United States Government Accountability Office

Report to Congressional Committees

June 2022

BUSINESS SYSTEMS

DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning

Accessible Version

GAO-22-105330

GAO Highlight

Highlights of GAO-22-105330, a report to congressional committees

June 2022

BUSINESS SYSTEMS

DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning

Why GAO Did This Study

For fiscal year 2022, DOD requested approximately $38.6 billion for its unclassified IT investments. These investments included programs such as communications and command and control systems. They also included major IT business programs, which are intended to help the department carry out key functions, such as financial management and health care.

The NDAA for FY 2019 included a provision for GAO to assess selected DOD IT programs annually through March 2023. GAO's objectives for this review were to (1) examine how DOD's portfolio of major IT acquisition business programs has performed; (2) determine the extent to which the department has implemented software development, cybersecurity, and supply chain risk management practices; and (3) describe actions DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address these objectives, GAO determined that DOD's major IT business programs were the 25 that DOD reported to the federal IT Dashboard as of December 2021 (The IT Dashboard is a public website that includes information on the performance of IT investments). GAO examined DOD's planned expenditures for these programs from fiscal years 2020 through 2022, as reported in the department's FY 2022 submission to the Dashboard.

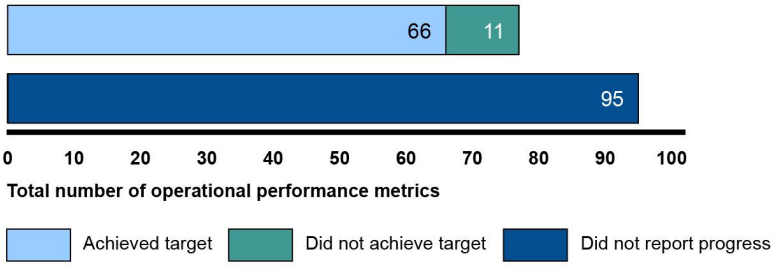
View GAO-22-105330. For more information, contact Kevin Walsh at 202-512-6151 or walshk@gao.gov.

What GAO Found

According to the Department of Defense's (DOD) fiscal year (FY) 2022 submission to the federal IT Dashboard, DOD planned to spend $8.8 billion on its portfolio of 25 major IT business programs between FY 2020 and 2022. In addition, 18 of the 25 programs reported experiencing cost or schedule changes since January 2020. Of these programs, 14 reported the extent to which program costs and schedules had changed, noting cost increases ranging from $0.1 million to $10.7 billion and schedule delays ranging from 5 to 19 months. Program officials attributed the changes to various factors, including requirement changes or delays, contract developments, and technical complexities.

Programs also reported operational performance data to the federal IT Dashboard. As of December 2021, the 25 programs collectively identified 172 operational performance metrics consistent with Office of Management and Budget (OMB) guidance. These metrics covered a range of performance indicators such as the timeliness of program deliverables and the percentage of time that systems were available to users. However, programs only reported progress on 77 of the 172 operational performance targets. (See figure.)

Officials for DOD's 25 Major IT Business Programs Reported Operational Performance Data to the Federal IT Dashboard, as of December 2021



Source: GAO analysis of Department of Defense data reported to the federal IT Dashboard. | GAO-22-105330

Nineteen programs did not fully report progress on their operational performance. Officials from the Office of the DOD CIO stated that programs that have operational performance measures should be reporting them to the Dashboard. They added that there were multiple factors that could have led to programs not reporting the metrics, including a reorganization that shifted responsibilities for IT investment management and confusion about the reporting requirement. Nevertheless, by reporting incomplete performance data, DOD limits Congress' and the public's understanding of how programs are performing.

As of February 2022, DOD program officials from all 11 (of the 25) major IT business programs that we considered to be actively developing new software functionality reported using recommended iterative development practices that can limit risks of adverse cost and schedule outcomes. Officials from eight of the 11 programs reported using Agile software development, which can support continuous iterative software development. Officials for five of the programs also reported delivering software functionality every 6 months or less, as called for in

OMB guidance. Officials for three programs reported a frequency greater than 6 months and officials from the remaining three did not indicate a frequency.

GAO obtained the programs' operational performance data from the Dashboard and compared the data to OMB guidance. It also met with DOD CIO officials to determine reasons why programs were not reporting data in accordance with guidance.

In addition, GAO aggregated program office responses to a GAO questionnaire that requested information about cost and schedule changes that the programs experienced since January 2020.

GAO also aggregated DOD program office responses to the questionnaire that requested information about software development, cybersecurity, and supply chain risk management plans and practices. GAO compared the responses to relevant guidance and leading practices.

Further, GAO reviewed actions DOD has taken to implement its plans for addressing previously identified legislative and policy changes that could affect its IT acquisitions. This included reviewing information associated with the department's efforts to (1) finalize strategies for its business system and software acquisition pathways; (2) implement modern approaches to software development such as transitioning to Agile; and (3) reorganize the responsibilities of the former Chief Management Officer throughout the department. GAO met with relevant DOD officials to discuss each of the topics addressed in this report.

What GAO Recommends

GAO is making three recommendations to DOD to ensure programs (1) report operational performance data to the federal IT Dashboard; (2) develop cybersecurity strategies; and (3) develop plans that address ICT supply chain risk management, as appropriate.

DOD concurred with GAO's recommendations and described actions it was taking, and planned to take, to address them.

In addition, as of February 2022, officials from the 25 major IT business programs reported on whether they had an approved cybersecurity strategy as required by DOD. (See table.)

Officials for Major DOD IT Business Programs Reported on Whether They Had an Approved Cybersecurity Strategy, as of February 2022

Programs' cybersecurity assessment status	Number of programs
Reported having an approved cybersecurity strategy and provided the strategy	15 of 25
Reported having an approved cybersecurity strategy but did not provide the strategy to support their response	7 of 15
Reported not having an approved cybersecurity strategy, but planned to develop one	2 of 25
Reported not having an approved cybersecurity strategy and did not plan to develop one	1 of 25

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-22-105330

Officials from DOD CIO stated that they will follow up with the programs that did not provide an approved cybersecurity strategy. Until DOD ensures that these programs develop strategies, programs lack assuance that they are effectively positioned to manage cybersecurity risks and mitigate threats.

Officials from the 25 programs also reported on whether they had a system security plan that addresses information and communications technology (ICT) supply chain risk management, as called for by leading practices. (See table.)

Officials for Major DOD IT Business Programs Reported on Whether They Had Information and Communications Technology (ICT) Supply Chain Risk Management Plans, as of February 2022

Programs' supply chain risk management plan status	Number of programs
Reported having a system security plan that addresses ICT supply chain risk management and provided the plan	10 of 25
Reported having a system security plan that addresses ICT supply chain risk management, but did not provide the plan to support their response	1 of 25
Reported not having a system security plan that addresses ICT supply chain risk management, but planned to develop one	7 of 25
Reported not having a system security plan that addresses ICT supply chain risk management and did not plan to develop one	7 of 25

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-22-105330

DOD guidance does not require programs to address ICT supply chain risk management in security plans. According to officials from DOD CIO, IT programs might address supply chain risk management in program protection plans. In addition, they noted that recent supply chain efforts have been focused on weapons systems. However, 15 of DOD's major IT programs did not demonstrate that they had a supply chain risk management plan. Until DOD ensures that these programs have such plans, they are less likely to be able to manage supply chain risks and mitigate threats that could disrupt operations.

Regarding actions to implement legislative and policy changes, the National Defense Authorization Act (NDAA) for FY 2021 eliminated the DOD chief management officer (CMO) position. This position previously had broad oversight

responsibilities for DOD business systems. In September 2021, the Deputy Secretary of Defense directed a broad realignment of the responsibilities previously assigned to the CMO. GAO will continue to monitor DOD's efforts to redistribute the roles and responsibilities formerly assigned to the CMO.

Contents

Tables

Figures

Abbreviations

AAF	adaptive acquisition framework
ATP	authority to proceed
CIO	Chief Information Officer
CMO	Chief Management Officer
COTS	commercial off-the-shelf
DA&M	Director of Administration and Management
DAU	Defense Acquisition University
DevOps	development and operations
DevSecOps	development, security, and operations
DHMSM	Department of Defense Healthcare Management System Modernization
DME	development, modernization, and enhancement
DOD	Department of Defense
FY	fiscal year
GCSS-A	Global Combat Support System–Army
GFEBS	General Fund Enterprise Business System
ICT	information and communications technology
MAIS	major automated information system
Navy ERP	Navy Enterprise Resource Planning
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
O&S	operations and sustainment
OMB	Office of Management and Budget
SEI	Software Engineering Institute
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)	Under Secretary of Defense (Comptroller)/Chief Financial Officer

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

June 14, 2022

Congressional Committees

The Department of Defense (DOD) is one of the largest and most complex organizations in the world. To protect the security of our nation and deter war, DOD relies heavily on the use of IT. For fiscal year (FY) 2022, the department requested approximately $38.6 billion for its unclassified IT investments.[1]

DOD's investments include its major IT programs, which are intended to help the department sustain its key operations. Collectively, these programs encompass communications, command and control systems, and business systems that support department business operations (e.g., financial management, human capital management, and health care). The programs also provide DOD and component officials with access to information used to organize, plan, direct, and monitor mission operations.

The John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 included a provision for GAO to conduct annual assessments of selected DOD IT programs through March 2023.[2] This report presents the results of our third annual assessment. Our specific

[1]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year (FY) 2022 Budget Request* (June 2021). This figure does not reflect all funding requested for DOD's IT systems. For example, classified systems are not included. In addition, not all DOD IT expenditures are reported separately from their respective programs if those programs are developing more than software and hardware to support the software. For example, our annual assessments of DOD's weapons programs include programs that do not report software expenditures separately. See GAO, *Weapon Systems Annual Assessment: Challenges to Fielding Capabilities Faster Persist*, GAO-22-105230 (Washington, D.C., June 8, 2022).

