a major investment for FY 2024.



by OMB.<sup>53</sup> We have previously reported on DOD IT business programs not fully reporting performance metrics data and made two recommendations to the department to do so.<sup>54</sup>

## DOD’s Planned Costs for the 21 Selected Business Programs Amounted to \$9.1 Billion from FY 2022 through FY 2024

According to DOD’s FY 2024 Federal IT Dashboard data, the department’s planned expenditures for the 21 selected IT business programs amounted to \$9.1 billion from FY 2022 through FY 2024. Specifically, DOD reported \$3 billion in actual costs for the 21 programs in FY 2022 and \$6.1 billion in planned costs for the programs between FY 2023 and FY 2024. Table 1 shows the department’s actual and planned costs for the 21 programs during the 3-year period.

**Table 1: The Department of Defense’s (DOD) Actual and Planned Costs for 21 Selected IT Business Programs from Fiscal Year (FY) 2022 through FY 2024**

Dollars in millions

| Program  | FY 2022 (actual) | FY 2023 (projected) | FY 2024 (requested) | 3-year total |
|--|------------------|---------------------|---------------------|--------------|
| DOD Healthcare Management System Modernization                             | 955              | 797                 | 539                 | 2,291        |
| Navy Enterprise Resource Planning  | 418              | 441                 | 574                 | 1,433        |
| Distribution Standard System   | 127              | 158                 | 168                 | 453          |
| Defense Enterprise Accounting and Management System                        | 143              | 138                 | 157                 | 438          |
| Global Combat Support System-Army  | 158              | 149                 | 129                 | 435          |
| Joint Operational Medicine Information Systems                             | 87               | 80                  | 248                 | 416          |
| Navy Personnel and Pay   | 99               | 120                 | 142                 | 361          |
| Navy Maritime Maintenance Enterprise Solution                              | 120              | 114                 | 122                 | 355          |
| Enterprise Business System   | 69               | 126                 | 160                 | 355          |
| General Fund Enterprise Business System                                    | 141              | 112                 | 96                  | 348          |
| Defense Agencies Initiative  | 103              | 107                 | 137                 | 347          |
| Naval-Maintenance, Repair, and Overhaul                                    | 76               | 105                 | 76                  | 257          |
| Real-Time Automated Personnel Identification System and Common Access Card | 62               | 89                  | 102                 | 253          |
| Defense Enrollment Eligibility Reporting System                            | 76               | 78                  | 78                  | 231          |
| Military Health System Information Platform                                | 55               | 85                  | 88                  | 228          |
| Global Combat Support System-Marine Corps/Logistics Chain Management       | 69               | 69                  | 71                  | 209          |
| Theater Medical Information Program-Joint Increment 2                      | 77               | 73                  | 14                  | 163          |
| Naval Air Systems Command Aviation Logistics Environment                   | 44               | 58                  | 55                  | 157          |
| Air Force Integrated Personnel and Pay System                              | 37               | 47                  | 51                  | 135          |

<sup>53</sup>Office of Management and Budget, *Circular No. A-11*. FY 2024 reporting requirements for IT investments are contained in Section 55 of OMB’s guidance and in GSA’s supporting guidance for complying with OMB’s submission requirements. General Services Administration, *BY 2024 IT Collect Submission Overview*.

<sup>54</sup>GAO-22-105330 and GAO-23-106117.

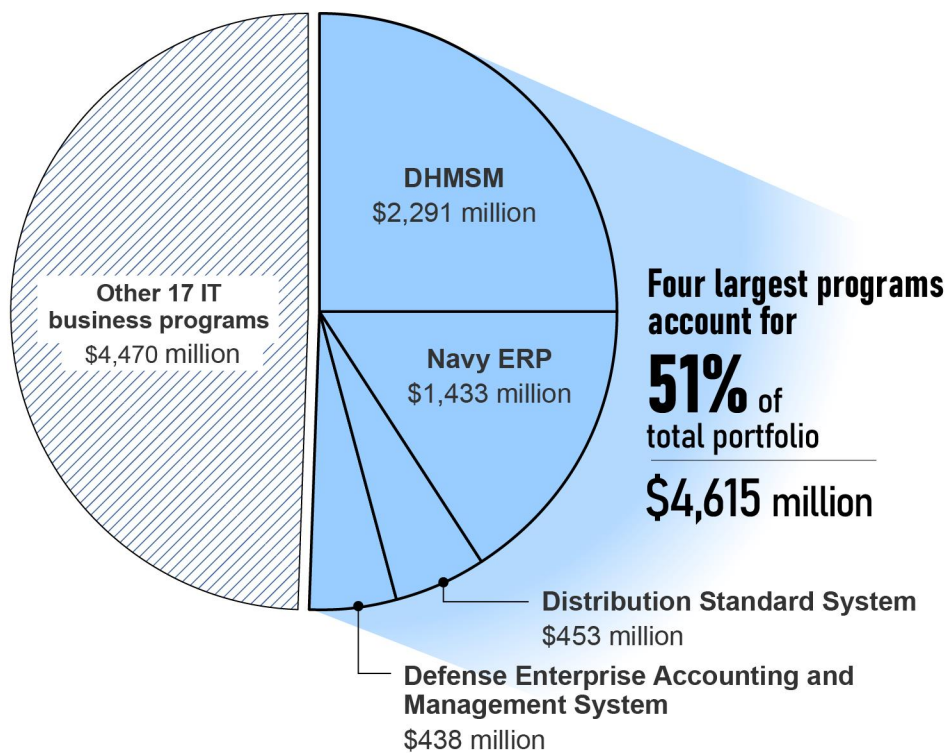
| Program                            | FY 2022 (actual) | FY 2023 (projected) | FY 2024 (requested) | 3-year total |
|------------------------------------|------------------|---------------------|---------------------|--------------|
| Defense Travel System              | 39               | 39                  | 40                  | 118          |
| Navy Electronic Procurement System | 29               | 39                  | 33                  | 101          |
| <b>Total</b>                       | <b>2,983</b>     | <b>3,023</b>        | <b>3,079</b>        | <b>9,086</b> |

Source: GAO analysis of DOD's FY 2024 Federal IT Dashboard data. | GAO-24-106912

Note: Numbers do not always add due to rounding.

The four largest programs—DOD Healthcare Management System Modernization (DHMSM), Navy Enterprise Resource Planning (Navy ERP), Distribution Standard System (DSS), and Defense Enterprise Accounting and Management System (DEAMS)—accounted for \$4.6 billion (51 percent) of the total \$9.1 billion in planned costs for this portfolio of 21 programs from FY 2022 through FY 2024. Figure 3 shows DOD's planned costs for the four largest programs compared to the portfolio of 21 during the 3-year period.

**Figure 3: The Department of Defense's (DOD) Planned Costs for the Four Largest IT Business Programs Compared to the Remaining 17 Selected Programs from Fiscal Year (FY) 2022 through FY 2024**



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

Source: GAO analysis of DOD's FY 2024 Federal IT Dashboard data. | GAO-24-106912

Based on officials' responses to our questionnaire, these four programs are collectively in more mature stages of their program life cycles. DHMSM and DEAMS officials each reported most recently achieving full deployment ATP, with their next milestone being capability support ATP. Navy ERP and DSS officials each reported achieving capability support ATP and remaining in sustainment.

Further, during the 3-year period, DOD's costs for operations and sustainment (O&S)<sup>55</sup> accounted for 70 percent (\$6.4 billion) of the total reported \$9.1 billion in planned cost for the 21 programs, with the other 30 percent (\$2.7 billion) for development, modernization, and enhancement (DME). These programs include "legacy" systems and the average age of all 21 systems is 17 years.<sup>56</sup> We have previously reported on DOD's spending on operating and maintaining systems (e.g., legacy systems), in lieu of spending on development,<sup>57</sup> and that a small number of aging systems can drive portfolio cost growth and put agencies at higher risk of wasteful spending.<sup>58</sup> Also see appendix II for summaries of all 21 programs, which include breakdowns of each program's planned costs for operating and maintaining the systems compared to for development.

---

## Programs Reported Experiencing Cost and Schedule Changes

In addition to our prior reporting on cost and schedule changes,<sup>59</sup> officials for 15 of the selected 21 DOD IT business programs reported experiencing cost or schedule changes since January 2022. Figure 4 shows the programs that reported cost or schedule changes and the direction of the changes.

---

<sup>55</sup>*Operations and sustainment* is a term used by DOD to describe a stage of the program life cycle equivalent to operations and maintenance.

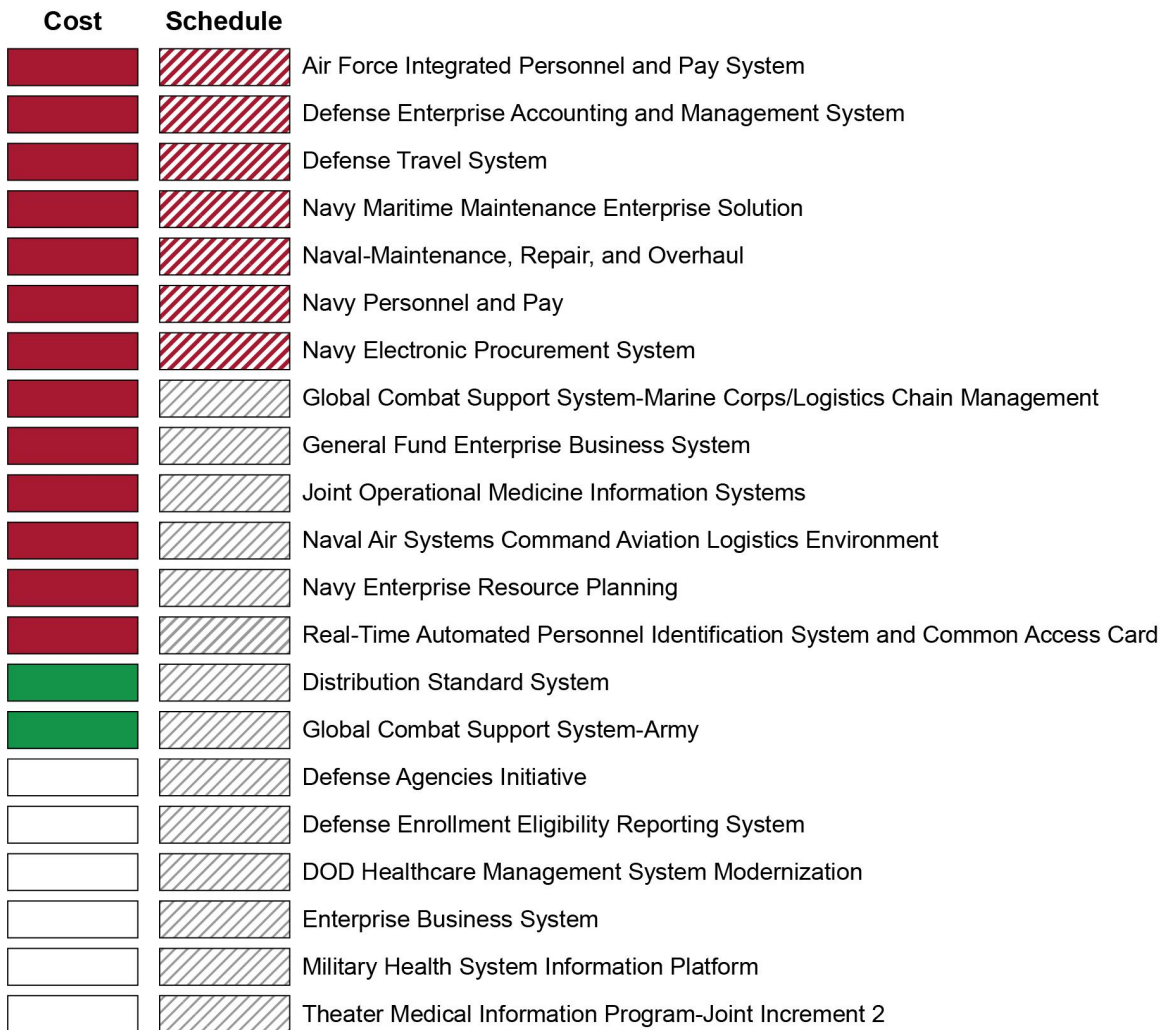
<sup>56</sup>According to DOD, a legacy business system is a system that the department plans to retire within 36 months. Department of Defense, *Defense Business Systems Investment Management Guidance*, Version 4.1 (Washington, D.C.: June 26, 2018). Based on this definition, these systems include Distributed Standard System (DSS) and Navy Enterprise Resource Planning (Navy ERP).

<sup>57</sup>See, for example, GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, [GAO-16-468](#) (Washington, D.C.: May 25, 2016).

<sup>58</sup>GAO, *Weapon Systems Annual Assessment: Limited Use of Knowledge-Based Practices Continues to Undercut DOD's Investments*, [GAO-19-336SP](#) (Washington, D.C.: May 7, 2019).

<sup>59</sup>See [GAO-23-106117](#), [GAO-22-105330](#), and [GAO-21-351](#).