[2]Pub. L. No 115-232,§ 833, 132 Stat. 1636, 1858 (Aug. 13, 2018), adding a new section 2229b, Comptroller General assessment of acquisition programs and initiatives, to Title 10 of the U.S. Code, since renumbered § 3072 and amended by Pub. L. No.116–283 (William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021), §§ 813, 1807(g)(1), 134 Stat. 3388, 3749 and 4159 (Jan. 1, 2021). Under this provision, we are to report on these assessments no later than March 30 of each year from 2020 through 2023. Our assessment of the performance of DOD's weapon programs is included in a separate report, which we also prepared in response to section 833 of the NDAA for FY 2019. See GAO-22-105230.

objectives for this assessment were to: (1) examine how DOD's portfolio of major IT acquisition business programs has performed; (2) determine the extent to which the department has implemented software development, cybersecurity, and supply chain risk management practices; and (3) describe actions DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, we initially considered the 27 major IT business programs that DOD had reported to the federal IT Dashboard as of December 2021.[3] We then excluded two of these programs: one program that the department no longer considered a major IT program and one program that it planned to retire before FY 2022. We determined the universe of major IT business programs to be the remaining 25. These included programs that support key areas such as personnel, financial management, health care, and logistics.

We examined how much the department reported spending on the programs in FY 2020 and planned to spend on these programs from FY 2021 through 2022 by reviewing DOD's FY 2022 submission to the Dashboard. Based on these data, we calculated the total actual and planned expenditures for the programs for the 3-year period. In addition, we obtained programs' operational performance metric data to determine the extent to which programs identified performance metrics and reported on program performance.

We aggregated program office responses to a GAO questionnaire that we developed and administered to all 25 programs in October 2021. Programs provided their responses between October 2021 and December 2021. The questionnaire sought information about program cost and schedule changes that had occurred since January 2020. We continued to follow-up with programs about information they reported in their questionnaires through February 2022.

To assess the reliability of the budget data that DOD reported in the department's federal IT Dashboard submission, we compared the data to planned cost information provided by the programs to identify any obvious inconsistencies. In addition, we prepared and sent the program summaries to the 10 (of the 25) programs that had the largest planned expenditures over the 3-year period discussed in this report and asked

[3]The federal IT Dashboard is a public, federal government website previously operated by OMB and currently by GSA at https://itdashboard.gov. It includes information on the performance of major IT investments.

program staff to review the summaries and confirm their accuracy. To assess the reliability of the operational performance metric data, we met with officials from the office of the DOD Chief Information Officer (CIO) to determine whether programs submitted data consistently with DOD instructions. We determined that the budget data and operational performance metrics data were sufficiently reliable for our reporting purposes.

To help ensure the reliability of the data collected via our questionnaire, including for information associated with the subsequent objective and program summaries, we took steps to reduce measurement error and non-response error. Specifically, we conducted pretests of the questionnaire with three programs to ensure that the questions were clear, unbiased, and consistently interpreted. The pretests allowed us to obtain initial program feedback and helped ensure that officials within each program understood the questions. The questionnaire allowed respondents to submit their answers electronically. 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.

To address the second objective, we included questions in our questionnaire seeking information about software development, cybersecurity, and supply chain risk management plans and approaches used by the DOD IT programs reviewed under our first objective. We aggregated program responses and compared this information to relevant guidance and leading practices to identify any risks and challenges that could affect acquisition outcomes.[4] In addition, we used the program questionnaire responses, supporting documentation, and program information from the Dashboard to create summaries for the 10 largest programs. We also interviewed program officials and DOD officials within the offices of the DOD CIO and the Under Secretary of Defense for

[4]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: Feb. 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Cybersecurity Test and Evaluation Guidebook* Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense, *Operation of the Defense Acquisition System*, Instruction 5000.02T (Washington, D.C.: Jan. 7, 2015); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 [incorporating change 2 (Jan. 24, 2020)] (Washington, D.C.: Feb. 2, 2017); NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015); Department of Defense, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, Instruction 5200.44 (Nov. 5, 2012, incorporating change 3, Oct. 15, 2018).

Acquisition and Sustainment USD(A&S) to gain additional insight related to information reported by programs.

To address the third objective, we reviewed actions DOD has taken to implement previously identified legislative and policy changes that could affect its IT acquisitions. Specifically, we reviewed information provided by department officials about their plans to implement these changes and requested status updates. We reviewed information associated with the department's efforts to finalize strategies for its business system and software acquisition pathways; to implement modern approaches to software development such as transitioning to Agile; and to reorganize the responsibilities of the former Chief Management Officer (CMO) throughout the department. We focused our objective on the reorganization of the former CMO responsibilities and included updated information on other matters in the report background. We also interviewed DOD officials with the offices of the DOD CIO, USD(A&S), the Under Secretary of Defense (Comptroller)/Chief Financial Officer (USD(C)), and the Director of Administration and Management (DA&M) to learn more about the department's plans and actions it had taken and to assess the implications of these changes. Appendix I provides a more detailed discussion of our objectives, scope, and methodology.

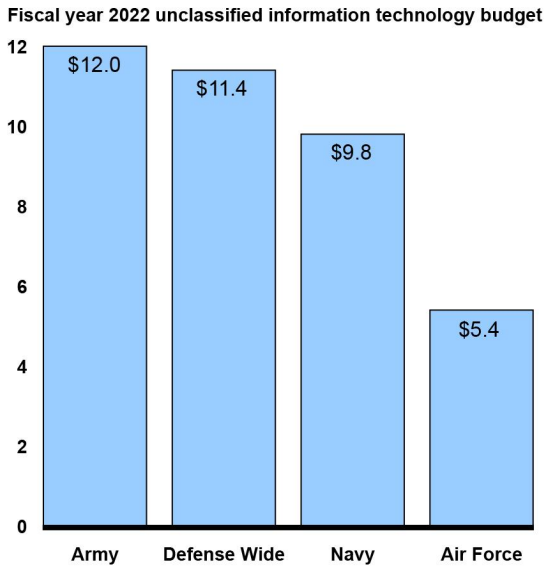
We conducted our work between July 2021 and June 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our 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, including investments in business, communications, and command and control systems. DOD requested approximately $50.6 billion for the total FY 2022 IT and Cyber Activities Budget, according to its FY 2022 budget request. The total unclassified DOD IT budget is $38.6 billion.

Figure 1 shows the amount of DOD's total unclassified requested FY 2022 IT budget (of $38.6 billion) that the department plans to spend by military department and defense wide.[5]

Figure 1: Department of Defense (DOD) Fiscal Year 2022 Unclassified IT Budget by Military Department and Defense Wide (projected)



Source: GAO analysis of DOD information technology budget information. | GAO-22-105330

DOD's Policy and Framework for Managing Major IT Acquisitions

In January 2020, DOD updated its acquisition policy to create an acquisition framework to enable flexible and responsive acquisitions. The reissued DOD Instruction 5000.02 established the new adaptive acquisition framework (AAF) as well as high-level policy for the AAF, and

[5]This figure does not include DOD's classified budget request. In June 2021, GAO reported a similar analysis with data provided with DOD's FY 2021 budget request (see 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]). Comparable data were not publicly available as part of DOD's FY 2022 budget request. Accordingly, these data may not be directly comparable to data included in previous GAO reports. "Defense wide" refers to entities outside of the military departments, such as defense agencies (e.g., the Defense Logistics Agency and Defense Health Agency).

assigned roles and responsibilities to acquisition officials.[6] The instruction described a transition from the department's previous acquisition approach, and the department subsequently issued new policies to continue replacing the old approach, currently in DOD Instruction 5000.02T.[7]

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

While Instructions 5000.02 and 5000.02T establish 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: the business systems acquisition pathway and the software acquisition pathway.

Business Systems Acquisitions Pathway

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

In January 2020, DOD updated the instruction for the defense business systems acquisition pathway to align defense business system acquisitions with the AAF. Instruction 5000.75 establishes policy for using the five-phase business capability acquisition cycle for business system requirements and acquisitions.[8] While maintaining the general structure of

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

[7]Department of Defense*, Operation of the Defense Acquisition System,* Instruction 5000.02T [incorporating change 10 (Dec. 31, 2020)] (Washington, D.C.: Jan. 7, 2015).

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

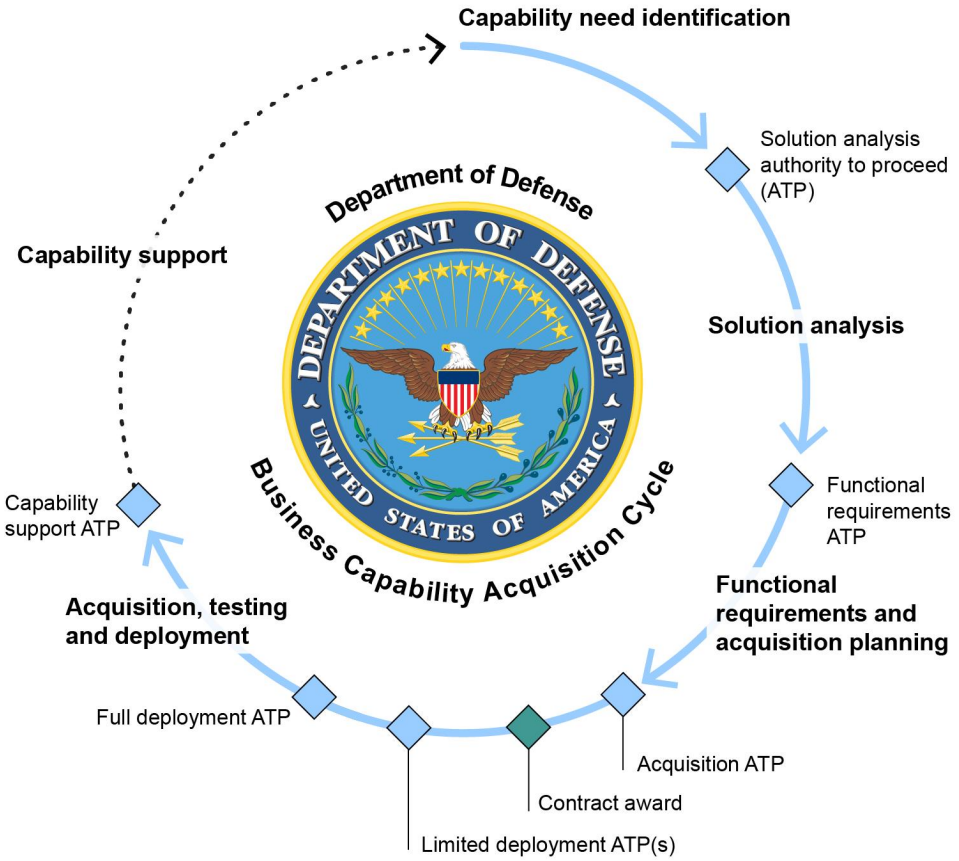
the defense business systems pathway, the 2020 update removed certain oversight requirements and encouraged a tailored approach to each program. The 2020 update also enabled and encouraged acquisition officials to delegate decision-making down to the "lowest practical level."

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

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

Figure 2 shows DOD's business capability acquisition cycle under the business systems pathway.

Figure 2: DOD's Business Capability Acquisition Cycle



Source: Department of Defense Instruction 5000.75 (January 2020). | GAO-22-105330

Software Acquisition Pathway

Section 800 of the NDAA for FY 2020 mandated that DOD develop the software acquisition pathway.[9] In October 2020, the department issued guidance titled Operation of the Software Acquisition Pathway, Instruction 5000.87.[10] According to this instruction, the purpose of the pathway is to

[9]Pub. L. No. 116-92, § 800, 133 Stat 1198, 1478 (Dec. 20, 2019).

[10]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).

provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software.

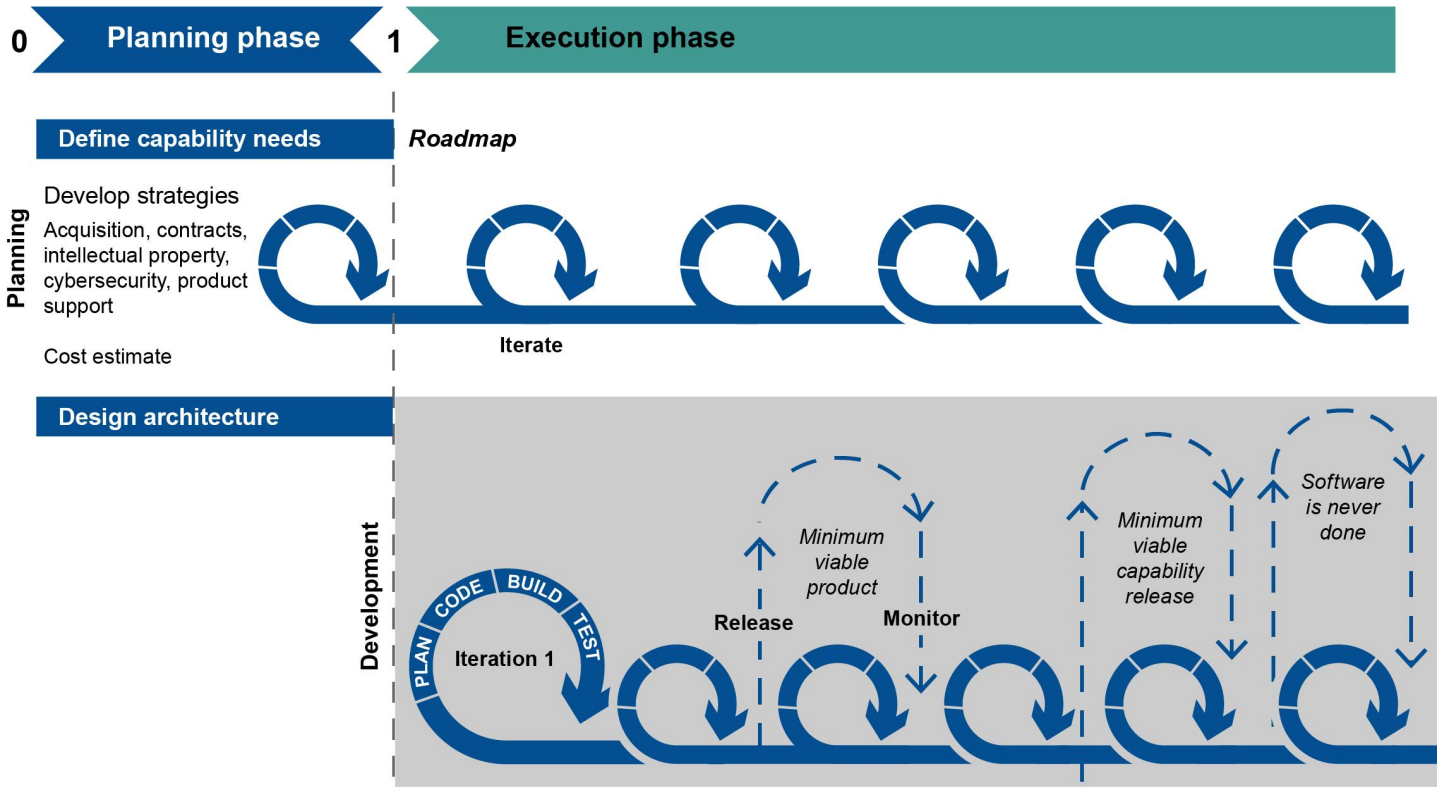
Designed for software-intensive systems, the pathway contains two paths: the applications path for deploying software running on commercial hardware and cloud platforms and the embedded software path for the upgrades and improvements to software embedded in military systems. The guidance in DOD Instruction 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.

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.[11] 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 user needs.

Under DOD Instruction 5000.87, the software acquisition pathway contains a planning phase and an execution phase. Figure 3 shows the pathway's two phases.

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

Figure 3: DOD's Software Acquisition Pathway



Source: Department of Defense Instruction 5000.87 (October 2020). | GAO-22-105330

DOD's Initial Implementation of Agile Software Development

Consistent with studies recommending DOD's transition toward Agile software development[12] and to implement statutory mandates to help

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

enable its transition,[13] the department has begun implementing Agile as part of its software modernization initiatives.

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

Further, sections 873 and 874 of the NDAA for FY 2018 mandated that DOD implement two pilot programs to enable selected acquisition programs to embrace Agile practices.[14] DOD provided participating programs with training and tailored Agile guidance. The section 874 pilot lasted 1 year and DOD has shared lessons learned from the pilot related to the implementation of these practices. The section 873 pilot targeted large acquisition programs and is to continue through FY 2023.

In February 2022, DOD issued a software modernization strategy.[15] The strategy is intended to support DOD's efforts to improve software delivery through modern infrastructure and platforms and enable these improvements by transforming processes and developing personnel. The strategy includes three goals:

- Accelerate the DOD enterprise cloud environment;
- Establish a department-wide software factory ecosystem; and
- Transform processes to enable resilience and speed.

The department has also established a Software Modernization Senior Steering Group to lead the collaboration of software modernization

[13]Section 873 and 874 of the NDAA for FY 2018 established two Agile pilot programs, Pub. L. No. 115-91, §§ 873-874, 131 Stat. 1283, 1498-1503 (Dec. 12, 2017). Section 800 of the NDAA for FY 2020 established a software acquisition pathway that, according to DOD Instruction 5000.02, is to, among other things, support Agile practices. Pub. L. No. 116-92, § 800, 133 Stat. 1478 (Dec. 20, 2019).

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

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

activities in support of the software modernization strategy. The group is to include membership from offices across the department, including the office of the DOD CIO; Under Secretary of Defense for Acquisition & Sustainment (A&S); Under Secretary of Defense for Research and Engineering; Under Secretary of Defense for Intelligence & Security; Director, Operational Test and Evaluation; and Director, Cost Assessment and Program Evaluation, as well as the military departments and services, Joint Chiefs of Staff, and the Defense Information Systems Agency.

DOD's Cybersecurity Guidance

DOD instruction 8500.01 describes cybersecurity requirements for all DOD acquisition programs containing IT.[16] 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. The instruction also includes guidance for high-level management of cybersecurity, technological requirements, and workforce considerations. DOD instruction 8510.01 documents specific guidance for IT risk management.[17]

Under 8510.01, all DOD IT systems must be categorized in accordance with Committee on National Security Systems Instruction 1253[18] and implement a corresponding set of security controls and assessments from National Institute of Standards and Technology (NIST) SP 800-53.[19] The guidance requires officials responsible for IT systems to identify resources needed to implement the risk management framework, develop and maintain milestones and a plan of action to address known

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

[17]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).

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

[19]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Revision 5 (Washington, D.C.: September 2020).

vulnerabilities, and designate an official responsible for authorizing the system's operation based on its risk posture. DOD 8510.01 clarifies that the risk management framework will inform but not replace acquisition processes for requirements development, procurement, and both developmental test and evaluation and operational test and evaluation.

Supply Chain Risk Management Guidance

NIST 800-161 provides guidance for federal agencies on identifying, assessing, selecting, and implementing risk management processes and mitigating controls to manage information and communications technology (ICT) supply chain risks.[20] The guidance describes foundational concepts, discusses ICT supply chain risk management processes and their integration into existing risk management processes, and provides a comprehensive set of baseline controls for organizations given their organizational and ICT needs. NIST recommends that high-impact systems follow the guidance,[21] but notes that agencies may choose to apply the guidance to lower-impact level systems as a result of interdependencies and the needs of individual systems. Furthermore, the guidance states that NIST 800-161 builds on foundational supply chain risk management practices and suggests agencies reach a base level of maturity before implementing more advanced practices.

In addition, DOD Instruction 5200.44[22] directs programs to implement supply chain risk management disciplines to manage the risks to system integrity and trust. The instruction does not require programs to include ICT considerations in system security plans or to develop separate plans for addressing supply chain risk management, as discussed later in the

[20]National Institute of Standards and Technology, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST SP 800-161 (Washington, D.C., April 2015).

[21]The National Institute of Standards and Technology defines systems as "high impact" if the loss of system confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

[22]Department of Defense, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, Instruction 5200.44 [incorporating change 3 (Nov. 5, 2012)] (Washington, D.C.: Oct. 15, 2018).

report.[23] In December 2020, GAO reported on the extent to which non-DOD federal agencies have implemented practices for providing an agency-wide approach to managing their supply chain risks.[24]

DOD's Chief Management Officer Position Repealed by Statute

In 2007, the DOD designated the Deputy Secretary of Defense as the department's Chief Management Officer (CMO). In addition, in 2008, the NDAA for FY 2008 established the position of deputy CMO. In 2016, the NDAA for FY 2017 established a standalone CMO position, effective February 1, 2018, that would be distinct from the Deputy Secretary of Defense and assigned a number of key responsibilities to the CMO.[25] In December 2017, the NDAA for FY 2018 codified the position in Title 10 of the U.S. Code.[26] Additional responsibilities and functions for the CMO were enacted in the NDAA for FY 2019.[27]

The CMO's responsibilities codified in section 132a of title 10, U.S. Code 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.