**Figure 4: Selected Department of Defense (DOD) IT Business Programs Reported Cost and Schedule Changes Since January 2022**



Source: GAO analysis of DOD program questionnaire responses as of February 2024. | GAO-24-106912

Officials for 15 programs reported cost changes. Among these, 13 programs reported cost increases ranging from \$0.5 million to \$1.3 billion (a median of \$163.3 million) and two programs reported decreases ranging from \$15.5 million to \$40 million (a median of \$27.8 million). Officials for seven programs reported schedule delays ranging from 15 months to 36 months (a median of 24 months).

Officials for three of the largest four programs mentioned earlier, DEAMS, DSS, and Navy ERP, each reported changes to their planned costs or schedules. Regarding these programs:

- DEAMS officials reported a schedule delay of 24 months toward achieving its capability support ATP decision, from December 2022 to January 2024, and an associated cost increase of \$221.6 million. The program officials attributed the changes to addressing cybersecurity vulnerabilities, updating and modernizing products, and the effects of inflation.
- DSS officials reported experiencing an estimated cost decrease of \$40 million due to requirements being shifted and hosting costs being reduced with the implementation of the Warehouse Management System, the new system that is intended to replace and modernize DSS. The officials also reported experiencing cost changes due to the reshaping of the new system's schedule, but stated that they could not currently quantify the full life cycle cost differences as they have added capabilities that did not exist in the legacy software. They added that the changes will be clarified as the program's modernization strategy is further developed. The officials attributed the changes to the COVID-19 pandemic, which resulted in policy and guidance changes impacting the program's ability to travel and deploy software to the distribution centers within the Defense Logistics Agency supply chain throughout 2021. In addition, program officials cited issues with contracts and the existing workforce.
- Navy ERP officials reported experiencing a cost increase for the legacy financial system, but stated that they could not quantify it at the time of our reporting. The officials attributed the increase to the replacement of an enterprise software solution, which will no longer be supported after 2030, with the Navy ERP technical software solution. They also stated that they were in the process of finalizing the new estimate and that it would include an additional 2 years of cost. The officials added that the new solution is intended to employ a modern enterprise IT service that will help meet Navy's unique financial, audit, and supply requirements.

#### Four Programs Rebaselined or Expected to Rebaseline

Officials for four of the DOD IT business programs that reported cost and schedule changes reported rebaselining or expecting to rebaseline as a result of the changes.<sup>60</sup> Repeated rebaselines may indicate that programs are not appropriately managing cost, schedule, or performance expectations or are experiencing other issues.<sup>61</sup> For example, repeated rebaselines might indicate other challenges, such as unexpected technical complexity or issues with program contractors. Specifically, the two programs that rebaselined reported the following:

- Air Force Integrated Personnel and Pay System (AFIPPS). AFIPPS officials reported that changes in the program's baseline were driven by its new acquisition strategy approved in March 2022, the development of manpower saving requirements for process automation, and technical challenges related to system configurations. The officials stated that these changes were associated with a cost increase that they were not able to provide a specific amount for at the time of our reporting and an extension of the program's schedule by 31 months. They added that the program still needed to have an assessment of the change in cost completed and needed to gain approval of the new cost estimate.

---

<sup>60</sup>OMB guidance states that agencies and contractors should establish a performance measurement baseline to track progress and report cost and schedule variance. Rebaselines are any revision to the investment's baseline and should be reviewed and approved according to agency governance processes.

<sup>61</sup>Increased costs or extended schedules in updated baselines that reflect additional work directed to programs are not necessarily indicative of the programs mismanaging their originally required work. For example, these could be instances where the program has new requirements as a result of being directed by DOD to provide their services to additional customers.

- Naval-Maintenance, Repair, and Overhaul (N-MRO). N-MRO officials reported rebaselining as a result of schedule delays in program deployment. The program officials reported that operational schedule concerns, additional cybersecurity testing needed to support compatibility with multiple legacy systems, and software stability issues caused the delays of 15 to 18 months, moving the deployment from the second quarter of FY 2023 to the third or fourth quarter of FY 2024. The officials also reported an associated cost increase of \$400 million to support the needed requirements to be included in the enterprise system.

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

- Defense Travel System (DTS). DTS officials reported expecting to rebaseline due to the cancellation of the MyTravel program, which was intended to replace the legacy travel system, as well as the archival system for DOD's travel modernization initiatives. The officials stated that this resulted in DTS, which was previously planned to be retired by FY 2027, being expected to support DOD travel for a minimum of at least 5 more years, an extension of the program's schedule by at least 24 months. They added that the total increase currently anticipated for the program across the next 5 years was \$68.4 million.
- Navy Electronic Procurement System (Navy EPS). Navy EPS officials reported experiencing a schedule delay of 15 months and expecting to rebaseline as a result of a change in contracting strategy and the execution of activities to compete and award the contract. The officials also reported a cost increase of \$310 million due to the program's updated cost estimate including additional years and including the costs of additional capabilities and integration efforts required for program completion.

Program officials for the 15 programs that reported cost or schedule changes and rebaselines or expected rebaselines collectively provided a variety of reasons for the changes, including workforce and contractor issues, new or unplanned requirements, and cloud migration or modernization developments. Additionally, officials reported cybersecurity issues, unanticipated technical complexities, the effects of inflation, and supply chain disruptions as reasons for changes. Later in this report, we discuss key challenges reported by program officials related to software development and cybersecurity and actions programs and DOD officials reported taking to address them.

---

## Most Programs Reported Mixed Progress Toward Achieving Goals

OMB requires DOD to submit current information on the performance of major IT investments to the Federal IT Dashboard.<sup>62</sup> Specifically, according to OMB's Circular No. A-11 guidance, the department is to report on the performance of the programs in meeting their business or mission purpose. This includes operational analysis, which is a method of examining the ongoing performance of an operating asset investment and measuring that performance against an established set of cost, schedule, and performance goals. Additionally, GSA's supporting guidance for complying with OMB's IT investment submission requirements specifies that the programs are to identify a minimum of five performance metrics. These metrics should best reflect the value of the investment and be consistent with the following four categories:<sup>63</sup>

---

<sup>62</sup>Office of Management and Budget.

<sup>63</sup>FY 2024 reporting requirements for IT investments are contained in Section 55 of OMB's Circular No. A-11 guidance and in GSA's supporting guidance for submissions to the Dashboard. General Services Administration, *BY 2024 IT Collect Submission Overview*.

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

The fifth metric, or more as programs may report more than five metrics, can come from any of the four categories. Further, programs are required to use the performance metrics they identified to measure progress toward achieving their goals. Specifically, the guidance states that program submissions must include actual results data for all of the identified metrics.

### Most Programs Reported Mixed Progress on Performance Metrics, while Some Did Not Fully Report Required Performance Data

Of the 21 selected IT business programs, 19 identified the minimum required number of performance metrics in DOD's FY 2024 Federal IT Dashboard data.<sup>64</sup> Of these 19 programs, four reported meeting all performance targets, 10 reported meeting at least one target,<sup>65</sup> and one reported meeting none. The six other programs did not report on any targets, including two that did not identify the required metrics.<sup>66</sup>

In total, the 19 programs identified 108 metrics (an average of 5.7 metrics per program) consistent with OMB's guidance.<sup>67</sup> Figure 5 shows programs' reported performance metrics and progress toward achieving their goals.

---

<sup>64</sup>DOD CIO officials stated that one program, N-MRO, did not identify any metrics because it was in an earlier stage of the system life cycle and did not yet have operational measures. Performance data for the other program, DTS, was not included in DOD's reporting to the Dashboard because the department did not list it as a major investment for FY 2024.

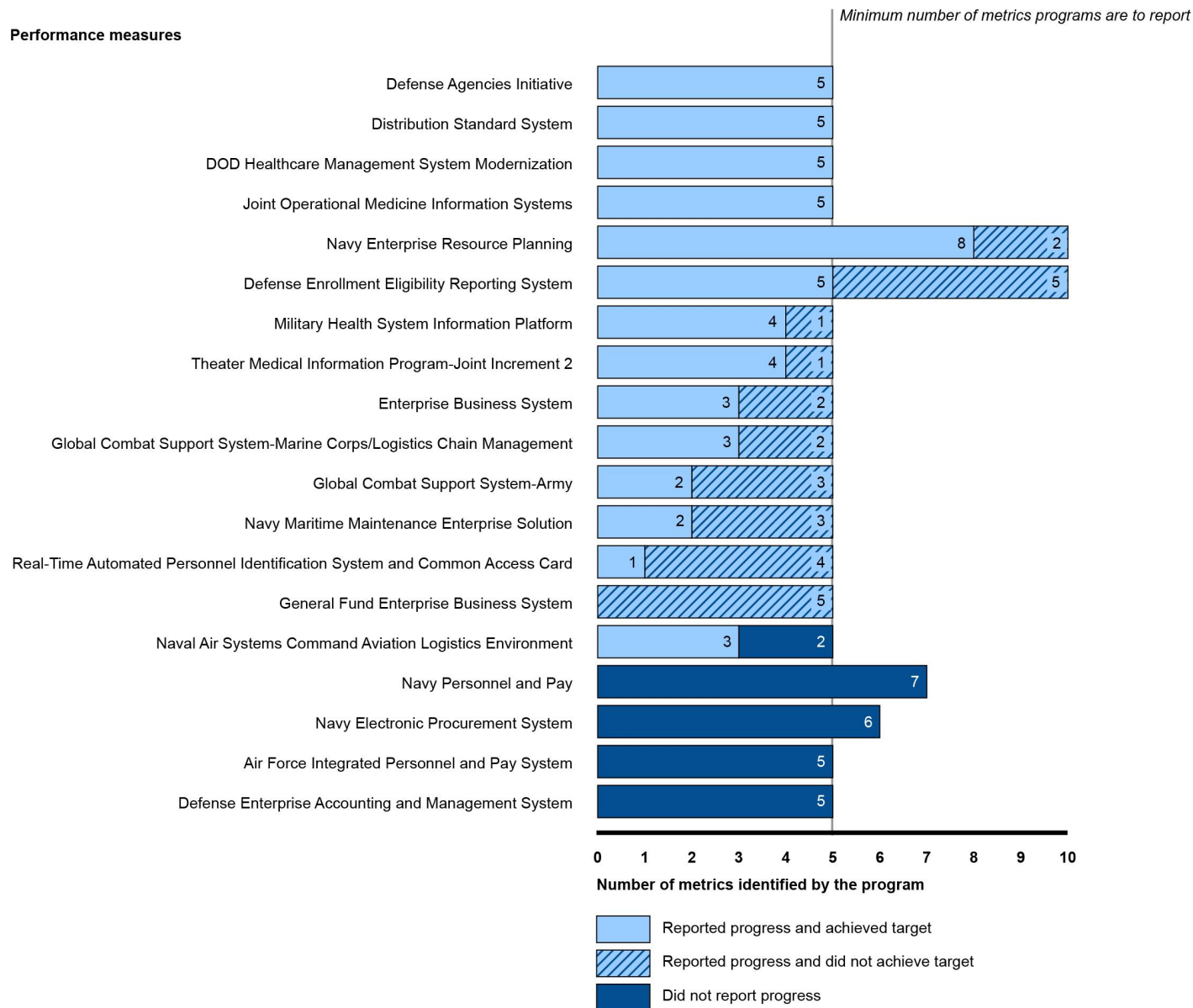
<sup>65</sup>One of these 10 programs reported achieving three of its targets but did not report progress against its other two targets.

<sup>66</sup>In our 2022 report ([GAO-22-105330](#)), we determined that 19 major IT business programs had not fully reported data indicating progress they were making toward achieving 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 reporting to the Federal IT Dashboard, and DOD concurred. Further, in our 2023 report, we found that 13 programs had not fully reported the performance measures and reiterated the importance of ensuring they do so.

<sup>67</sup>In our 2023 report ([GAO-23-106117](#)), we determined that three of DOD's major IT business programs had not identified the minimum required number of operational performance metrics. We recommended that the DOD CIO ensure these programs identify the required metrics, as appropriate, in the department's reporting to the Dashboard, and DOD concurred.