On February 1, 2018, the Secretary of Defense announced the establishment of a separate CMO position with responsibility for directing all enterprise business operations of the department and other duties as set forth in law. Congress and DOD created this position, in part, in

[23]In October 2021, DOD issued a memo in response to the NDAA for FY 2021 identifying required security measures for information systems identified as handling controlled unclassified information. This included additional enhancements associated with the NIST 800-53 supply chain protection security control area. Among other things, the memo called for components to ensure that information systems that process controlled unclassified information implement relevant security measures prior to March 1, 2022.

[24]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

[25]Pub. L. No. 114-328, § 901, 130 Stat. 2000, 2341 (Dec. 23, 2016).

[26]Pub. L. No. 115-91, § 910, 131 Stat. 1283, 1516-1519 (Dec. 12, 2017), codified at 10 U.S.C. § 132a.

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

response to our recommendations that called for such a position to be established.[28]

In December 2019, section 904 of the FY 2020 NDAA mandated an assessment of responsibilities and authorities of the CMO, including an independent assessment conducted by the Defense Business Board or experts selected by the Secretary of Defense.[29] Further, the Conference Report accompanying the FY 2020 NDAA stated that the conferees noted significant structural challenges in implementing the CMO position since its inception.[30]

In June 2020, the Defense Business Board reported that the CMO position neither delivered the level of department-wide business transformation envisioned in the legislation, nor met the expectations of multiple Secretaries of Defense, Deputy Secretaries of Defense, other senior officials, or the congressional defense leadership.[31] In short, the report stated the CMO had not been set up for success. The report also recommended that the CMO be "disestablished" and replaced with one of several alternatives.

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 officials, organizations, and elements of DOD and provide a report to Congress with any associated recommendations for legislative action by January 2022.[32] 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 a requirement that the responsibilities be transferred no later than January 2022.

[28]See for example, GAO-07-310, GAO-07-229T, GAO-06-1006T, and GAO-05-520T.

[29]Pub. L. No. 116-92, § 904, 133 Stat 1198, 1541 (Dec. 20, 2019).

[30]H. Conf. Rept. 116-333 at 1333 (Dec. 9, 2019).

[31]Defense Business Board, *The Chief Management Officer of the Department of Defense: An Assessment*, DBB FY 20-01 (Washington, D.C., June 1, 2020).

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

GAO Has Identified DOD's Business Systems Modernization Efforts as High Risk

DOD's business systems modernization efforts have been on our High Risk List since 1995, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments.[33] GAO's high-risk program focuses attention on government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement, or that are in need of transformation to address economy, efficiency, or effectiveness challenges. As we reported in March 2021, among other things, DOD has only partially met the leadership commitment criterion of our High Risk List.[34]

For example, we reported that department officials stated that, in March 2020, the department had established a Defense Business Systems and Enterprise Business Optimization Directorate within the office of the CMO. This new office was intended to assist the office of the CMO with implementing statutory requirements for, among other things, managing defense business systems. We also reported that, in October 2020, the department developed a draft management playbook intended to assist the former office of the CMO with effectively delivering its mission. The draft playbook included information such as performance measures associated with streamlining the defense business systems environment. As of March 2022, we have 13 recommendations that DOD has not yet implemented associated with this high-risk area.

The Federal IT Dashboard

A provision of what is commonly known as the Federal Information Technology Acquisition Reform Act requires that the Director of the Office of Management and Budget (OMB) make information on major federal IT investments of covered agencies (including DOD) publicly available, in

[33]For example, see our latest update to the High Risk List; GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021). In addition, see GAO, *High-Risk* Series, GAO-HR-95-1 (Washington, D.C.: Feb. 1, 1995) and additional work such as GAO-19-199 and GAO-19-157SP.

[34]GAO-21-119SP.

accordance with detailed OMB guidance.[35] This information is displayed on the federal IT Dashboard, a public, federal government website that includes information on the performance of major IT investments.[36] While OMB provides a general definition of a major IT investment, it gives each covered agency the flexibility to establish specific criteria.

According to officials from the office of the DOD CIO and DOD guidance,[37] the department's major IT investments include: (1) major defense acquisition programs[38] determined to be IT investments by the DOD CIO; (2) IT programs with a budget greater than $43 million for FY 2022 or greater than $569.2 million greater across the future years defense plan;[39] and (3) IT investments designated as major by department leadership.

Currently, the federal IT Dashboard displays information on the cost, schedule, and performance of major IT investments at 26 federal agencies. In addition, OMB requires each agency's CIO to submit ratings to the Dashboard, which, according to OMB's instructions, 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 OMB, other oversight bodies, and the general public to hold agencies accountable for mission-

[35]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).

[36]The General Services Administration's Office of Government-wide Policy took over management of the federal IT Dashboard, including the collection, analysis, and presentation of IT budget and performance data from OMB on March 21, 2022. GSA's FY 2019 budget justification included this change.

[37]Department of Defense, *FY 2023 Information Technology/Cyberspace Activities Budget Guidance* (Washington, D.C.: July 15, 2021). DOD officials stated that the FY23 Guidance reflects the latest guidelines applied to the FY22 list of major IT investments. DOD officials added that this definition of a "major" IT investment was not reflected in the FY22 guidance because it was implemented after the guidance was released.

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

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

related outcomes. We have issued a series of reports that have noted both the significant steps OMB has taken to enhance the oversight, transparency, and accountability of federal IT investments by creating the federal IT Dashboard, as well as issues with the accuracy and reliability of the data it contains.[40] Accordingly, we made recommendations to OMB to address these issues, which it has implemented.

GAO's Recent Reviews of DOD IT Systems

In 2020 and 2021, GAO reported on DOD's portfolio of major IT business systems and DOD's efforts to modify how it collects and reports acquisition program data.[41] Among other things, our 2021 report addressed the program risk ratings that DOD reported to the federal IT Dashboard. In June 2021, GAO made recommendations aimed at improving how DOD approaches both of these efforts.

OMB requires that each federal agency CIO rate the risk of its major IT investments on a scale of 1 to 5, with 1 reflecting more risk and 5 reflecting less risk. These ratings are to be reported on the federal IT Dashboard. In June 2021, GAO reported that some DOD IT programs could be underreporting risks.[42]

For example, we found that, of 22 programs that were actively using a risk register to manage program risks, our assessments of program risk for 10 programs reflected greater risk than reported by DOD. Among

[40]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).

[41]GAO, *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, GAO-21-182 (Washington, D.C.: Dec. 23, 2020); *Software Development: DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices*, GAO-21-351 (Washington, D.C.: June 23, 2021).

[42]GAO-21-351.

other things, DOD CIO officials stated that different approaches for assessing program risks was likely a factor in the difference between the DOD CIO's and our risk ratings.[43] Nevertheless, our assessments showed that some programs could be underreporting program risks.

We recommended that the DOD CIO revisit program risk ratings for its next submission to federal IT Dashboard for the programs where the DOD CIO's program risk ratings indicated less risk than GAO's assessment of program risk. DOD concurred with our recommendation. In January 2022, officials from the office of the DOD CIO stated that they asked the programs that had CIO risk assessments that indicated less risk than GAO's risk ratings to reassess their program risk ratings for their next submission to the federal IT Dashboard. As of March 2022, the recommendation remains open, and we will revisit the status of the recommendation after updates to program risk ratings are publicly available on the federal IT Dashboard.

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

We recommended that, in consultation with appropriate stakeholders, DOD ensure the data strategies and data collection efforts for the business system and software acquisition pathways define, collect, automate, and share, with the appropriate level of visibility, the metrics necessary for stakeholders to monitor acquisitions and that are critical to the department's ability to assess acquisition performance. DOD concurred with our recommendation. In October 2021, an official from DOD's Washington Headquarters Services provided a corrective action plan that described a number of actions intended to help address the

[43]GAO-21-351 describes our detailed approach for assessing program risk.

recommendation. This included establishing a software pathway data collection strategy and a reporting template and collecting data in October 2021 and April 2022. In addition, the plan stated that DOD would identify reporting thresholds and identify metrics for the business systems pathway by the third quarter of FY 2022 and document required data elements by the fourth quarter of FY 2022. As of March 2022, the recommendation remains open.

In addition, in June 2021, GAO reported on cybersecurity at the Defense Logistics Agency (DLA) in which we assessed critical DOD IT systems to determine whether they had fully addressed steps for cybersecurity risk management and made one recommendation aimed at ensuring systems had approved cybersecurity strategies.[44] As of March 2022, the recommendation remains open.

DOD IT Program Officials Reported Cost and Schedule Changes Due to Various Reasons

According to DOD's FY 2022 IT Dashboard data, the department plans to spend $8.8 billion on its portfolio of 25 major IT business programs between FY 2020 and 2022.[45] Based on questionnaire responses, 18 of the 25 major IT business programs reported experiencing a variety of cost or schedule changes since January 2020. Of these programs, 14 reported the extent to which program costs and schedules had changed, noting cost increases that ranged from $0.1 million to $10.7 billion and cost decreases that ranged from $15.5 to $46.3 million. Programs also reported schedule delays that ranged from 5 to 19 months.

Additionally, four programs reported rebaselining since January 2020 and another three programs reported that they expected a program rebaseline

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

[45]In June 2021, we released the 2021 "DOD IT Quick Look" report (GAO-21-351), which discussed 29 major DOD business IT programs that DOD reported to the federal IT Dashboard. As a result of program retirements and reclassifications, this report discusses 25 major IT business programs that DOD reported to the federal IT dashboard. This includes the 27 major IT business programs that DOD reported to the dashboard in June 2021 and excludes one program that the department no longer considered to be a major IT program and one program that the department planned to retire before FY 2022.

to occur.[46] Program officials attributed the changes and rebaselines to various factors, including requirement changes or delays, contracting developments, and unanticipated technical complexities.

Programs also reported performance data to the federal IT Dashboard. As of December 2021, all 25 programs identified operational performance metrics consistent with OMB guidance. However, 19 out of the 25 major DOD IT programs did not fully report data indicating progress they were making toward meeting their operational performance metrics. One program reported that it was not yet operational and therefore did not have progress measurements to report. Fourteen programs that did not report progress measurements were in more advanced life cycle phases[47] and would be more likely to have the ability to report operational performance measurements. Officials from the office of the DOD CIO stated they would work with programs to ensure they were reporting performance measurements in future submissions to the federal IT Dashboard.

DOD Planned to Spend $8.8 Billion on its Major IT Business Programs, FY 20 through FY 22

Based on our analysis of DOD's FY 2022 IT Portfolio submission to the federal IT dashboard,[48] DOD reported that the department spent $2.7 billion on its 25 major IT business programs in FY 2020. DOD also reported that it planned to invest $6.1 billion on these programs between FY 2021 and FY 2022. Table 1 shows total actual and planned expenditures for the portfolio of 25 major IT business programs for FYs 2020 through FY 2022, broken down by program and fiscal year.

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

[47]Officials from 13 of the 14 programs reported that the programs were in sustainment and an official from the one remaining program reported that it had most recently achieved full deployment ATP. Operations and sustainment is a term used by DOD to describe a stage of the program life cycle equivalent to operations and maintenance.

[48]According to the federal IT Dashboard, DOD submitted its data on June 22, 2021. GAO obtained DOD's IT Portfolio data from the Dashboard on August 26, 2021. As of December 31, 2021, the June 2021 data were the most current data publicly available on the Dashboard.

Table 1: DOD's Planned Expenditures for its 25 Major IT Business Programs from Fiscal Years (FY) 2020 through 2022, as of December 2021

Dollars in millions

Program	FY20 (actual)	FY21 (projected)	FY22 (requested)	3-year total
Department of Defense Healthcare Management System Modernization	573	720	980	2,273
Navy Enterprise Resource Planning	365	406	446	1,217
Global Combat Support System – Army	315	284	225	824
General Fund Enterprise Business System	170	167	152	490
Defense Enterprise Accounting and Management System – Increment 1	106	127	141	374
Navy Maritime Maintenance Enterprise Solution	107	113	117	338
Enterprise Business System	77	88	119	284
Defense Agencies Initiative	87	79	105	271
Defense Enrollment Eligibility Reporting System	98	104	69	271
Distribution Standard System	49	97	121	267
Global Combat Support System Marine Corps / Logistics Chain Management	68	74	70	211
Real-Time Automated Personnel Identification System and Common Access Card	74	77	60	211
Armed Forces Health Longitudinal Technology Application	80	67	50	197
Defense Medical Logistics – Enterprise Solution	56	58	73	187
Defense Medical Information Exchange	53	54	55	162
Military Entrance Processing Command Integrated Resource System	59	49	52	160
Navy Standard Integrated Personnel System	69	35	48	151
Military Health System Information Platform	36	48	55	138
Defense Travel System	42	49	46	138
Navy Electronic Procurement System	32	44	43	119
Air Force Integrated Personnel and Pay System	46	41	32	119
Army Contract Writing System	25	35	53	113
Defense Civilian Personnel Data System	43	34	34	111
Maintenance Repair and Overhaul Initiative	22	36	48	106
Standard Procurement System	35	36	33	103
Totals:	**2,688**	**2,921**	**3,227**	**8,836**

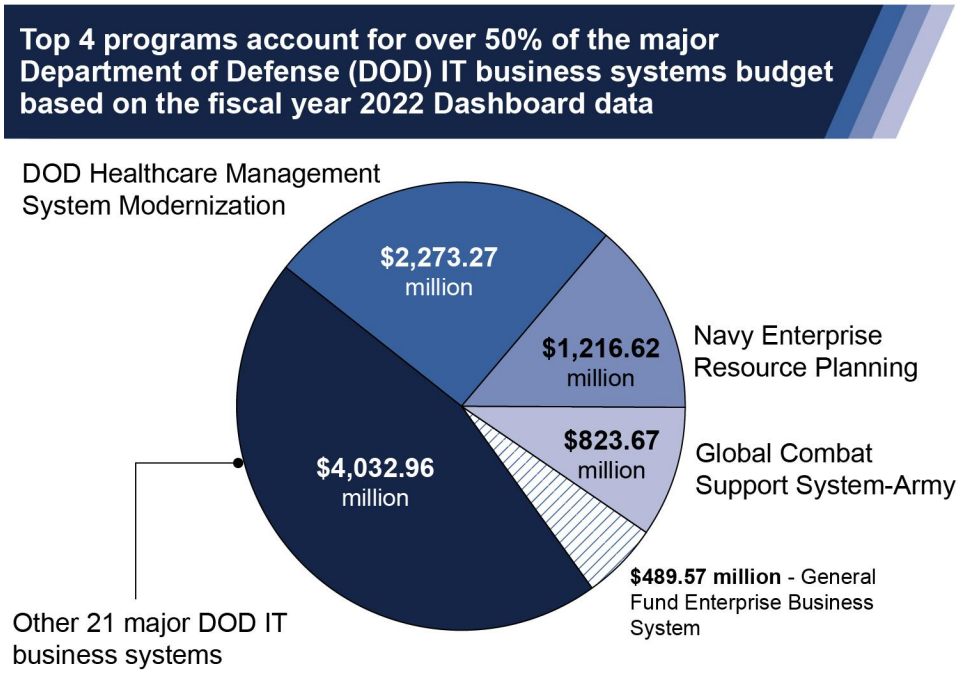
Source: GAO analysis of Department of Defense data reported to the federal IT Dashboard. | GAO-22-105330

Notes: Numbers do not always add due to rounding. In addition, this analysis uses data that DOD reported to the Office of Management and Budget's federal IT Dashboard. In June 2021, GAO reported similar analysis with data provided with DOD's FY 2021 budget request (see GAO-21-351). Comparable data were not publicly available as part of DOD's FY 2022 budget request. Accordingly, these data may not be directly comparable to data included in previous GAO reports. For example, the data available on the Dashboard did not include projections for the year after the FY 2022 budget request. In addition, since OMB reported the data on the Dashboard in June 2021, some programs may have subsequently experienced cost estimate changes that would be reflected in future submissions. In addition, according to a program official, funding reported on the federal IT Dashboard for Navy Standard Integrated Personnel System also includes funding associated with the

Department of Navy's effort to modernize its future Pay and Personnel capabilities, known as Navy Personnel and Pay.

The DOD Healthcare Management System Modernization (DHMSM), the Navy Enterprise Resource Planning (Navy ERP), the Global Combat Support System–Army (GCSS-A), and the General Fund Enterprise Business System (GFEBS) accounted for $4.8 billion (54 percent) of the $8.8 billion in actual and planned spending from FY 2020 through FY 2022. Figure 4 shows a breakdown of DOD's FY 2020 to FY 2022 major IT spending.

Figure 4: Top Four DOD IT Business Programs' Expenditures Compared to the Full Portfolio of Major IT Business Systems, Fiscal Year 2020 through Fiscal Year 2022



Source: GAO analysis of Department of Defense data reported to the federal IT Dashboard. | GAO-22-105330

Accessible Data Table for Figure 4

	Millions of Dollar
Department of Defense Healthcare Management System Modernization	2273.27
Navy Enterprise Resource Planning	1216.62
Global Combat Support System-Army	823.672
General Fund Enterprise Business System	489.57
The other 21 Major DOD IT Business Systems	4032.96

Based on these programs' responses to our questionnaire, these four programs are collectively in more mature stages of their program life cycles. Navy ERP, GCSS-A, and GFEBS officials reported that their programs are currently in sustainment.[49] DHMSM officials stated that the next program acquisition milestone is full deployment ATP.[50] In addition, DHMSM, Navy ERP, and GFEBS each reported changes to their planned costs since January 1, 2020. Regarding these programs:

- DHMSM program officials reported a cost increase of $10.7 billion for the planned life cycle from FY 2014 through FY 2034. Program officials also reported a schedule change but noted that these changes did not affect the program's original deployment date. Program officials attributed these changes to an updated deployment schedule, optimization, and COVID-19 pandemic impacts; the addition of a capability gap risk mitigation strategy; and reevaluation of deployment and management oversight risks.
- Navy ERP program officials reported a cost increase of $1.3 billion for the planned life cycle from FY 2022 through FY 2032. Program officials attributed this increase to changes to technical strategies and contract awards since January 1, 2020.
- GFEBS program officials reported an overall cost decrease of $46.3 million. Program officials attributed this change to a cost increase of $18.7 million associated with IT support during a transition to the Army Shared Services Center. Program officials also reported a

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

[50]Full deployment ATP is a decision point where the milestone decision authority approves deployment to the entire user community.

program management reduction in September 2021 that resulted in a cost reduction of $65 million.

Eighteen of the 25 Programs Reported Cost or Schedule Changes

As of January 2022, 18 of the 25 major IT business programs reported that they had experienced either cost or schedule changes since January 1, 2020. Specifically, 15 programs reported experiencing changes to planned costs and 13 programs reported experiencing changes to planned schedules. Ten programs reported both cost and schedule changes, including 8 programs that reported both cost increases and schedule delays. Moreover, officials from four programs reported that the programs rebaselined and officials from another three programs reported that they expected the program to rebaseline. Figure 5 shows cost and schedule changes reported by program officials.

Figure 5: DOD Program Officials Reported Cost and Schedule Changes since January 1, 2020

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-22-105330

Officials from 13 of the 15 programs that reported cost changes provided the associated dollar values.[51] Specifically, 11 programs reported total cost increases ranging from $0.1 million to $10.7 billion, while two programs reported total cost decreases ranging from $15.5 to $46.3 million respectively.

Officials from eight of the 13 programs that reported schedule changes provided the associated magnitude of those changes.[52] Specifically, seven programs reported delays ranging from 5 to 19 months. Officials from one program reported a schedule improvement of one release in the program's deployment schedule.