**Figure 5: Selected Department of Defense (DOD) IT Business Programs' Performance Measures**



Source: GAO analysis of DOD's fiscal year 2024 Federal IT Dashboard data. | GAO-24-106912

**Accessible Data for Figure 5: Selected Department of Defense (DOD) IT Business Programs' Performance Measures**

| Number of Reported Metrics                     | Reported achieved | Reported not achieved | Did not report |
|--|-------------------|-----------------------|----------------|
| Defense Agencies Initiative                    | 5                 | 0                     | 0              |
| Distribution Standard System                   | 5                 | 0                     | 0              |
| DOD Healthcare Management System Modernization | 5                 | 0                     | 0              |
| Joint Operational Medicine Information Systems | 5                 | 0                     | 0              |



| Number of Reported Metrics   | Reported achieved | Reported not achieved | Did not report |
|--|-------------------|-----------------------|----------------|
| Navy Enterprise Resource Planning  | 8                 | 2                     |                |
| Defense Enrollment Eligibility Reporting System                            | 5                 | 5                     |                |
| Military Health System Information Platform                                | 4                 | 1                     |                |
| Theater Medical Information Program-Joint Increment 2                      | 4                 | 1                     |                |
| Enterprise Business System   | 3                 | 2                     |                |
| Global Combat Support System-Marine Corps/Logistics Chain Management       | 3                 | 2                     |                |
| Global Combat Support System-Army  | 2                 | 3                     |                |
| Navy Maritime Maintenance Enterprise Solution                              | 2                 | 3                     |                |
| Real-Time Automated Personnel Identification System and Common Access Card | 1                 | 4                     |                |
| General Fund Enterprise Business System                                    |                   | 5                     |                |
| Naval Air Systems Command Aviation Logistics Environment                   | 3                 |                       | 2              |
| Navy Personnel and Pay   |                   |                       | 7              |
| Navy Electronic Procurement System   |                   |                       | 6              |
| Air Force Integrated Personnel and Pay System                              |                   |                       | 5              |
| Defense Enterprise Accounting and Management System                        |                   |                       | 5              |

Source: GAO analysis of DOD's fiscal year 2024 Federal IT Dashboard data. | GAO-24-106912

In our 2023 report, officials from DOD's Office of the CIO acknowledged that the programs should be fully reporting the required performance data and stated that DOD's CIO put audit checks in place that should improve program reporting, but that some programs still had incomplete reporting because the checks were made incrementally and had only been partially implemented. The officials added that they expected the checks to be fully implemented before the department's FY 2024 submission to the Dashboard in June 2023; however, we found that gaps in the performance reporting remained in the FY 2024 data. While DOD has made progress toward addressing our prior recommendations that programs identify the required metrics and report measures against their metrics, programs continue to not fully report the required performance data.

In March 2024, officials from DOD's Office of the CIO acknowledged that gaps remained in the FY 2024 performance reporting and stated that they had implemented additional checks to address these issues going forward. The officials added that this should ensure full reporting by the programs when they submit the FY 2025 data by June 2024. Full performance reporting will help improve the programs' accountability and assist the department and Congress in effectively overseeing program performance.

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

As of February 2024, officials for all 10 (of the 21) selected DOD IT business programs that we identified as actively developing software reported using recommended Agile and iterative approaches and practices,<sup>68</sup> as

<sup>68</sup>For the purposes of this assessment, we considered programs to be actively developing software if officials reported they were actively developing new software functionality.

recommended by the Defense Science Board.<sup>69</sup> However, in areas related to tracking customer satisfaction and progress of software development, four of the 10 programs did not use metrics and management tools required by DOD and consistent with ones identified in GAO's *Agile Guide*,<sup>70</sup> or did not provide documentation. Additionally, while all of the 21 programs reported conducting a variety of cybersecurity testing and assessments, several programs did not have an approved cybersecurity strategy,<sup>71</sup> as required by DOD.<sup>72</sup>

Program officials reported facing a variety of key challenges related to software development and cybersecurity, including changing requirements, and leadership and staff turnover. Officials also reported program and DOD efforts to address these challenges, which included programs working with customers to clarify expectations and the department coordinating to implement its software modernization strategy.

---

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

As of February 2024, officials for all 10 (of the 21) selected DOD IT business programs that we identified as actively developing software reported using recommended Agile and iterative approaches and practices, as recommended by the Defense Science Board.<sup>73</sup> For example, officials for each of the 10 programs reported delivering a minimum viable product (i.e., an early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on). Nine of the 10 programs reported delivering software functionality every 6 months or less, as called for in OMB guidance.<sup>74</sup>

However, in areas related to tracking customer satisfaction and progress of software development efforts, four of the 10 programs did not use metrics and management tools required by DOD and consistent with ones identified in GAO's *Agile Guide*, or did not provide documentation demonstrating their use.

### All 10 Programs Actively Developing Software Reported Using Recommended Iterative Approaches

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). An iterative software development approach is a way of breaking down the development of large applications into smaller pieces or increments that reflect updates based on user feedback. The board assessed that the iterative approach to software development is applicable to DOD

---

<sup>69</sup>Defense Science Board, *Design and Acquisition of Software*. The Defense Science Board provides independent advice and recommendations on science, technology, manufacturing, acquisition process, and other matters of special interest to the Secretary of Defense.

<sup>70</sup>[GAO-24-105506](#).

<sup>71</sup>We have previously reported on major DOD IT business programs not having an approved cybersecurity strategy, which included recommending they each develop one in [GAO-22-105330](#) and reiterating the importance of doing so in [GAO-23-106117](#).

<sup>72</sup>Department of Defense, Instruction 8500.01 and Instruction 5000.89.

<sup>73</sup>Officials for all 10 programs reported using Agile or iterative approaches that align with Agile, such as DevSecOps.

<sup>74</sup>OMB, Memorandum M-15-14.

and should be adopted as quickly as possible. Table 2 describes the recommended iterative software development approaches.

**Table 2: Iterative Software Development Approaches Recommended by the Defense Science Board**

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

Source: GAO analysis of Defense Science Board Information. | GAO-24-106912

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 an iterative software development approach may reduce cost growth compared to a Waterfall approach.<sup>75</sup>

As of February 2024, officials for all 10 (of the 21) selected DOD IT business programs that we identified as actively developing software reported using one of,<sup>76</sup> or a mix of, the recommended iterative approaches that could result in cost or schedule benefits.<sup>77</sup> This included all of the 10 programs reporting the use of Agile or DevSecOps.

### All 10 Programs Reported Using a Variety of Recommended Practices that Support Iterative Development

The Defense Science Board also recommended that DOD implement certain practices that support continuous, iterative software development. Officials for each of the 10 programs actively developing software reported using a variety of the recommended iterative practices. For example, officials for all 10 programs reported delivering a minimum viable product. In addition, nine of the 10 programs reported conducting

---

<sup>75</sup>Defense Innovation Board, *Software Is Never Done*.

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

<sup>77</sup>The 10 programs that we identified as actively developing software included Air Force Integrated Personnel and Pay System, Defense Enterprise Accounting and Management System, Global Combat Support System-Army, General Fund Enterprise Business System, JOMIS, Naval Air Systems Command Aviation Logistics Environment, Navy Electronic Procurement System, Navy ERP, N-MRO, and NP2.

iterative development training for program managers and staff. Table 3 describes the iterative development practices that programs reported using.

**Table 3: The Selected Department of Defense (DOD) IT Business Programs Actively Developing Software Reported Using Recommended Iterative Practices**

| Practice  | Description   | Number of programs that reported using practice |
|---|---|---|
| Delivery of a minimum viable product, followed by successive next viable product                  | An early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on  | 10 of 10  |
| Software documentation provided at each production milestone                                      | Written text or illustrations that accompany computer software or are embedded in the source code   | 9 of 10   |
| Iterative development training for program managers and staff                                     | The development of a training curriculum to create and train a cadre of software-informed program managers, sustainers, and software acquisition specialists      | 9 of 10   |
| Use of a software factory for development   | A low-cost, cloud-based computing technique used to assemble a set of software tools enabling developers, users, and management to work together on a daily basis | 2 of 10   |
| Establishment of a software factory as a key evaluation criterion in the source selection process | The development of a software factory as a factor in evaluating proposals for a potential government contractor   | 0 of 10   |

Source: GAO analysis of DOD program questionnaire responses as of February 2024. | GAO-24-106912

Further, the Defense Science Board recommended establishing the creation of a software factory as a key evaluation criterion in the source selection process for software development and called for programs to transition to the use of a software factory. Officials from DOD’s Office of the CIO stated that the reason the majority of these programs reported not conducting these practices is because the business systems heavily leverage commercial off-the-shelf products to deliver their services. There has been a DOD-wide effort to transition programs to using software factories and this practice supports programs developing their own code for software, such as for weapon systems.

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

OMB guidance calls for certain agency CIOs and chief acquisition officers to ensure and certify that acquisition strategies and plans apply adequate incremental development.<sup>78</sup> OMB defines incremental development as planned and actual delivery of new or modified technical functionality to users at least every 6 months. Additionally, the Defense Innovation Board calls for program staff using Agile and DevSecOps practices to deliver working software to users on a continuing basis—as frequently as every week. According to the Defense Innovation Board, if program officials do not allow for more frequent software delivery, they may lose opportunities to obtain information from users and may face challenges adjusting requirements to meet customer needs.

<sup>78</sup>OMB, Memorandum M-15-14. OMB’s guidance applies to agencies covered by the Chief Financial Officers Act and their divisions and offices, except where otherwise noted. At DOD, the Under Secretary of Defense for Acquisition and Sustainment is the chief acquisition officer.

Officials for nine of the 10 programs in active development reported delivering software functionality every 6 months or less, as called for in OMB’s guidance. Officials for the remaining program, AFIPPS, reported that the average length of time between software releases was 10 to 12 months.

**Four of the 10 Programs Did Not Use Required Agile Metrics and Management Tools or Did Not Provide Documentation**

DOD’s *Agile Metrics Guide* includes guidance for Agile development teams related to actionable metrics for Agile products and services and identifies key metrics, such as those related to the efficiency, quality, and value of the work being provided.<sup>79</sup> The *Guide* states that it is meant to be a starting point and that the metrics should be tailored for the unique considerations of the program. In addition, DOD’s guidebook for DevSecOps activities and tools includes required activities that all programs using the DevSecOps approach must use to meet DOD’s criteria, such as in areas related to tracking customer satisfaction and progress of software development efforts.<sup>80</sup>

Also, as mentioned earlier in this report, GAO’s *Agile Guide* discusses various metrics and management tools that programs are encouraged to use when pursuing Agile software development.<sup>81</sup> These metrics and management tools are used to measure performance and outcomes intended to help meet customer needs and are best practices for Agile adoption and implementation. Additionally, the *Guide* describes management tools that programs may use to help capture the metrics and support decision making. Several of these metrics and management tools are consistent with ones required in DOD’s guidance.

Officials for the 10 selected DOD IT business programs actively developing software and using Agile, and iterative approaches consistent with Agile, used various metrics and management tools identified in GAO’s *Agile Guide*. Table 4 shows the Agile metrics that the DOD IT business programs reported using. Table 5 shows the Agile management tools that the DOD IT business programs demonstrated using.

**Table 4: The Selected Department of Defense (DOD) IT Business Programs Reported Using Metrics Identified in GAO’s *Agile Assessment Guide***

| Metric  | Description  | Number of programs that reported using metric |
|---|--|---|
| Number of defects or bugs                       | The number of defects identified after deploying a product into the production environment                   | 10 of 10                                      |
| Customer satisfaction                           | The level of satisfaction measured by customers and monitored throughout the development cycle               | 9 of 10                                       |
| Time required to restore service after outage   | A measure of time to restore service after an outage   | 9 of 10                                       |
| Features or user stories <sup>a</sup> delivered | The number of user stories completed in an iteration and whether any were carried over to the next iteration | 8 of 10                                       |

<sup>79</sup>Department of Defense, *Agile Metrics Guide; Strategy Considerations and Sample Metrics for Agile Development Solutions*, Version 1.2 (Washington, D.C.: Nov. 11, 2020).

<sup>80</sup>Department of Defense, *DevSecOps Fundamentals Guidebook*.

<sup>81</sup>[GAO-24-105506](#).

| Metric  | Description   | Number of programs that reported using metric |
|---|---|---|
| Time required for full regression test                          | A measure of time to complete a full regression test  | 8 of 10                                       |
| Velocity  | The volume of work accomplished in a specific time by a team, compared against a metric that quantifies the work developers can deliver in each iteration                     | 7 of 10                                       |
| Metrics that measure a team's adherence to Agile best practices | A measure of a team's effort to adhere to Agile software development practices  | 7 of 10                                       |
| Cumulative flow   | The flow of work over a period of time represented by a cumulative flow diagram or by reporting the number of features or capabilities delivered in each iteration or release | 6 of 10                                       |

Source: GAO analysis of DOD program questionnaire responses as of February 2024. | GAO-24-106912

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

**Table 5: The Selected Department of Defense (DOD) IT Business Programs Demonstrated Using Management Tools Identified in GAO's Agile Assessment Guide**

| Management tool            | Description  | Number of programs that demonstrated using tool |
|----------------------------|--|---|
| Sprint backlog             | An ordered list of tasks to be accomplished during the sprint  | 8 of 10   |
| Product backlog            | A high-level backlog that contains all the requirements for the entire program                                       | 8 of 10   |
| Release plan               | A plan that identifies different sets of usable functionality or products scheduled for delivery to the customer     | 6 of 10   |
| Burn up or burn down chart | A visual tool displaying progress via a simple line chart representing work accomplished or remaining work over time | 5 of 10   |
| Cumulative flow diagram    | An analytical tool that allows teams to visualize their effort and a program's progress                              | 5 of 10   |
| Budget baseline            | A cost baseline used to measure program performance  | 4 of 10   |

Source: GAO analysis of DOD program questionnaire responses as of February 2024. | GAO-24-106912

However, of the 10 programs, four that reported using DevSecOps did not use metrics and management tools required of these programs by DOD and consistent with ones identified in GAO's *Agile Guide*, or did not provide documentation demonstrating their use. Specifically, of the four programs, three did not use cumulative flow or a cumulative flow diagram, two did not use release plans, one did not track customer satisfaction and one did not provide documentation demonstrating its use of a product backlog.

Programs that did not use these required Agile metrics and management tools, or did not provide documentation demonstrating their use, reported a variety of reasons for not doing so. These included the programs being in early stages of development or of Agile implementation, not yet establishing the management tools, and not having access to the tools or to certain features within the tools. In March 2024, Office of the DOD CIO and A&S officials acknowledged that the adoption of modern software approaches like Agile and DevSecOps and the related practices are still fairly new to DOD and stated that, as more programs adopt and mature these practices, the use of the metrics and tools will increase.

By not ensuring that programs use the required metrics and management tools, the department is at risk of not having complete information to measure performance and progress of its Agile software development efforts to meet customer needs.

### Programs Reported Conducting Cybersecurity Testing and Assessments, but Continued to Lack Required Strategies

DOD Instruction 5000.89 requires that DOD IT program staff complete developmental and operational cybersecurity testing.<sup>82</sup> According to DOD’s *Cybersecurity Test and Evaluation Guidebook*,<sup>83</sup> developmental testing is intended to identify cybersecurity issues and vulnerabilities early in the system life cycle to facilitate the remediation and reduction of impact on cost, schedule, and performance. Operational testing is intended to provide information that helps identify vulnerabilities, describe operational effects of discovered vulnerabilities, and resolve operational cybersecurity issues.

Officials for all 21 of the selected IT business programs reported conducting developmental cybersecurity testing, operational cybersecurity testing, or both. Programs may have conducted certain types of cybersecurity testing and not others due, in part, to being in different phases of the system life cycle. For example, systems in an earlier life cycle phase may conduct developmental testing, but may not be mature enough to conduct operational testing. Table 6 summarizes the types of cybersecurity testing that the programs reported conducting.

**Table 6: The Selected Department of Defense (DOD) IT Business Programs Reported Conducting Developmental and Operational Cybersecurity Testing**

| Testing phase         | Description  | Number of programs that reported conducting testing |
|-----------------------|--|---|
| Developmental testing | Identifies cybersecurity vulnerabilities before program deployment to help remediate vulnerabilities and reduce the risk of negative impacts on cost, schedule, or performance | 18 of 21  |
| Operational testing   | Evaluates operational programs’ cybersecurity for effectiveness, suitability, and survivability  | 15 of 21  |

Source: GAO analysis of DOD program questionnaire responses as of February 2024. | GAO-24-106912

Additionally, DOD Instructions 5000.75 and 5000.90 require IT program staff to conduct cybersecurity assessments.<sup>84</sup> The assessments are included in programs’ cybersecurity testing processes and, according to the *Test and Evaluation Guidebook*, are intended to identify and mitigate exploitable system vulnerabilities.

Officials for each of the 21 programs also reported conducting some form of cybersecurity assessment. For example, a majority of the programs reported conducting full system assessments, table top exercises, and

<sup>82</sup>Department of Defense, Instruction 5000.89.

<sup>83</sup>Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0.

<sup>84</sup>Department of Defense, *Business System Requirements and Acquisition*, Instruction 5000.75; Department of Defense, *Cybersecurity for Acquisition Decision Authorities and Program Managers*, Instruction 5000.90 (Washington D.C.: Dec. 31, 2020).

penetration tests.<sup>85</sup> Several programs also reported conducting other types of cybersecurity assessments, such as static code and privacy impact assessments.

### Several Programs Did Not Have an Approved Cybersecurity Strategy

DOD Instruction 8500.01, *Cybersecurity*, and DOD Instruction 5000.89 require that DOD IT program officials use an approved cybersecurity strategy.<sup>86</sup> This strategy is to include information such as cybersecurity and resilience requirements and key system documentation for cybersecurity testing and evaluation analysis and planning. Such information is intended to ensure that program staff plan for and document cybersecurity risk management efforts, which begin early in the programs' life cycle.

In our June 2022 report, we found that 10 of DOD's major IT business programs had not demonstrated having an approved cybersecurity strategy.<sup>87</sup> We recommended that DOD's CIO ensure that these programs develop such a strategy, as appropriate, and DOD concurred with our recommendation. Further, in our June 2023 report, we also found that six of the department's major IT business programs lacked an approved strategy and reiterated the importance of ensuring that these programs develop one.<sup>88</sup>

As of February 2024, several programs did not have an approved strategy.<sup>89</sup> Officials for the programs reported planning to develop such a strategy by 2025 or stated that they follow other DOD cybersecurity and risk management framework guidance.

In March 2024, DOD officials acknowledged that the programs should have an approved cybersecurity strategy. Officials stated that they were continuing to take actions to address the recommendation by following up with the programs that did not provide such a strategy to ensure that they develop one.

The officials added that the department provides the programs with guidance on developing a cybersecurity strategy, including in DOD's June 2021 cybersecurity outline and guide, and that it was in the process of updating its guidance to reflect comprehensive revisions to the adaptive acquisition framework for the business systems that follow its pathways. Further, they stated that several of the programs they followed up with had developed draft strategies and were in the process of getting them approved by leadership.

Ensuring that approved strategies are in place should help position the programs to effectively manage cybersecurity risks and mitigate threats. Doing so should also reduce the risk of adverse impacts on cost, schedule, and performance.

---

<sup>85</sup>Full-system assessments are performed on a complete system to evaluate its compliance with specified requirements. Table top exercises involve small teams who discuss how they would respond to various simulated emergency or rapid response situations and prepare briefings on potential threat scenarios and responses. Penetration tests involve independent assessors typically working under specific constraints, who attempt to circumvent or defeat the security features of an information system.

<sup>86</sup>Department of Defense, Instruction 8500.01 and Instruction 5000.89 (Nov. 19, 2020).

<sup>87</sup>[GAO-22-105330](#).

<sup>88</sup>[GAO-23-106117](#).

<sup>89</sup>We did not evaluate the content of these cybersecurity strategies.



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

Officials among the 21 selected IT business programs included in our review reported facing a number of key challenges associated with software development and cybersecurity and collectively reported actions taken by the programs to address them. Table 7 summarizes the reported challenges and actions taken by the programs.

**Table 7: The Selected Department of Defense (DOD) IT Business Programs Reported Key Software Development and Cybersecurity Challenges and Actions to Address Them**

| Challenge  | Reported action taken by programs to address challenge   | Number of programs that reported challenge |
|--|--|--|
| Budget constraints   | <ul style="list-style-type: none"> <li>Working with sponsors to acquire additional funds</li> <li>Working with requirements owner to reprioritize requirements</li> </ul>                                | 12 of 21                                   |
| Changing customer requirements   | <ul style="list-style-type: none"> <li>Regularly updating program roadmaps</li> <li>Working with customers to adjust expectations</li> </ul>   | 9 of 21                                    |
| Rapidly evolving cybersecurity requirements  | <ul style="list-style-type: none"> <li>Regularly scanning and monitoring cybersecurity requirements</li> <li>Structuring sustainment contract(s) to respond to new cybersecurity requirements</li> </ul> | 7 of 21                                    |
| Technical issues related to software development and commercial off-the-shelf software | Revising licensing needs and requesting resources to mitigate costs of upgrading software licenses   | 5 of 21                                    |
| Leadership and staff turnover  | Communicating staffing needs to appropriate officials  | 5 of 21                                    |

Source: GAO analysis of DOD program questionnaire responses as of February 2024. | GAO-24-106912

Additionally, in March 2024, officials in DOD’s Office of the CIO and A&S officials provided information about the department’s efforts to address the identified challenges:

- Officials acknowledged that **budget constraints** remain a challenge. They stated that DOD continues to emphasize the importance of defense business systems to the department’s mission and the importance of prioritizing business systems modernization appropriately while also supporting the warfighter as DOD’s top priority.
- Officials stated that the department was addressing **changing customer requirements, rapidly evolving cybersecurity requirements, and technical issues related to software development and commercial off-the-shelf software**, in part through their coordination efforts with DOD’s A&S and Office of the Under Secretary for Research and Engineering to implement the department’s software modernization strategy. Specifically, these efforts include the programs’ transition to using DevSecOps as the preferred software development approach and continued adoption of Agile practices. Officials added that, through programs’ continued adoption of these practices, addressing these challenges can be built into planned work and addressed much more quickly than through traditional software development approaches.
- Officials stated that the department was making efforts to address **leadership and staff turnover** by providing leadership and staff with the knowledge and skills needed to understand modern software

development (e.g., related to adopting Agile and DevSecOps). In addition, the officials stated that DOD added new work roles for software engineering, data, and artificial intelligence to the department's cyber workforce framework and that the department provides related training to the existing workforce.

For additional information on the 21 DOD 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 to Implement Legislative and Policy Changes

DOD continues to make efforts to improve its management of IT investments as a result of legislative and policy changes. These efforts include revising its business systems investment management guidance, modernizing its business enterprise architecture (BEA), and adopting zero trust cybersecurity.

Officials from DOD's Offices of the Director of Administration and Management and CIO described a revised approach for the department's efforts to implement changes associated with its defense business systems investment management guidance and the DOD BEA. Specifically, those efforts include the following:

**Defense business systems investment management guidance.** We previously reported that DOD's CIO planned to issue a revised investment management guide by May 31, 2023. Subsequently, in September 2023, DOD's Office of the CIO updated its plans to issue the revised guide by June 30, 2024. This guide is to incorporate the results of a portfolio manager survey to improve the department's business process re-engineering efforts. DOD's CIO also prioritized the issuance of the FY 2024 annual certification guidance and is documenting potential investment management processes to incorporate into the investment management guide.<sup>90</sup> The annual certification guidance is related to both statutory requirements and minimum documentation substantiating compliance requirements for priority business and financial systems.<sup>91</sup>

In support of the above efforts, in January 2024, DOD described that the Office of the CIO developed a roadmap detailing key actions and milestones to enhance the department's ability to manage its portfolio of defense business systems. For example, DOD is implementing a data-driven decision-making platform to determine defense business system compliance with DOD policy and priorities to drive auditable investment decisions and enable rationalization opportunities.

**Business enterprise architecture modernization.** We previously reported that DOD's CIO indicated plans for the department to publish a BEA modernization strategy and a new BEA by June 30, 2023. Subsequently, the framework was signed and published in January 2024. In addition, in March 2024, DOD reported that DOD's CIO plans to publish a BEA guidebook by September 30, 2024.

---

<sup>90</sup>Department of Defense, *Fiscal Year 2024 Defense Business Systems Annual Certification Guidance* (Washington, D.C.: July 31, 2023).

<sup>91</sup>Our March 2023 report, [GAO-23-104539](#), focuses on DOD financial management systems and discusses guidance for business systems. We reported on our evaluation of the department's existing guidance, which showed that it 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 does not describe how systems are to demonstrate system compliance or how decision makers are to substantiate it.

- The framework establishes DOD’s modernization approach and highlights component roles and responsibilities for BEA development, maintenance, and usage. DOD further elaborated that the framework is a high-level document intended to establish a federated, question-based, and data-centric architecture.
- The guidebook is to detail BEA governance, roles, and responsibilities, use cases, use of enterprise-level tools, and development best practices. In January 2024, DOD further elaborated that the guidebook will build upon the framework and is to provide the instruction necessary to develop and maintain a modernized BEA.

However, we reported in our 2023 High-Risk List report that the department has not taken consistent and sustained steps toward completing these planned actions and has again revamped its efforts.<sup>92</sup> Addressing these critical areas could assist DOD to achieve better cost, schedule, and performance outcomes; manage its portfolio of business system investments more effectively and efficiently; and help identify and address potential duplication and overlap.

**Zero trust cybersecurity:** As previously mentioned in this report, a May 2021 executive order requires DOD to adopt zero trust cybersecurity, including developing a plan to implement a zero trust architecture.<sup>93</sup> In addition, the NDAA for FY 2022 directed the department to develop a zero trust strategy, a model architecture, and implementation plans.<sup>94</sup> In response, DOD has established an office and published several documents that will guide the agency’s efforts to adopt zero trust principles in the coming years. Specifically, in January 2022, the department established the zero trust Portfolio Management Office within DOD’s Office of the CIO to accelerate its adoption of zero trust. Subsequently, the department published the following documents:

- In July 2022, DOD updated its *Zero Trust Reference Architecture*.<sup>95</sup> This document is to be the authoritative source of information used to guide the agency in implementing a zero trust framework. In addition, the *Reference Architecture* outlines an end-state vision and strategy for developing a data-centric approach to strengthen cybersecurity.
- In October 2022, the department published *its Zero Trust Strategy*.<sup>96</sup> The strategy describes the necessary guidance for advancing zero trust concept development, including requirements development, procurement, and deployment of required capabilities and activities.
- In January 2023, DOD published the *Zero Trust Capability Execution Roadmap – Course of Action 1 (COA 1)*.<sup>97</sup> Additionally, to accelerate zero trust adoption, the department is developing complementary capability roadmap courses of action, including those that will cover commercial and government-owned cloud-based enterprise services (i.e., COA 2 and COA 3, respectively). The capability roadmap courses of action will lay out the department’s vision for achieving zero trust target levels by progressively

---

<sup>92</sup>GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

<sup>93</sup>The White House, *Improving the Nation’s Cybersecurity*, Executive Order 14028.