Program officials from the 18 programs that reported cost or schedule changes provided a variety of reasons for these changes, including:[53]

- **Requirements changes or delays.** Officials from nine programs reported cost or schedule changes due to new or unplanned requirements. This included requirements changes related to COVID-19, the creation of the U.S. Space Force, the addition of organizations or waves to program deployment schedules, unique entity identifiers, technical strategies, and cybersecurity.
- **COVID-19.** Officials from seven programs reported cost or schedule changes due to the COVID-19 pandemic. This included new requirements introduced as a result of pandemic conditions, the addition of COVID-19-related programs, and a longer than expected follow-on contract award.
- **Cloud migration and modernization changes.** Officials from five programs reported cost or schedule changes due to changes to cloud migration and modernization efforts. This included a transition to the Army Shared Services Center, Defense Civilian Human Resources Management System implementation, and capability consolidation.

[51]Two programs that reported cost changes did not provide dollar amounts for these changes.

[52]Five programs that reported schedule changes did not provide information about the extent of these changes.

[53]Program officials provided multiple reasons for cost or schedule changes. We included two instances or reported changes associated with the inclusion of COVID-related requirements in two different categories.

- **Contracting developments.** Officials from five programs reported cost or schedule changes due to contracting developments such as new software development contracts, contract modifications, and a follow-on contract award.
- **Unanticipated technical complexities.** Officials from four programs reported cost or schedule changes due to greater technical complexities than anticipated during development, identification of software bugs during quality assurance, software security concerns, and test defects and requirements traceability issues with the minimum viable solution software release.[54]
- **Workforce-related changes.** Officials from two programs reported cost or schedule changes due to cost reductions for program management personnel and workforce savings.

Seven Programs Rebaselined or Expected to Rebaseline

Officials from seven of the 18 programs reported that the program either rebaselined since January 2020 or they expected a rebaseline to occur. Repeated rebaselines may indicate that programs are not appropriately managing cost, schedule, or performance expectations or that they are experiencing other issues. For example, repeated rebaselines might be indicative of other challenges, such as unexpected technical complexity or issues with program contractors. Specifically, four programs reported a rebaseline:

- **Army Contract Writing System**. A program official reported that the program rebaselined in May 2020 due to a schedule delay of 7 months. An additional rebaseline occurred in December 2021 due to a schedule delay in March 2021 caused by software defects. A program official reported that this additional rebaseline resulted in a cost increase of $30.7 million and a schedule delay of 8 months.
- **Defense Agencies Initiative.** A program official reported that the addition of the U.S. Marine Corps to the program's FY 2020 deployment schedule resulted in a rebaseline. This official reported that the rebaseline was the result of a total cost increase of $306.5 million and a schedule delay caused by adding two releases.[55] The official added that the program anticipated an additional rebaseline

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

[55]The Defense Agencies Initiative program is an incrementally fielded software-intensive program comprised of multiple releases.

during the first quarter of FY 2022 due to the addition of Naval Special Warfare Center for FY 2021 and cloud hosting for FY 2023 or 2024. Program officials stated that this additional rebaseline is expected to reflect a schedule improvement of one release and an associated cost increase.

- **Maintenance Repair and Overhaul Initiative.** A program official reported that a delayed follow-on contract award during COVID-19, an extended conference room pilot, and a pre decisional expansion of software functionality and implementation resulted in a rebaseline. This official stated that the rebaseline was due to a cost increase of $35.2 million and an overall schedule delay of 6 months.[56]
- **Navy Electronic Procurement System.** A program official reported that greater than anticipated technical complexity during development activities delayed the system's limited deployment. As a result, the official stated that the program expects to replace the original contract. The program official stated that the rebaseline was due to a cost increase of $6.2 million and a schedule delay of 10 months.

In addition, officials from the following three programs reported anticipating a rebaseline:

- **Air Force Integrated Personnel and Pay System.** A program official reported that testing revealed defects that require time to correct. The program official stated that the program has developed a new schedule, which officials planned to provide to senior leadership in February 2022. The official stated that officials do not plan to rebaseline the program until senior leadership provides direction on schedule and funding.
- **Defense Medical Logistics – Enterprise Solutions.** A program official stated that schedule delays due to COVID-19 requirements, financial system modernizations, and issues related to the prime development contractor are expected to result in a program rebaseline.
- **Distribution Standard System.** A program official stated that a rebaseline may occur in 2022. The rebaseline will be intended to align project schedule and costs due to pandemic conditions abating and a more predictable forecast for the remainder of the program.

[56]The Maintenance, Repair and Overhaul Initiative experienced a 12-month delay at the full deployment ATP; this was later reduced to a 6-month delay at the capability support ATP.

DOD IT Programs Had Not Fully Reported Required Performance Data

OMB requires major IT programs to submit major IT business case details to the federal IT Dashboard.[57] These submissions include, among other things, program-specific information about operational performance. These operational performance metrics are intended to demonstrate an investment's delivery of expected value in support of an agency's needs or strategic plan.

As of December 2021,[58] we found that the 25 major IT business programs identified 172 operational performance metrics consistent with OMB guidance in their business case detail submissions. However, our analysis found that 19 of the 25 programs did not fully report progress relative to these metrics, including 11 programs that did not report any data. DOD CIO officials stated they would work with programs to ensure they report performance measurements in future submissions to the federal IT Dashboard, as appropriate.

Programs Had Identified Operational Performance Metrics Consistent with OMB Guidance

OMB requires IT programs to submit current information on program operational performance to the federal IT Dashboard. According to OMB's FY 22 IT Budget Capital Planning Guidance, programs must report a minimum of five operational performance metrics consistent with the following four categories:

- **Customer satisfaction.** These metrics are intended to measure an investment's ability to deliver its goods or services. Programs must report a minimum of one metric under this category.
- **Strategic and business results.** These metrics are intended to measure an investment's effectiveness or its contribution to the organization's achievement of strategic goals, fulfillment of its mission,

[57]Office of Management and Budget, *FY22 IT Budget - Capital Planning Guidance*, (Washington, D.C.: Nov. 16, 2020).

[58]GAO obtained DOD's reported operational metrics from the federal IT Dashboard on August 26, 2021. According to the Dashboard, the data was most recently updated as of May 18, 2021.

and/or meeting service level agreements with its customers. Programs must report a minimum of three metrics under this category. Additionally, at least one metric must contribute to a strategic objective[59] or agency priority goal.[60]

- **Financial performance.** These metrics are intended to compare an investment's current performance with a pre-established cost baseline. The metric also supports periodical reviews for reasonableness compared to benchmarks or similar investments. Programs are not required to report a metric under this category.
- **Innovation.** These metrics are intended to measure an investment's means of maintaining or improving performance in terms of customer satisfaction, strategic and business results, and financial performance. Programs are not required to report a metric under this category.

As of December 2021, each of the 25 DOD business IT programs had identified, at a minimum, the required number of operational performance metrics in each of the required categories. In total, the programs reported 172 operational performance metrics (an average of 6.9 metrics per program) consistent with OMB's guidelines for operational performance metric categories. For example:

- Distribution Standard System reported six operational performance metrics: four strategic and business results metrics, one customer satisfaction metric, and one financial performance metric. This includes metrics associated with providing customers needed functionality on time and cost performance.
- Enterprise Business System reported five operational performance metrics: four strategic and business results metrics and one customer satisfaction metric. This includes metrics associated with responsiveness to critical priority incidents and system availability.

As a result of identifying operational performance metrics consistent with OMB guidance, programs have taken the initial steps needed to support more effective insight into and oversight of their programs.

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

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

Programs Reported Mixed Progress on Operational Performance Metrics; Nineteen Had Not Fully Reported Data

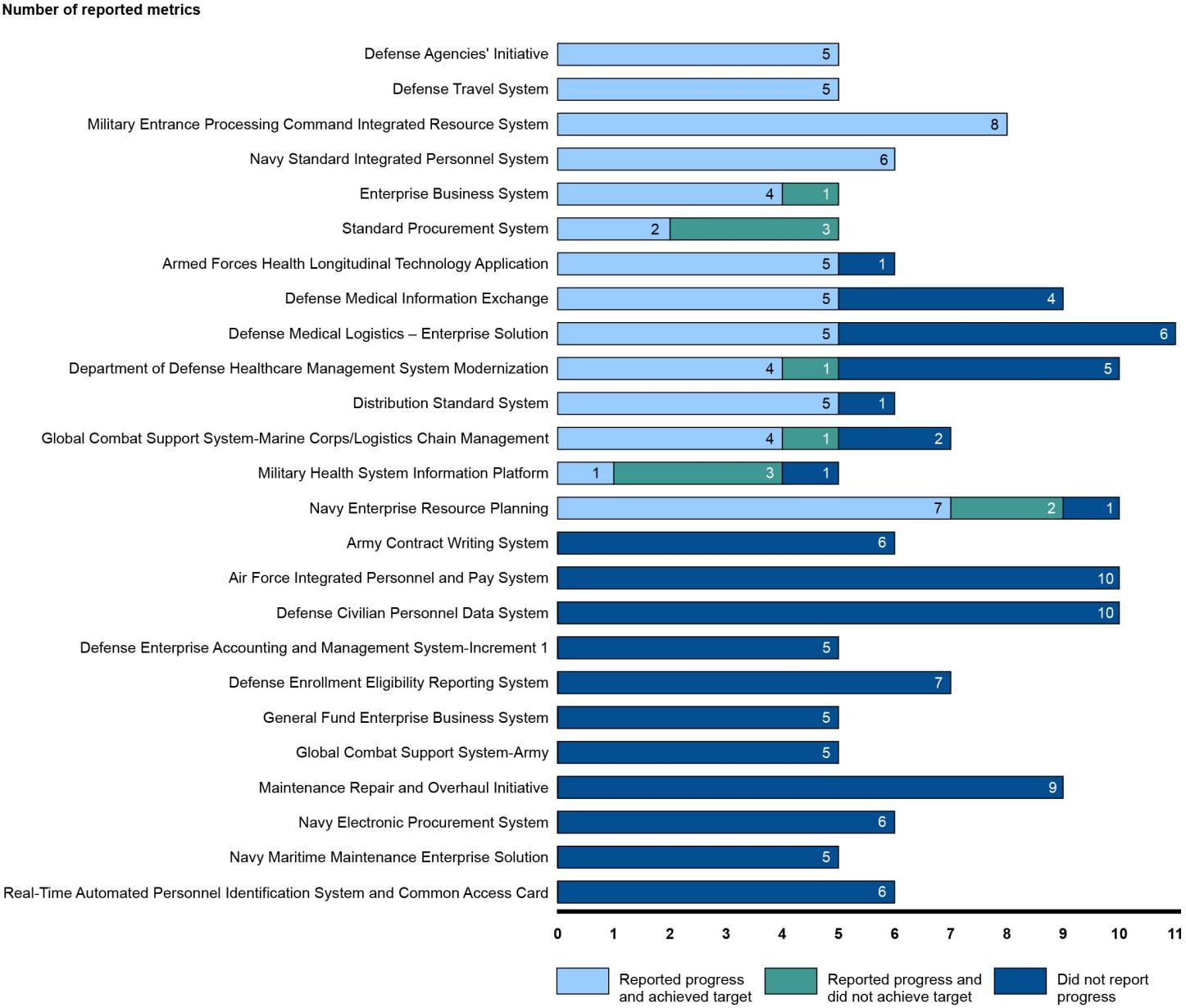
OMB's guidance further calls for programs to report actual operational performance measurements to track progress toward achieving operational performance goals.[61] Additionally, OMB's guidance states program submissions must include operational performance targets for the current fiscal year and a measurement condition.[62]

Out of the 25 major DOD IT programs, 19 programs did not fully report on the extent to which they achieved their operational performance targets. Specifically, eight programs reported incomplete data and 11 programs did not report any data. Of the programs that reported on the extent to which they achieved their operational performance metrics, four programs reported achieving all targets and 10 reported achieving some of their targets. Figure 6 shows a breakdown of programs' reported operational performance metrics and their progress toward achieving their targets.

[61]Office of Management and Budget, *FY22 IT Budget - Capital Planning Guidance*, (Washington, D.C.: Nov. 16, 2020).

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

Figure 6: Department of Defense Major IT Business Programs' Performance Measurement Results Reported to the Federal IT Dashboard, as of December 2021



Source: GAO analysis of Department of Defense data reported to the federal IT Dashboard. | GAO-22-105330

Accessible Data Table for Figure 6

Program Name	Achieved	Not Achieved	Did not Report Progress
DEFENSE AGENCIES INITIATIVE	5	0	0
DEFENSE TRAVEL SYSTEM	5	0	0
MEPCOM Integrated Resource System	8	0	0
Navy Standard Integrated Personnel System	6	0	0
Enterprise Business System	4	1	0
STANDARD PROCUREMENT SYSTEM	2	3	0
Armed Forces Health Longitudinal Technology Application	5	0	1
Defense Medical Information Exchange	5	0	4
Defense Medical Logistics – Enterprise Solution	5	0	6
Department of Defense Healthcare Management System Modernization	4	1	5
DISTRIBUTION STANDARD SYSTEM	5	0	1
GLOBAL COMBAT SUPPORT SYSTEM-MARINE CORPS/LOGISTICS CHAIN MANAGEMENT	4	1	2
MHS Information Platform	1	3	1
Navy Enterprise Resource Planning	7	2	1
Army Contract Writing System	0	0	6
Air Force Integrated Personnel and Pay System	0	0	10
DEFENSE CIVILIAN PERSONNEL DATA SYSTEM	0	0	10

Program Name	Achieved	Not Achieved	Did not Report Progress
Defense Enterprise Accounting and Management System-Increment 1	0	0	5
DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM	0	0	7
General Fund Enterprise Business System	0	0	5
Global Combat Support System-Army	0	0	5
Maintenance Repair and Overhaul Initiative	0	0	9
Navy Electronic Procurement System	0	0	6
NAVY MARITIME MAINTENANCE ENTERPRISE SOLUTION	0	0	5
REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM AND COMMON ACCESS CARD	0	0	6

Note: Operational performance metric data reported for individual programs on the federal IT Dashboard contain more metrics than are depicted in the figure. We excluded operational performance metrics that were marked as closed from this analysis. The Maintenance Repair and Overhaul Initiative program did not have measures to report because, according to Dashboard data, the program was not yet in production. For this assessment, we counted it as a program that did not report progress.

As noted above, 19 of the 25 programs did not fully report progress on their operational performance metrics. Programs in earlier life cycle stages might not have complete progress measurements available for their operational performance metrics, while programs in later life cycle stages would likely have a greater ability to report progress measurements. Officials from these 19 programs reported that the programs were in varying life cycle stages. Specifically,

- Officials from 13 programs reported that the programs were in sustainment,
- Officials from three programs reported that the programs had most recently achieved the limited deployment ATP milestone,

- An official from one program reported that the program had most recently achieved full deployment ATP,
- An official from one program reported that the program had most recently achieved acquisition ATP, and
- An official from one program reported that the program had most recently achieved the decision authority authorizes entry into planning phase milestone.

Officials in the office of the DOD CIO stated that programs that have operational performance measures should be reporting them to the Dashboard.[63] They added that there were multiple factors that could have led to programs not reporting the metrics, including a reorganization that shifted responsibilities of IT investment management between different offices and confusion about the reporting requirement due to personnel turnover. They stated that they are working with the components to resolve these issues and will revisit the program submissions to determine which programs should be reporting measures and ensure they report them in future submissions to the federal IT Dashboard.

Nevertheless, by reporting only incomplete operational performance data to the federal IT Dashboard, DOD limits the understanding of how programs are performing for stakeholders, federal agencies, and the public and limits the ability of Congress to conduct effective external oversight.

Program Officials Reported Using Software Development Approaches That May Limit Risks, but Did Not All Have Cybersecurity and Supply Chain Plans

As of February 2022, DOD program officials reported using approaches that may help to limit risks to cost and schedule outcomes for all 11 of the 25 major IT business programs we assessed were most likely to be

[63]Programs report their data to the Office of the DOD CIO before DOD CIO submits the data to OMB.

actively developing new software functionality.[64] For example, program officials for all 11 programs reported using a variety of iterative software development practices. In addition, officials from eight of the 11 programs reported using Agile as a software development approach, which can support continuous iterative software development as recommended by the Defense Science Board.[65] Officials for five of the programs also reported delivering software functionality every 6 months or less, as called for in OMB guidance.

However, officials from 10 of the 25 programs did not demonstrate that they had an approved cybersecurity strategy as required by DOD.[66] These strategies are intended to help ensure that program staff are planning for and documenting cybersecurity risk management efforts, which begin early in the programs' life cycle.

Further, officials from 15 of the 25 programs also did not demonstrate that they had a system security plan that addresses information and communications technology (ICT) supply chain risk management, as

[64]For the purposes of this assessment, we considered programs to be actively developing new software functionality if program officials reported they were actively developing new software functionality, reported they had not yet reached full deployment ATP, or reported a life cycle phase of "other" and indicated they were in the process of migrating functionality to the cloud. Of the 11 programs that we identified, officials from seven programs reported they were actively developing new software functionality. An official from one program reported that limited deployment ATP was the most recent milestone they had achieved. An official from one other program reported that the most recent milestone the program achieved was acquisition ATP. Officials from the two remaining programs reported a lifecycle phase of "other" and indicated that they were in the process of migrating functionality to the cloud. Officials from the other 14 programs reported that their software development efforts were either intended to sustain existing functionality or involved minor enhancements to a program currently in sustainment or reported that their program had proceeded past full deployment ATP or its equivalent milestone (e.g., capability support). The 11 programs we identified were the ones we expected to most likely be using the more modern approaches to software development discussed in this section of the report.

[65]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: Feb. 2018). According to the Defense Science Board, the Agile software development approach is when software is delivered in increments throughout the project, but built iteratively by refining or discarding portions as required based on user feedback.

[66]Department of Defense, *Cybersecurity*, Instruction 8500.01 (Washington, D.C.: Mar. 14, 2014; rev. Oct. 7, 2019).

called for by the National Institute of Standards and Technology.[67] Such plans, whether developed as standalone plans or integrated into other program plans, are important for managing supply chain risks and focusing appropriate resources on the most critical functions and components based on requirements and their risk environment.

Program officials also reported facing a variety of associated challenges related to DOD's major IT business programs. These challenges included budget constraints, changing customer requirements, and updated cybersecurity requirements that posed a challenge for current business practices. DOD officials stated that they recognize these challenges and the department is taking steps to address them.

Program Officials Reported Using Recommended Software Development Practices

Officials for Programs Developing Software Reported Using a Variety of Recommended Iterative Practices

Program officials from all 11 programs that we identified as actively developing new software functionality reported using a variety of recommended iterative development practices that could result in cost or schedule benefits. In February 2018, the Defense Science Board recommended that DOD implement certain iterative software development practices for its IT programs.[68] According to the Defense Science Board report, the main benefit of iterative development is the ability to catch errors quickly and continuously, integrate new code with ease, and obtain user feedback throughout the development of the application. Table 2 describes these iterative software development practices and the number of programs developing software that reported using them.

[67]National Institute of Standards and Technology, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Special Publication 800-161 (April 2015).

[68]The Defense Science Board provides independent advice and recommendations on science, technology, manufacturing, acquisition process, and other matters of special interest to the DOD to the Secretary of Defense. Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington, D.C.: February 2018).

Table 2: Officials from Major DOD IT Business Programs Developing Software Reported Using Recommended Development Practices

Development practices	Description	Number of programs that reported using each practice
Continuous iterative development	Approach that involves developing software in smaller blocks that a user community can incrementally evaluate. This incremental approach allows programs to rapidly incorporate updates into the software.	11 of 11
Delivery of minimum viable product, followed by successive next viable product	Development technique in which a new product or website is developed with sufficient features to satisfy early adopters.	10 of 11
Software documentation	Written text or illustration that accompanies computer software or is embedded in the source code.	10 of 11
Iterative development training for program managers and staff	Development of a training curriculum to create and train a cadre of software-informed program managers, sustainers, and software acquisition specialists.	7 of 11
Use of a software factory for development	Low-cost, cloud-based computing approach used to assemble a set of software tools enabling developers, users, and management to work together on a daily tempo.	4 of 11
Establishing the creation of a software factory as a key evaluation criterion in the source selection process	Development of a software factory as a factor in evaluating proposals for a potential government contractor.	1 of 11
None of the above[a]		2 of 11

Source: GAO analysis of Department of Defense questionnaire responses (December 2021). | GAO-22-105330

[a]Program officials who selected "none of the above" reported additional development practices and tools (e.g., "best of suite") that were not options for responses to the question associated with this table on the questionnaire we provided to program officials.