<sup>94</sup>Pub. L. No. 117-81, § 1528, 135 Stat. 1541, 2044-2048 (Dec. 27, 2021).

<sup>95</sup>Department of Defense, *Zero Trust Reference Architecture*, Version 2.0 (July 2022). Version 1.0 was published in February 2021, before the May 2021 executive order.

<sup>96</sup>Department of Defense, *DOD Zero Trust Strategy* (Oct. 21, 2022).

<sup>97</sup>Department of Defense, *DOD Zero Trust Capability Execution Roadmap (COA 1)* (Jan. 06, 2023).

implementing outcomes and activities.<sup>98</sup> The COA 1 roadmap describes a timeline where all DOD organizations achieve the planned zero trust targets by 2027.

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).<sup>99</sup> Additionally, we will monitor DOD's efforts associated with its business systems modernization, approach to business transformation high-risk areas, and adoption of zero trust cybersecurity.

---

## Conclusions

Several DOD IT business programs reported experiencing cost increases and schedule delays and reported mixed progress on performance. Six programs did not fully report performance data, as required by OMB. In addition, several programs did not have an approved cybersecurity strategy, as required by DOD. Implementation of prior recommendations to address performance reporting and cybersecurity planning is essential to improving program accountability and reducing the risk to DOD of adverse impacts on cost, schedule, and performance.

Four of the programs developing software did not demonstrate use of Agile metrics and management tools, as required by DOD and consistent with GAO's *Agile Guide*. Addressing this issue is essential to ensuring that DOD has sound information on its software development efforts.

---

## Recommendation for Executive Action

We are making one recommendation to the Department of Defense that the Secretary direct the Chief Information Officer and Under Secretary of Defense for Acquisition and Sustainment to ensure that IT business programs developing software use the metrics and management tools required by DOD and consistent with those identified in GAO's *Agile Assessment Guide*.

---

## Agency Comments

DOD provided written comments on a draft of this report, which are reproduced in appendix III. In its comments, the department concurred with our recommendation to ensure that IT business programs developing software use the metrics and management tools required by DOD and consistent with those identified in GAO's *Agile Assessment Guide*. The department stated that the DOD CIO would include guidance on metrics and management tools for Agile development in its next Software Modernization Implementation Plan. We will monitor DOD's actions in response to our recommendation.

---

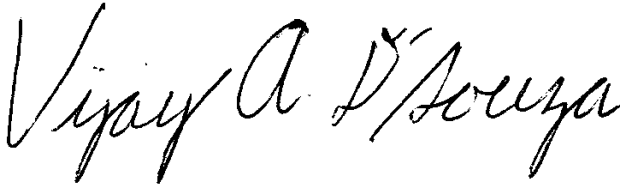
<sup>98</sup>A Zero Trust target level includes the minimum set of capability outcomes and activities necessary to secure and protect DOD's data, applications, assets, and services to manage risks from currently known threats. It is the level set by the department's Zero Trust Portfolio Management Office, which all of DOD must minimally achieve.

<sup>99</sup>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. See GAO, *Defense Management: Action Needed to Advance Progress on Reform Efforts*, [GAO-24-105793](#) (Washington, D.C.: Oct. 18, 2023).

We also requested that DOD assess the sensitivity of the document, and we made changes to remove information that the agency determined to be sensitive. DOD subsequently concurred that the report was suitable for public release.

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

If you or your staff members have any questions on matters discussed in this report, please contact me at (202) 512-7650 or [dsouzav@gao.gov](mailto: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

*List of Committees*

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 the cost, schedule, and performance of selected Department of Defense (DOD) IT business programs, (2) assess the extent to which DOD has implemented key software development and cybersecurity practices for selected programs, and (3) describe DOD actions to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, we selected 21 IT business programs for review,<sup>1</sup> including 20 business programs that DOD listed as major IT investments in its fiscal year (FY) 2024 Federal IT Dashboard (Dashboard) data.<sup>2</sup> We added an additional business program to our review, the Defense Travel System, based on it being previously designated as major, continuing to have high annual costs (e.g., the total requested amount exceeded \$30 million), and having an important role in DOD's mission, consistent with Office of Management and Budget (OMB) guidance for designating major investments.<sup>3</sup> We also selected the program due to officials reporting significant changes to its plans, including the department extending its use of the system at least an additional 5 years.<sup>4</sup>

We analyzed the Dashboard data to examine DOD's planned costs for the 21 selected IT business programs during the 3-year period from FY 2022 through FY 2024, including a breakdown of the costs for operating and maintaining the systems compared to for development and modernization.

To assess and ensure the reliability of the budget data DOD reported on the Federal IT Dashboard, we compared the data to cost information and supporting documentation provided by program officials to identify any obvious inconsistencies. In addition, we prepared and sent summaries to the 21 program offices and asked program staff to review them to confirm their accuracy. The 21 program summaries are included in appendix II. We also met with officials in DOD's Office of the Chief Information Officer (CIO) and asked them to validate program cost information included in the report. We determined that the cost data were sufficiently reliable for our reporting purposes.

We also analyzed program officials' responses to a questionnaire we developed and administered to all 21 programs in September 2023. Officials provided their responses and we followed up with programs through February 2024. The questionnaire addressed such issues as whether (1) programs had experienced cost or schedule changes since January 1, 2022 and (2) programs had rebaselined or expected to rebaseline as a

---

<sup>1</sup>DOD classifies these programs as defense business systems.

<sup>2</sup>The Federal IT Dashboard (Dashboard) is a public, government website operated by the General Services Administration (GSA) at <https://itdashboard.gov>. It includes streamlined data on IT investments to enable agencies and Congress to better understand and manage federal IT portfolios. We initially considered 21 business programs that DOD listed as major IT investments in its FY 2024 reporting to the Dashboard. We excluded one of the programs based on the department reporting no planned expenditures for it in FY 2024, planning to retire the system, and no longer considering it to be a major investment.

<sup>3</sup>Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (Washington, D.C.: Aug. 15, 2022).

<sup>4</sup>The changes to the program's plans were a result of DOD cancelling the intended new system known as MyTravel. GAO, *Defense Management: DOD Challenges with Travel Programs and Business Process Reforms*, [GAO-23-106945](https://www.gao.gov/products/23-106945) (Washington, D.C.: July 26, 2023).

result of the changes.<sup>5</sup> Additionally, we collected and analyzed supporting documentation, including key program documents pertaining to each program's life cycle cost, schedule estimates, and baselines (e.g., acquisition program baseline reports).

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 a pretest of the questionnaire with one program to ensure that the questions were clear, unbiased, and would be consistently interpreted. The pretest allowed us to obtain initial program feedback and helped ensure that officials within each program would understand the questions. We 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 analyzed programs' performance metrics data included in DOD's FY 2024 reporting to the Dashboard and compared the data to OMB guidance.<sup>6</sup> We also met with officials in the department's Office of the CIO to determine reasons for differences between how the performance data were reported and guidance for such reporting.

To assess and ensure the reliability of the programs' performance metrics data, we compared the data to performance metrics documentation provided by the programs to identify any obvious inconsistencies. We also met with officials in DOD's Office of the CIO 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 practices used by the 21 programs via our questionnaire, including 10 programs that we identified as actively developing software.<sup>7</sup> We aggregated the program office responses to our questionnaire and compared the information to relevant guidance and best practices (e.g., Defense Science Board and Defense Innovation Board reports, DOD instructions, and OMB guidance) to identify where there were gaps.<sup>8</sup> In addition, we collected and analyzed key information and supporting documents related to the programs' reported practices, including their use of metrics and management tools identified in GAO's *Agile Assessment Guide (Agile Guide)* and

---

<sup>5</sup>OMB's guidance states that agencies and contractors should establish a performance measurement baseline to track progress and report cost and schedule variance. Rebaselines are any revision to the investment's baseline and should be reviewed and approved according to agency governance processes.

<sup>6</sup>FY 2024 reporting requirements for IT investments are contained in Section 55 of OMB's Circular No. A-11 guidance and in GSA's supporting guidance for complying with OMB's submission requirements. General Services Administration, *BY 2024 IT Collect Submission Overview* (Washington, D.C.: January 27, 2023).

<sup>7</sup>For the purposes of this assessment, we considered programs to be actively developing software if officials reported that they were actively developing new software functionality. Officials for the other 11 programs reported either that their software development efforts were to sustain existing functionality, involved minor enhancements, or that they were not actively developing software.

<sup>8</sup>Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75, Incorporating Change 2, Jan. 24, 2020 (Washington, D.C.: Feb. 2, 2017); Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense, *Test and Evaluation*, Instruction 5000.89 (Nov. 19, 2020); OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (Washington, D.C.: June 10, 2015).



development of approved cybersecurity strategies and compared it to DOD's guidance.<sup>9</sup> In doing so, we identified risks associated with not following the guidance and best practices that may affect acquisition outcomes relative to cost, schedule, and performance. For programs that did not follow the guidance or demonstrate having such documentation, we followed up with program officials and officials in DOD's Office of the CIO and the Office of the Under Secretary of Defense for Acquisition and Sustainment (A&S) for reasons why they did not do so.

Further, we obtained information from program officials about key challenges the programs were facing related to software development and cybersecurity and actions these programs reported taking to mitigate them. We also obtained information from officials in DOD's Office of the CIO and A&S officials about actions the department was taking to address the challenges.

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 DOD actions to implement previously identified legislative and policy changes that could affect its IT acquisitions.<sup>10</sup> In addition, we reviewed DOD actions to implement recent legislative requirements (i.e., its efforts to adopt zero trust cybersecurity).<sup>11</sup> More specifically, the objective focused on DOD's planned improvements to the department's IT portfolio management (i.e., updates to its investment management guidance and business enterprise architecture) and actions it has taken to adopt zero trust principles, such as developing a zero trust strategy. To assess the actions DOD has taken toward implementation of these changes, we requested and reviewed policies, plans, and guidance provided by DOD; reports that the department submitted to Congress; and internal program documentation. We also met with officials in DOD's Office of the CIO to discuss their efforts in these areas and coordinated with the GAO team conducting a companion assessment examining weapon system acquisition programs.<sup>12</sup>

We conducted this performance audit from June 2023 to July 2024 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.

---

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

<sup>10</sup>The previously identified legislative and policy changes are discussed in GAO, *IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Development Planning*, [GAO-23-106117](#) (Washington, D.C.: June 13, 2023).

<sup>11</sup>Zero trust is a set of cybersecurity principles that are founded on the concept that no actor, system, network, or service operating outside of or within an organization's security perimeter should be trusted. Instead, the principles suggest that organizations must verify anything that attempts to establish access to their systems, services, and networks.

<sup>12</sup>[GAO-24-106831](#).

## Appendix II: Program Summaries

This appendix provides summaries of the 21 selected Department of Defense (DOD) IT business programs included in our review. Each summary provides key information about the program, including the program's planned expenditures and reported software development practices. These programs are:

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

---

### Air Force Integrated Personnel and Pay System (AFIPPS)

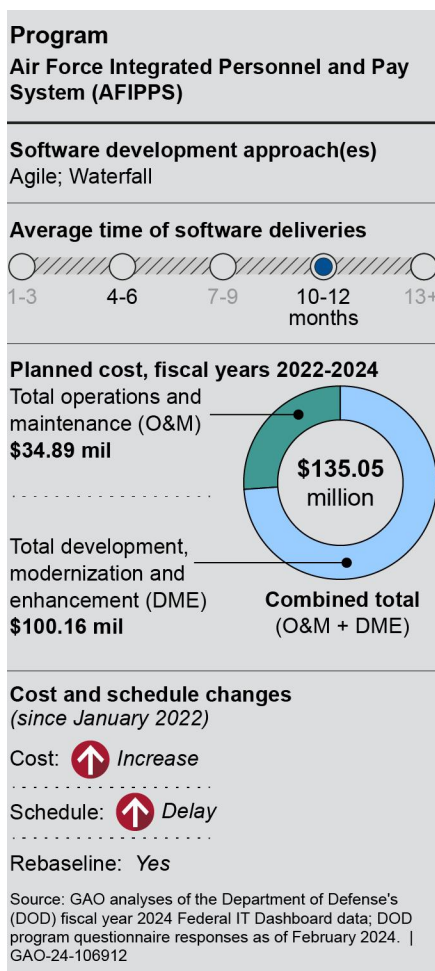
#### Program description

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

#### Program essentials (reported by DOD officials as of February 2024)

Appendix II: Program Summaries

- Lead DOD component: Air Force
- Program owner: Air Force
- Year investment began: 2009
- Acquisition pathway: Defense business systems acquisition
- Last milestone achieved: Acquisition authority to proceed (ATP)
- Next planned milestone: Limited deployment ATP
- Chief Information Officer (CIO) evaluation rating: 3 – Medium risk
- Year investment is estimated to reach end of useful life: 2036



**Table 8: Air Force Integrated Personnel and Pay System's (AFIPPS) Reported Software Development Approaches and Practices**

| Approach or practice                     | Program response |
|--|------------------|
| Developing new software functionality    | Yes              |
| Use of an iterative development approach | Yes              |

---

**Appendix II: Program Summaries**

---

| <b>Approach or practice</b>                                   | <b>Program response</b> |
|---|-------------------------|
| Software development approach                                 | Agile; Waterfall        |
| Delivery of a minimum viable product                          | Yes                     |
| Software documentation provided at each production milestone  | Yes                     |
| Iterative development training for program managers and staff | Yes                     |
| Use of a software factory                                     | No                      |
| Use of commercial off-the-shelf products                      | Yes                     |
| Software releases to date                                     | 0                       |
| Planned releases  | 2                       |
| Average time between releases                                 | 10-12 months            |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Defense Agencies Initiative (DAI)

### Program description

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 improved decision-making. The initiative is a critical part of the department's financial management modernization efforts.

### Program essentials (reported by DOD officials as of February 2024)

|  |   |                                |
|--|---|--------------------------------|
| Lead DOD component:<br>Defense-wide                            | Program owner:<br>Defense Logistics Agency (DLA)    | Year investment began:<br>2017 |
| Acquisition pathway:<br>Defense business systems acquisition   | Last milestone achieved:<br>Limited deployment ATPs |                                |
| Next planned milestone:<br>Limited deployment ATPs             | CIO evaluation rating:<br>5 – Low risk              |                                |
| Year investment is estimated to reach end of useful life: 2035 |   |                                |

**Table 9: Defense Agencies Initiative's (DAI) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response |
|---|------------------|
| Developing new software functionality                         | No               |
| Use of an iterative development approach                      | Yes              |
| Software development approach                                 | Incremental      |
| Delivery of a minimum viable product                          | Yes              |
| Software documentation provided at each production milestone  | Yes              |
| Iterative development training for program managers and staff | No               |
| Use of a software factory                                     | No               |
| Use of commercial off-the-shelf products                      | Yes              |
| Software releases to date                                     | 5                |
| Planned releases  | 7                |
| Average time between releases                                 | 10-12 months     |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Defense Enrollment Eligibility Reporting System (DEERS)

### Program description

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

### Program essentials (reported by DOD officials as of February 2024)

|  |  |                                |
|--|--|--------------------------------|
| Lead DOD component:<br>Defense-wide                          | Program owner:<br>Defense Health Agency (DHA)      | Year investment began:<br>1978 |
| Acquisition pathway:<br>Defense business systems acquisition | Last milestone achieved:<br>Capability support ATP |                                |

Appendix II: Program Summaries

|   |   |
|---|---|
| Next planned milestone:<br>N/A (program is in sustainment)                    | CIO evaluation rating:<br>3 – Medium risk |
| Year investment is estimated to reach end of useful life: No current end date |   |

**Program**  
**Defense Enrollment Eligibility Reporting System (DEERS)**

---

**Software development approach(es)**  
 Agile; Waterfall; Development, Security, and Operations (DevSecOps)

---

**Average time of software deliveries**

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

---

**Planned cost, fiscal years 2022-2024**

Total operations and maintenance (O&M)  
**\$231.14 mil**

**\$231.14 million**

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

**Combined total (O&M + DME)**

---

**Cost and schedule changes**  
*(since January 2022)*

Cost: No change

Schedule: No change

Rebaseline: No

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 10: Defense Enrollment Eligibility Reporting System's (DEERS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response  |
|---|---|
| Developing new software functionality                         | No  |
| Use of an iterative development approach                      | Yes   |
| Software development approach                                 | Agile; Development, Security, and Operations (DevSecOps); Waterfall |
| Delivery of a minimum viable product                          | No  |
| Software documentation provided at each production milestone  | Yes   |
| Iterative development training for program managers and staff | No  |
| Use of a software factory                                     | No  |

| Approach or practice                     | Program response  |
|--|---|
| Use of commercial off-the-shelf products | Yes   |
| Software releases to date                | N/A (unknown due to the program's age and variations in release parameters over time)                       |
| Planned releases                         | N/A (applications plan for quarterly releases, with some products requiring semi-annual or annual releases) |
| Average time between releases            | 1-3 months  |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Defense Enterprise Accounting and Management System (DEAMS)

### Program description

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

### Program essentials (reported by DOD officials as of February 2024)

|   |   |                                |
|---|---|--------------------------------|
| Lead DOD component:<br>Air Force  | Program owner:<br>Air Force                     | Year investment began:<br>2003 |
| Acquisition pathway:<br>Defense business systems acquisition                  | Last milestone achieved:<br>Full deployment ATP |                                |
| Next planned milestone:<br>Capability support ATP                             | CIO evaluation rating:<br>5 – Low risk          |                                |
| Year investment is estimated to reach end of useful life: No current end date |   |                                |

**Table 11: Defense Enterprise Accounting and Management System's (DEAMS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response   |
|---|--|
| Developing new software functionality                         | Yes  |
| Use of an iterative development approach                      | Yes  |
| Software development approach                                 | Agile; Development, Security, and Operations (DevSecOps)                         |
| Delivery of a minimum viable product                          | Yes  |
| Software documentation provided at each production milestone  | No   |
| Iterative development training for program managers and staff | No   |
| Use of a software factory                                     | No   |
| Use of commercial off-the-shelf products                      | Yes  |
| Software releases to date                                     | 435  |
| Planned releases  | N/A (releases on a 3-week or 12-week iteration until all capability is released) |
| Average time between releases                                 | Less than 1 month  |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Defense Travel System (DTS)

|  |   |                             |
|--|---|-----------------------------|
| <b>Program description</b>   |   |                             |
| DTS is DOD's travel management system that automates temporary duty travel, including authorizations and vouchers. |   |                             |
| <b>Program essentials (reported by DOD officials as of February 2024)</b>  |   |                             |
| Lead DOD component: Defense-wide   | Program owner: Defense Human Resources Activity, Defense Management Data Center | Year investment began: 2003 |
| Acquisition pathway: Defense business systems acquisition  | Last milestone achieved: Capability support ATP                                 |                             |
| Next planned milestone: N/A (program is in sustainment)  | CIO evaluation rating: 3 – Medium risk  |                             |
| Year investment is estimated to reach end of useful life: No current end date (at least an additional 5 years)     |   |                             |

**Table 12: Defense Travel System's (DTS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response   |
|---|--|
| Developing new software functionality                         | No   |
| Use of an iterative development approach                      | Yes  |
| Software development approach                                 | Agile; Development, Security, and Operations (DevSecOps) |
| Delivery of a minimum viable product                          | Yes  |
| Software documentation provided at each production milestone  | Yes  |
| Iterative development training for program managers and staff | Yes  |
| Use of a software factory                                     | Yes  |
| Use of commercial off-the-shelf products                      | Yes  |
| Software releases to date                                     | 40   |
| Planned releases  | 4 (minimum) per year                                     |
| Average time between releases                                 | 1-3 months   |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Distribution Standard System (DSS)

|  |
|--|
| <b>Program description</b>   |
| DSS is DLA's standard automated system for managing warehouse operations and distributing DOD materiel (i.e., equipment and supplies). The legacy system is intended to provide worldwide service and support to the warfighter, peacekeepers, and federal and civilian customers. |
| <b>Program essentials (reported by DOD officials as of February 2024)</b>  |



Appendix II: Program Summaries

|  |  |                                |
|--|--|--------------------------------|
| Lead DOD component:<br>Defense-wide                            | Program owner:<br>DLA                              | Year investment began:<br>1992 |
| Acquisition pathway:<br>Defense business systems acquisition   | Last milestone achieved:<br>Capability support ATP |                                |
| Next planned milestone:<br>N/A (program is in sustainment)     | CIO evaluation rating:<br>5 – Low risk             |                                |
| Year investment is estimated to reach end of useful life: 2026 |  |                                |

**Program**  
**Distribution Standard System (DSS)**

---

**Software development approach(es)**  
Agile

---

**Average time of software deliveries**

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

---

**Planned cost, fiscal years 2022-2024**

Total operations and maintenance (O&M)  
**\$382.13 mil**

Total development, modernization and enhancement (DME)  
**\$70.77 mil**

**Combined total (O&M + DME)**  
**\$452.90 million**

---

**Cost and schedule changes**  
*(since January 2022)*

Cost: Decrease

Schedule: No change

Rebaseline: No

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 13: Distribution Standard System's (DSS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response |
|---|------------------|
| Developing new software functionality                         | No               |
| Use of an iterative development approach                      | Yes              |
| Software development approach                                 | Agile            |
| Delivery of a minimum viable product                          | Yes              |
| Software documentation provided at each production milestone  | Yes              |
| Iterative development training for program managers and staff | Yes              |
| Use of a software factory                                     | Yes              |
| Use of commercial off-the-shelf products                      | No               |

---

**Appendix II: Program Summaries**

---

| <b>Approach or practice</b>   | <b>Program response</b> |
|-------------------------------|-------------------------|
| Software releases to date     | 40                      |
| Planned releases              | 92                      |
| Average time between releases | Monthly                 |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

# DOD Healthcare Management System Modernization (DHMSM)

## Program description

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

## Program essentials (reported by DOD officials as of February 2024)

|  |   |                                |
|--|---|--------------------------------|
| Lead DOD component:<br>Defense-wide                          | Program owner:<br>DHA                             | Year investment began:<br>2014 |
| Acquisition pathway:<br>Defense business systems acquisition | Last milestone achieved:<br>Full deployment ATP   |                                |
| Next planned milestone:<br>Capability support ATP            | CIO evaluation rating:<br>4 – Moderately low risk |                                |

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

**Program**  
**Department of Defense Healthcare Management System Modernization (DHMSM)**

*N/A (Deploys commercial off-the-shelf products)*

**Average time of software deliveries**

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

**Planned cost, fiscal years 2022-2024**

|  |                           |
|--|---------------------------|
| Total operations and maintenance (O&M)                 | \$1,222.66 mil            |
| Total development, modernization and enhancement (DME) | \$1,068.68 mil            |
| <b>Combined total (O&amp;M + DME)</b>                  | <b>\$2,291.35 million</b> |

**Cost and schedule changes (since January 2022)**

Cost: No change

Schedule: No change

Rebaseline: No

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 14: Department of Defense Healthcare Management System Modernization’s (DHMSM) Reported Software Development Approaches and Practices**

| <b>Approach or practice</b>                                   | <b>Program response</b>   |
|---|---|
| Developing new software functionality                         | No  |
| Use of an iterative development approach                      | N/A (deploys commercial off-the-shelf products)   |
| Software development approach                                 | N/A   |
| Delivery of a minimum viable product                          | N/A   |
| Software documentation provided at each production milestone  | N/A   |
| Iterative development training for program managers and staff | N/A   |
| Use of a software factory                                     | N/A   |
| Use of commercial off-the-shelf products                      | Yes   |
| Software releases to date                                     | 5,368 (releases capabilities to users through commercial off-the-shelf software deployment processes) |
| Planned releases  | 35 (minimum)  |
| Average time between releases                                 | Less than 1 month   |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

# Enterprise Business System (EBS)

## Program description

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 DOD officials as of February 2024)

|  |  |                                |
|--|--|--------------------------------|
| Lead DOD component:<br>Defense-wide                            | Program owner:<br>DLA                              | Year investment began:<br>2001 |
| Acquisition pathway:<br>Defense business systems acquisition   | Last milestone achieved:<br>Capability support ATP |                                |
| Next planned milestone:<br>N/A (program is in sustainment)     | CIO evaluation rating:<br>3 – Medium risk          |                                |
| Year investment is estimated to reach end of useful life: 2030 |  |                                |

**Program**  
Enterprise Business System (EBS)

---

**Software development approach(es)**  
Agile; Incremental; Development, Operations (DevOps); Development, Security, and Operations (DevSecOps)

---

**Average time of software deliveries**

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

---

**Planned cost, fiscal years 2022-2024**

|  |                         |
|--|-------------------------|
| Total operations and maintenance (O&M)                 | \$344.68 mil            |
| Total development, modernization and enhancement (DME) | \$10.50 mil             |
| <b>Combined total (O&amp;M + DME)</b>                  | <b>\$355.18 million</b> |

---

**Cost and schedule changes (since January 2022)**

Cost: No change

Schedule: No change

Rebaseline: No

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 15: Enterprise Business System’s (EBS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response  |
|---|---|
| Developing new software functionality                         | No  |
| Use of an iterative development approach                      | Yes   |
| Software development approach                                 | Agile; Development, Operations (DevOps); Development, Security, and Operations (DevSecOps); Incremental |
| Delivery of a minimum viable product                          | Yes   |
| Software documentation provided at each production milestone  | Yes   |
| Iterative development training for program managers and staff | Yes   |
| Use of a software factory                                     | Yes   |
| Use of commercial off-the-shelf products                      | Yes   |
| Software releases to date                                     | 1396  |
| Planned releases  | 73  |
| Average time between releases                                 | Less than 1 month   |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## General Fund Enterprise Business System (GFEBs)

| Program description  |  |                                |
|--|--|--------------------------------|
| GFEBs is Army’s core financial management system intended to administer its general fund finances, improve financial visibility and information reliability, and standardize business processes. |  |                                |
| Program essentials (reported by DOD officials as of February 2024)   |  |                                |
| Lead DOD component:<br>Army  | Program owner:<br>Army                             | Year investment began:<br>2005 |
| Acquisition pathway:<br>Defense business systems acquisition   | Last milestone achieved:<br>Capability support ATP |                                |
| Next planned milestone:<br>N/A (program is in sustainment)   | CIO evaluation rating:<br>5 – Low risk             |                                |
| Year investment is estimated to reach end of useful life: 2032   |  |                                |

**Table 16: General Fund Enterprise Business System’s (GFEBs) Reported Software Development Approaches and Practices**

| Approach or practice   | Program response |
|--|------------------|
| Developing new software functionality                        | Yes              |
| Use of an iterative development approach                     | Yes              |
| Software development approach                                | Agile            |
| Delivery of a minimum viable product                         | Yes              |
| Software documentation provided at each production milestone | Yes              |

Appendix II: Program Summaries

| Approach or practice  | Program response |
|---|------------------|
| Iterative development training for program managers and staff | Yes              |
| Use of a software factory                                     | No               |
| Use of commercial off-the-shelf products                      | Yes              |
| Software releases to date                                     | 221              |
| Planned releases  | 234              |
| Average time between releases                                 | 1-3 months       |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

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

| Program description   |  |                                |
|---|--|--------------------------------|
| GCSS-A is intended to provide functional services to Army's business mission areas. The system is focused on supply operations, tactical maintenance, and enterprise aviation logistics, along with associated logistics management and tactical finance functionality. |  |                                |
| Program essentials (reported by DOD officials as of February 2024)  |  |                                |
| Lead DOD component:<br>Army   | Program owner:<br>Army                             | Year investment began:<br>2002 |
| Acquisition pathway:<br>Defense business systems acquisition  | Last milestone achieved:<br>Capability Support ATP |                                |
| Next planned milestone:<br>N/A (program is in sustainment)  | CIO evaluation rating:<br>5 – Low risk             |                                |
| Year investment is estimated to reach end of useful life: 2032  |  |                                |

**Table 17: Global Combat Support System-Army's (GCSS-A) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response |
|---|------------------|
| Developing new software functionality                         | Yes              |
| Use of an iterative development approach                      | Yes              |
| Software development approach                                 | Agile            |
| Delivery of a minimum viable product                          | Yes              |
| Software documentation provided at each production milestone  | Yes              |
| Iterative development training for program managers and staff | Yes              |
| Use of a software factory                                     | No               |
| Use of commercial off-the-shelf products                      | Yes              |
| Software releases to date                                     | 71               |
| Planned releases  | 4 quarterly      |
| Average time between releases                                 | 1-3 months       |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

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

### Program description

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

### Program essentials (reported by DOD officials as of February 2024)

|   |   |                                |
|---|---|--------------------------------|
| Lead DOD component:<br>Navy, Marine Corps                         | Program owner:<br>Navy                      | Year investment began:<br>2004 |
| Acquisition pathway:<br>Defense business systems acquisition      | Last milestone achieved:<br>Full deployment |                                |
| Next planned milestone:<br>Sustainment                            | CIO evaluation rating:<br>5 – Low risk      |                                |
| Year investment is estimated to reach end of useful life:<br>2035 |   |                                |

**Table 18: Global Combat Support System-Marine Corps/Logistics Chain Management's (GCSS-MC/LCM) Reported Software Development Approaches and Practices**

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

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Joint Operational Medicine Information Systems (JOMIS)

### Program description

JOMIS pursues efforts to sunset costly and difficult-to-maintain legacy systems and modernizes medicine information systems to provide integrated, timely, and accurate information to make critical command and control and medical decisions.



Appendix II: Program Summaries

| Program essentials (reported by DOD officials as of February 2024)  |   |                                |
|---|---|--------------------------------|
| Lead DOD component:<br>Defense-wide   | Program owner:<br>DHA   | Year investment began:<br>2016 |
| Acquisition pathway:<br>Middle tier of acquisition, major capability acquisition, software acquisition (JOMIS is a portfolio of products) | Last milestone achieved:<br>For Medical Common Operating Picture (MEDCOP), minimum viable capability release capability |                                |
| Next planned milestone:<br>For MEDCOP, operational test   | CIO evaluation rating:<br>4 – Moderately low risk   |                                |
| Year investment is estimated to reach end of useful life: 2045  |   |                                |

**Table 19: Joint Operational Medicine Information Systems’ (JOMIS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response  |
|---|---|
| Developing new software functionality                         | Yes   |
| Use of an iterative development approach                      | Yes   |
| Software development approach                                 | Agile   |
| Delivery of a minimum viable product                          | Yes   |
| Software documentation provided at each production milestone  | Yes   |
| Iterative development training for program managers and staff | Yes   |
| Use of a software factory                                     | No  |
| Use of commercial off-the-shelf products                      | Yes   |
| Software releases to date                                     | Medical Common Operating Picture (MEDCOP) has delivered 90 releases   |
| Planned releases  | MEDCOP has 1 release every two weeks, with a plan to continue releasing biweekly for the full life cycle of the product |
| Average time between releases                                 | Less than 1 month   |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Military Health System Information Platform (MIP)

### Program description

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

### Program essentials (reported by DOD officials as of February 2024)

|  |  |                                |
|--|--|--------------------------------|
| Lead DOD component:<br>Defense-wide                            | Program owner:<br>Program Executive Office, Defense<br>Healthcare Management Systems | Year investment<br>began: 2016 |
| Acquisition pathway:<br>Defense business systems acquisition   | Last milestone achieved:<br>Capability support ATP                                   |                                |
| Next planned milestone:<br>N/A (program is in sustainment)     | CIO evaluation rating:<br>4 – Moderately low risk                                    |                                |
| Year investment is estimated to reach end of useful life: 2035 |  |                                |

**Table 20: Military Health System Information Platform’s (MIP) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response  |
|---|---|
| Developing new software functionality                         | No  |
| Use of an iterative development approach                      | Yes   |
| Software development approach                                 | Agile; Development, Security, and Operations (DevSecOps); Incremental   |
| Delivery of a minimum viable product                          | Yes   |
| Software documentation provided at each production milestone  | Yes   |
| Iterative development training for program managers and staff | Yes   |
| Use of a software factory                                     | Yes   |
| Use of commercial off-the-shelf products                      | Yes   |
| Software releases to date                                     | MIP has continuous development releases   |
| Planned releases  | MIP has continuous development releases   |
| Average time between releases                                 | Releases user interface improvements continuously; releases are variable in size and frequency depending on requirements and priority |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

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

### Program description

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

### Program essentials (reported by DOD officials as of February 2024)

|                             |                        |                                |
|-----------------------------|------------------------|--------------------------------|
| Lead DOD component:<br>Navy | Program owner:<br>Navy | Year investment began:<br>2017 |
|-----------------------------|------------------------|--------------------------------|

|   |   |
|---|---|
| Acquisition pathway:<br>Defense business systems acquisition, other transaction authority | Last milestone achieved:<br>Requirements approved |
|---|---|

|  |   |
|--|---|
| Next planned milestone:<br>Limited deployment ATP(s) | CIO evaluation rating:<br>4 – Moderately low risk |
|--|---|

Year investment is estimated to reach end of useful life: 2040

### Program

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

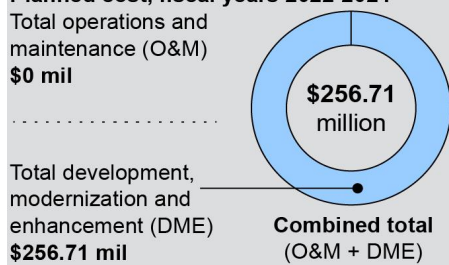
### Software development approach(es)

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

### Average time of software deliveries



### Planned cost, fiscal years 2022-2024



### Cost and schedule changes

(since January 2022)

Cost: Increase

Schedule: Delay

Rebaseline: Yes

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 21: Naval-Maintenance, Repair, and Overhaul’s (N-MRO) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response  |
|---|---|
| Developing new software functionality                         | Yes   |
| Use of an iterative development approach                      | Yes   |
| Software development approach                                 | Agile; Development, Security, and Operations (DevSecOps); Incremental |
| Delivery of a minimum viable product                          | Yes   |
| Software documentation provided at each production milestone  | Yes   |
| Iterative development training for program managers and staff | Yes   |
| Use of a software factory                                     | No  |
| Use of commercial off-the-shelf products                      | Yes   |
| Software releases to date                                     | 0   |
| Planned releases  | 23 (projected)  |
| Average time between releases                                 | 1-3 months  |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Naval Air Systems Command Aviation Logistics Environment (NAVAIR ALE)

### Program description

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

### Program essentials (reported by DOD officials as of February 2024)

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

**Table 22: Naval Air Systems Command Aviation Logistics Environment’s (NAVAIR ALE) Reported Software Development Approaches and Practices**

| Approach or practice                     | Program response                                  |
|--|---|
| Developing new software functionality    | Yes   |
| Use of an iterative development approach | Yes   |
| Software development approach            | Development, Security, and Operations (DevSecOps) |

---

**Appendix II: Program Summaries**

---

|   |            |
|---|------------|
| Delivery of a minimum viable product                          | Yes        |
| Software documentation provided at each production milestone  | Yes        |
| Iterative development training for program managers and staff | Yes        |
| Use of a software factory                                     | No         |
| Use of commercial off-the-shelf products                      | Yes        |
| Software releases to date                                     | 8          |
| Planned releases  | 2 per year |
| Average time between releases                                 | 4-6 months |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

---

## Navy Electronic Procurement System (Navy EPS)

---

**Program description**

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

---

**Program essentials (reported by DOD officials as of February 2024)**

|   |  |                                |
|---|--|--------------------------------|
| Lead DOD component:<br>Navy, Marine Corps   | Program owner:<br>Navy   | Year investment began:<br>2013 |
| Acquisition pathway:<br>Defense business systems acquisition,<br>software acquisition | Last milestone achieved:<br>Entry into software pathway execution<br>phase |                                |
| Next planned milestone:<br>Deliver capabilities                                       | CIO evaluation rating:<br>3 – Medium risk                                  |                                |
| Year investment is estimated to reach end of useful life: No current end date         |  |                                |

---

Appendix II: Program Summaries

**Program**  
**Navy Electronic Procurement System (NAVY EPS)**

---

**Software development approach(es)**  
 Agile; Development, Security, and Operations (DevSecOps)

---

**Average time of software deliveries**

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

---

**Planned cost, fiscal years 2022-2024**

Total operations and maintenance (O&M) **\$16.30 mil**

Total development, modernization and enhancement (DME) **\$84.89 mil**

**Combined total (O&M + DME) \$101.20 million**

---

**Cost and schedule changes (since January 2022)**

Cost: No change

Schedule: Delay

Rebaseline: *Expects to*

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 23: Navy Electronic Procurement System's (Navy EPS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response   |
|---|--|
| Developing new software functionality                         | Yes  |
| Use of an iterative development approach                      | Yes  |
| Software development approach                                 | Agile; Development, Security, and Operations (DevSecOps) |
| Delivery of a minimum viable product                          | Yes  |
| Software documentation provided at each production milestone  | Yes  |
| Iterative development training for program managers and staff | Yes  |
| Use of a software factory                                     | Yes  |
| Use of commercial off-the-shelf products                      | Yes  |
| Software releases to date                                     | 9  |
| Planned releases  | 3 major releases   |

Appendix II: Program Summaries

| Approach or practice          | Program response                                     |
|-------------------------------|--|
| Average time between releases | Less than one month;<br>Quarterly for minor releases |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Navy Enterprise Resource Planning (Navy ERP)

| Program description  |  |                                |
|--|--|--------------------------------|
| Navy ERP is Navy’s legacy financial system of record. The system is intended to streamline Navy’s business operations and is focused on financial and supply chain management. |  |                                |
| Program essentials (reported by DOD officials as of February 2024)   |  |                                |
| Lead DOD component:<br>Navy, Marine Corps  | Program owner:<br>Navy                           | Year investment began:<br>2004 |
| Acquisition pathway:<br>Defense business systems acquisition   | Last milestone achieved:<br>Full-rate production |                                |
| Next planned milestone:<br>N/A (program is in sustainment)   | CIO evaluation rating:<br>3 – Medium risk        |                                |
| Year investment is estimated to reach end of useful life:<br>2027  |  |                                |

**Table 24: Navy Enterprise Resource Planning’s (Navy ERP) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response  |
|---|---|
| Developing new software functionality                         | Yes   |
| Use of an iterative development approach                      | Yes   |
| Software development approach                                 | Development, Security, and Operations (DevSecOps);<br>Incremental |
| Delivery of a minimum viable product                          | Yes   |
| Software documentation provided at each production milestone  | Yes   |
| Iterative development training for program managers and staff | Yes   |
| Use of a software factory                                     | No  |
| Use of commercial off-the-shelf products                      | Yes   |
| Software releases to date                                     | 85  |
| Planned releases  | 0   |
| Average time between releases                                 | Less than 1 month   |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Navy Maritime Maintenance Enterprise Solution (NMMES)

| Program description |
|---------------------|
|---------------------|

Appendix II: Program Summaries

NMMES is intended to consolidate overlapping application functionality and databases, data centers, and infrastructure for ship and submarine maintenance into an integrated enterprise solution.

**Program essentials (reported by DOD officials as of February 2024)**

|  |  |                                |
|--|--|--------------------------------|
| Lead DOD component:<br>Navy, Marine Corps  | Program Owner:<br>Navy                             | Year investment began:<br>2012 |
| Acquisition pathway:<br>Defense business systems acquisition, software acquisition, acquisition of service | Last milestone achieved:<br>Capability support ATP |                                |
| Next planned milestone:<br>N/A (program is in sustainment)   | CIO evaluation rating:<br>4 – Moderately low risk  |                                |
| Year investment is estimated to reach end of useful life: 2034   |  |                                |

**Program**  
Navy Maritime Maintenance Enterprise Solution (NMMES)

---

**Software development approach(es)**  
Agile; Waterfall; Development and Operations (DevOps); Development, Security, and Operations (DevSecOps)

---

**Average time of software deliveries**

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

---

**Planned cost, fiscal years 2022-2024**

Total operations and maintenance (O&M) **\$317.10 mil**

Total development, modernization and enhancement (DME) **\$38.34 mil**

**Combined total (O&M + DME) \$355.43 million**

---

**Cost and schedule changes (since January 2022)**

Cost: Increase

Schedule: Delay

Rebaseline: No

Source: GAO analyses of the Department of Defense's (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 25: Navy Maritime Maintenance Enterprise Solution’s (NMMES) Reported Software Development Approaches and Practices**

| Approach or practice                  | Program response |
|---------------------------------------|------------------|
| Developing new software functionality | No               |



**Appendix II: Program Summaries**

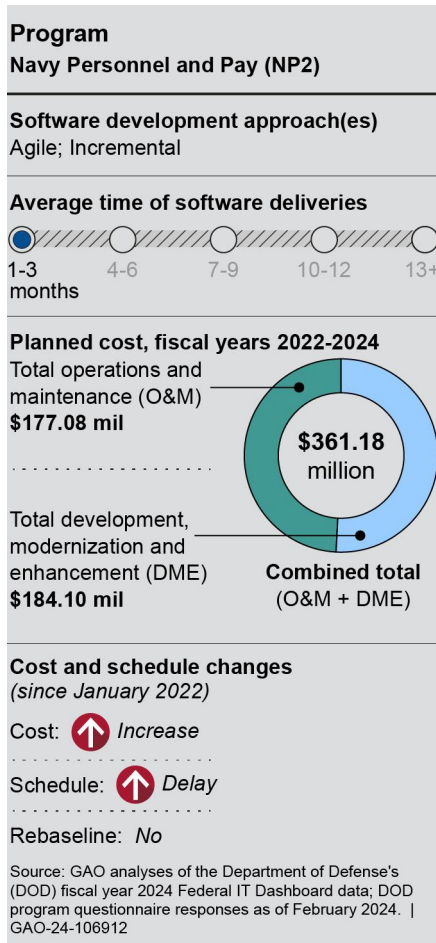
| <b>Approach or practice</b>                                   | <b>Program response</b>  |
|---|--|
| Use of an iterative development approach                      | Yes  |
| Software development approach                                 | Agile; Development and Operations (DevOps); Development, Security, and Operations (DevSecOps); Waterfall |
| Delivery of a minimum viable product                          | Yes  |
| Software documentation provided at each production milestone  | Yes  |
| Iterative development training for program managers and staff | Yes  |
| Use of a software factory                                     | No   |
| Use of commercial off-the-shelf products                      | Yes  |
| Software releases to date                                     | 327 (24 software and 303 production data fix releases)   |
| Planned releases  | 24   |
| Average time between releases                                 | 1-3 months   |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

## Navy Personnel and Pay (NP2)

| <b>Program description</b>   |  |                                |
|--|--|--------------------------------|
| NP2 is Navy's business solution to human resources management and will provide the future integrated personnel and pay capability, supporting over 400,000 active and reserve sailors worldwide. |  |                                |
| <b>Program essentials (reported by DOD officials as of February 2024)</b>  |  |                                |
| Lead DOD component:<br>Navy  | Program owner:<br>Navy   | Year investment began:<br>2019 |
| Acquisition pathway:<br>Defense business systems acquisition   | Last milestone achieved:<br>Transformation portfolio baseline approved |                                |
| Next planned milestone:<br>Fiscal year 2025 transformation portfolio baseline  | CIO evaluation rating:<br>3 – Medium risk                              |                                |
| Year investment is estimated to reach end of useful life: 2028   |  |                                |

Appendix II: Program Summaries



**Table 26: Navy Personnel and Pay's (NP2) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response   |
|---|--------------------|
| Developing new software functionality                         | Yes                |
| Use of an iterative development approach                      | Yes                |
| Software development approach                                 | Agile; Incremental |
| Delivery of a minimum viable product                          | Yes                |
| Software documentation provided at each production milestone  | Yes                |
| Iterative development training for program managers and staff | Yes                |
| Use of a software factory                                     | Yes                |
| Use of commercial off-the-shelf products                      | Yes                |
| Software releases to date                                     | 27                 |
| Planned releases  | 32                 |
| Average time between releases                                 | 1-3 months         |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

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

## Program description

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

## Program essentials (reported by DOD officials as of February 2024)

|                                     |   |                                   |
|-------------------------------------|---|-----------------------------------|
| Lead DOD component:<br>Defense-wide | Program owner:<br>Defense Human Resources Activity,<br>Defense Manpower Data Center | Year investment<br>began:<br>1997 |
|-------------------------------------|---|-----------------------------------|

|  |  |
|--|--|
| Acquisition pathway:<br>Defense business systems acquisition | Last milestone achieved:<br>Capability support ATP |
|--|--|

|  |   |
|--|---|
| Next planned milestone:<br>Functional requirements ATP | CIO evaluation rating:<br>3 – Medium risk |
|--|---|

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

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

---

**Software development approach(es)**  
Development and Operations (DevOps)

---

**Average time of software deliveries**

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

---

**Planned cost, fiscal years 2022-2024**

|  |                         |
|--|-------------------------|
| Total operations and maintenance (O&M)                 | \$222.85 mil            |
| Total development, modernization and enhancement (DME) | \$29.66 mil             |
| <b>Combined total (O&amp;M + DME)</b>                  | <b>\$252.51 million</b> |

---

**Cost and schedule changes (since January 2022)**

Cost: Increase

Schedule: No change

Rebaseline: No

Source: GAO analyses of the Department of Defense’s (DOD) fiscal year 2024 Federal IT Dashboard data; DOD program questionnaire responses as of February 2024. | GAO-24-106912

**Table 27: Real-Time Automated Personnel Identification System and Common Access Card's (RAPIDS) Reported Software Development Approaches and Practices**

| Approach or practice  | Program response  |
|---|---|
| Developing new software functionality                         | No  |
| Use of an iterative development approach                      | Yes   |
| Software development approach                                 | Development and Operations (DevOps)   |
| Delivery of a minimum viable product                          | No  |
| Software documentation provided at each production milestone  | Yes   |
| Iterative development training for program managers and staff | Yes   |
| Use of a software factory                                     | No  |
| Use of commercial off-the-shelf products                      | Yes   |
| Software releases to date                                     | Unknown due to the age of the program                                       |
| Planned releases  | 7 yearly releases, with 11 yearly releases for the rest of the RAPIDS suite |
| Average time between releases                                 | 1-3 months  |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

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

### Program description

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

### Program essentials (reported by DOD officials as of February 2024)

|   |  |                                |
|---|--|--------------------------------|
| Lead DOD component:<br>Defense-wide   | Program owner:<br>DHA                              | Year investment began:<br>2009 |
| Acquisition pathway:<br>Defense business systems acquisition  | Last milestone achieved:<br>Delivered capabilities |                                |
| Next planned milestone:<br>Decommissioning  | CIO evaluation rating:<br>4 – Moderately low risk  |                                |
| Year investment is estimated to reach end of useful life:<br>2030 for maritime medical modules, 2025 for other sections of TMIP-J |  |                                |

**Table 28: Theater Medical Information Program-Joint Increment 2's (TMIP-J) Reported Software Development Approaches and Practices**

| Approach or practice                     | Program response |
|--|------------------|
| Developing new software functionality    | No               |
| Use of an iterative development approach | Yes              |

---

**Appendix II: Program Summaries**

---

|   |                  |
|---|------------------|
| Software development approach                                 | Agile; Waterfall |
| Delivery of a minimum viable product                          | No               |
| Software documentation provided at each production milestone  | Yes              |
| Iterative development training for program managers and staff | Yes              |
| Use of a software factory                                     | No               |
| Use of commercial off-the-shelf products                      | Yes              |
| Software releases to date                                     | 625              |
| Planned releases  | 6                |
| Average time between releases                                 | 3-4 months       |

Source: GAO analysis of Department of Defense program questionnaire responses as of February 2024. | GAO-24-106912

# Appendix III: Comments from the Department of Defense



CHIEF INFORMATION OFFICER

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

APR 26 2024

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 provides the Department of Defense (DoD) response to the GAO Draft Report, GAO-24-106912, "IT SYSTEMS ANNUAL ASSESSMENT: DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps," dated March 29, 2024 (GAO Code 106912).

**RECOMMENDATION 1:** The GAO recommends that the Secretary of Defense direct the Chief Information Officer and Under Secretary of Defense for Acquisition and Sustainment to ensure that IT business programs developing software use the metrics and management tools required by DoD and consistent with those identified in GAO's Agile Assessment Guide.

**DoD RESPONSE:** Concur

DoD recognizes the importance of delivering resilient software securely and rapidly to the Warfighter. DoD agrees that IT business programs developing software should align with industry best practices including the use of metrics and management tools that encourage agile development of software where appropriate. DoD published the Software Modernization Strategy in 2022 and accompanying Implementation Plan in 2023, putting the Department on the path to adopt modern software development practice. DoD Chief Information Officer will include guidance on metrics and management tools for agile development in the next Software Modernization Implementation Plan.

My point of contact for this matter is Mr. George Lamb who may be reached at (202) 913-5858 or [george.w.lamb16.civ@mail.mil](mailto:george.w.lamb16.civ@mail.mil).

  
John B. Sherman

# Accessible Text for Appendix III: Comments from the Department of Defense

APR 26 2024

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 provides the Department of Defense (DoD) response to the GAO Draft Report, GAO-24-106912, "IT SYSTEMS ANNUAL ASSESSMENT: DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps," dated March 29, 2024 (GAO Code 106912).

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Chief Information Officer and Under Secretary of Defense for Acquisition and Sustainment to ensure that IT business programs developing software use the metrics and management tools required by DoD and consistent with those identified in GAO's Agile Assessment Guide.

DoD RESPONSE: Concur

DoD recognizes the importance of delivering resilient software securely and rapidly to the Warfighter. DoD agrees that IT business programs developing software should align with industry best practices including the use of metrics and management tools that encourage agile development of software where appropriate. DoD published the Software Modernization Strategy in 2022 and accompanying Implementation Plan in 2023, putting the Department on the path to adopt modern software development practice. DoD Chief Information Officer will include guidance on metrics and management tools for agile development in the next Software Modernization Implementation Plan.

My point of contact for this matter is Mr. George Lamb who may be reached at (202) 913-5858 or [george.w.lamb16.civ@mail.mil](mailto:george.w.lamb16.civ@mail.mil).

John B. Sherman

# 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, Chris Businsky, Kathryn Howarth, Jess Lionne, Sarah Ong, and Richard Sayoc. Other key contributors included Bea Alff, Amanda Andrade, Margaret Best, Scott Borre, Erin Carson, Richard Geiger, Andrea Harvey, Michael Holland, Jennifer Leotta, Lori Martinez, Anne McDonough, Sukhjoot Singh, Jonathan Wall, Walter Vance, and Adam Vodraska.



---

---

---

## GAO's Mission

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

---

## Obtaining Copies of GAO Reports and Testimony

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

---

## Order by Phone

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

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

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

---

## Connect with GAO

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

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

---

## Congressional Relations

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

---

## Public Affairs

Sarah Kaczmarek, Acting Managing Director, [KaczmarekS@gao.gov](mailto:KaczmarekS@gao.gov), (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

---

---

---

## Strategic Planning and External Liaison

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