Officials for All Programs Developing Software Reported Using an Iterative Approach

In February 2018, the Defense Science Board recommended that DOD acquisition program staff implement continuous iterative software development approaches, such as Agile; development and operations (DevOps); and development, security, and operations (DevSecOps).[69] An iterative software development approach is a way of breaking down the development of large applications into smaller chunks. The board assessed that the iterative approach to software development is applicable to DOD and should be adopted as quickly as possible.

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

According to the Defense Science Board, continuous iterative software development 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 a waterfall approach may be appropriate in some circumstances, in May 2019, the Defense Innovation Board concluded that iterative software development may reduce cost growth compared to a waterfall approach.

Officials from all 11 of the programs that were actively developing new software functionality reported using at least one of the software development approaches that supports continuous, iterative development. An official from only one program reported that the program was using a waterfall approach. This official also reported that this program was using another software development approach that supports continuous, iterative development. Table 3 defines the software development approaches and shows the approaches that officials from the major DOD IT business programs that were developing software reported using.

Table 3: Officials from Major DOD IT Business Programs Developing Software Reported Using a Variety of Development Approaches

Approach	Description	Number of programs that reported using each approach[a]
Approaches that support continuous, iterative development		11 of 11
Agile	Software is delivered in increments throughout the project, but built iteratively by refining or discarding portions as required based on user feedback.	8 of 11
DevSecOps	This model combines “development,” “security,” and “operations,” and emphasizes communication, collaboration, and continuous integration between software developers and users.	7 of 11
Incremental	This model sets high-level requirements early in the effort and functionality is delivered in stages. Multiple increments each deliver part of the overall required program capability. Several builds and deployments are typically necessary to satisfy approved requirements.	6 of 11
DevOps	This approach combines “development” and operations”, emphasizing communication, collaboration, and continuous integration between both software developers and users.	2 of 11
Approaches that may or may not support continuous, iterative development		5 of 11[b]
Mixed	This approach is a combination of two or more different approaches.	5 of 11
Other	Other software development approach.	1 of 11

Approach	Description	Number of programs that reported using each approach[a]
Approach that likely does not support continuous, iterative development		1 of 11
Waterfall	This approach uses linear and sequential phases of development that may be implemented over a longer period of time before resulting in a single delivery of software capability.	1 of 11

Source: GAO analysis of Department of Defense questionnaire responses (December 2021). | GAO-22-105330

[a]Officials from some programs reported using multiple approaches.

[b]Not all program officials responded to every response option.

Officials for Five of the 11 Programs Reported Delivering Software At Least Every 6 Months

OMB guidance calls for certain agency CIOs and chief acquisition officers to ensure and certify that acquisition strategies and plans apply adequate incremental development, which OMB defines as planned and actual delivery of new or modified technical functionality to users at least every 6 months.[70] 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.[71] 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 face challenges when adjusting requirements to meet and adjust to customer needs.

Officials from five of the 11 programs that were actively developing new software functionality reported delivering software functionality every 6 months or less, as called for in OMB's guidance.[72] Officials from three programs reported that the average length of time between software releases was greater than 6 months. For the remaining three programs, officials reported either that they did not know the average number of

[70]At DOD, the Under Secretary of Defense for Acquisition and Sustainment is the chief acquisition officer. OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (Washington, D.C.: June 10, 2015). OMB's guidance applies to agencies covered by the Chief Financial Officers Act and their divisions and offices, except where otherwise noted.

[71]Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 3, 2019).

[72]One program reported an average length between releases of between 1 to 6 months, and checked off both the answers 1 to 3 months, and 4 to 6 months.

months between releases or that the practice was not applicable to their program.[73] An official from one of these three programs reported that the program was in the planning phase and had not yet issued a release, while an official from another program reported that they plan to have only one release. An official from the third program responded "not applicable or don't know" because, according to this official, program releases vary in size and frequency depending on their requirements and their priorities.

Officials for Two Legacy Programs Demonstrated Having Retirement Plans

According to DOD, a legacy business system is a system that the department plans to retire within 36 months.[74] In addition, according to the Software Engineering Institute (SEI), an organization should develop a plan to migrate legacy system software to a new system.[75]

Of the 25 programs the department considered to be major IT business programs, officials for two programs reported being legacy systems. Officials from these programs also reported having a plan for migrating to a new system and deactivating the legacy system and demonstrated that these plans existed.[76] As a result, these programs have better positioned themselves to successfully migrate their software functionality to new systems.

[73]"N/A or don't know" was a single option provided to program officials. Officials from one program reported that they were only planning one software release.

[74]Department of Defense, *Defense Business Systems Investment Management Guidance*, Version 4.1 (Washington, D.C.: June 26, 2018). This guidance defines legacy systems as systems that are to be terminated within 36 months of the date the program has its funds approved as part of the annual defense business system certification and approval process.

[75]Software Engineering Institute, *DOD Software Migration Planning*, CMU/SEI-2001-TN-012 (Pittsburgh, PA: August 2001). SEI is a nationally recognized, federally funded research and development center established at Carnegie Mellon University in Pittsburgh, Pennsylvania, to address software development issues.

[76]We did not evaluate the content of these plans. According to the plans, DOD intends to migrate all functionality from one of the programs to another program by the second quarter of FY 2024. DOD plans to retire the other program in the fourth quarter of FY 2024.

Program Officials Reported Conducting a Variety of Cybersecurity Tests, but Did Not All Have Cybersecurity and Supply Chain Plans

Officials from 15 of the 25 Programs Demonstrated Having Approved Cybersecurity Strategies

DOD Instruction 8500.01, *Cybersecurity*, requires that DOD major IT program officials use approved cybersecurity strategies.[77] These approved strategies are to include information such as cybersecurity and resilience requirements and key system documentation for cybersecurity testing and evaluation analysis and planning. These strategies are intended to help ensure that program staff are planning for and documenting cybersecurity risk management efforts, which begin early in the programs' life cycle.

As of February 2022, officials from 15 of the 25 major IT business programs demonstrated that they had an approved cybersecurity strategy.[78] Officials from seven of the 25 programs reported having a cybersecurity strategy but did not provide supporting documentation to validate that they had one. Program officials from the remaining three programs reported not having a strategy. Officials from two of these three programs reported having a planned date to develop an approved strategy. An official for the remaining program reported having no plans to develop a cybersecurity strategy because the program is a collection of previously independent applications, systems, and networks. The official noted that a comprehensive cybersecurity strategy was never required for those pieces.

Consistent with DOD guidance, officials from the office of the DOD CIO noted that only mission essential or mission critical programs were initially required to develop cybersecurity strategies. They added that DOD Instruction 5000.75 now requires business systems to develop cybersecurity strategies. They stated that they will follow up with the programs that did not provide an approved cybersecurity strategy and ensure that they have developed strategies, if appropriate. Nevertheless,

[77]Department of Defense, *Cybersecurity*, Instruction 8500.01 (Washington, D.C.: Mar. 14, 2014; rev. Oct. 7, 2019).

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

as discussed above, 10 of DOD's major IT programs did not demonstrate that they had an approved cybersecurity strategy.[79]

Until DOD ensures that these programs develop and document approved cybersecurity strategies, programs lack assurance that they are effectively positioned to manage cybersecurity risks and mitigate threats. As a result, programs are at increased risk of adverse cost, schedule, and performance impacts.

Officials from 22 of the 25 Programs Reported Conducting Cybersecurity Assessments

DOD Instructions 5000.75[80] and 5000.90[81] require major IT program staff to conduct cybersecurity assessments. Assessments for potential cybersecurity vulnerabilities are included in programs' cybersecurity testing and assessment processes. These assessments include cooperative vulnerability identification and a cooperative vulnerability and penetration assessment, but program staff may also conduct other types of assessments.[82]

In addition, according to DOD's Test and Evaluation Guidebook, cybersecurity testing and evaluation is intended to identify and mitigate exploitable system vulnerabilities.[83] The guidebook notes that early discovery of system vulnerabilities can facilitate remediation and reduce impact on program cost, schedule, and performance.

Officials from 22 of the 25 programs reported conducting some form of cybersecurity assessment. Officials from the remaining three programs reported that they did not conduct a cybersecurity assessment, with two

[79]In our June 2021 report on DLA cybersecurity (GAO-21-278), we similarly found that three of six DOD IT systems deemed critical to inventory management operations did not have approved cybersecurity strategies and we recommended they develop such strategies.

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

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

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

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

of the three reporting that they plan to complete a cybersecurity assessment. Officials from the remaining program reported that it is a collection of previously independent applications, systems, and networks and was never required to conduct assessments at the program level. Instead, these officials reported that cybersecurity assessments of the systems and networks are conducted at the component level. Table 4 summarizes the cybersecurity assessments that officials from major IT business programs reported using.

Table 4: Officials from Major DOD IT Business Programs Reported Conducting Cybersecurity Assessments

Cybersecurity assessments	Assessment description	Number of programs that reported each assessment
Full-system assessment	A test performed on a complete system to evaluate its compliance with specified requirements.	18 of 25
Cooperative assessment	Tests by independent assessors in which program office representatives, including developer support, are encouraged to participate to observe and characterize vulnerabilities, potential exploits, and follow-on fixes that may be needed. These assessments may involve any number of cybersecurity test events, such as system and network scans, vulnerability validation, penetration tests, access control checks, physical inspection, personal interviews, and reviews of system architecture and components.	18 of 25
Table top exercise	An activity in which key personnel are gathered to discuss and think through how they would respond to various simulated emergency or rapid response situations, often involving small collaborative teams that prepare briefings on potential threat scenarios. Based on those results, officials can create a path forward for addressing those scenarios, which could include administering additional testing and training, conducting follow-on analysis, or accepting the risk posed by the potential threat.	15 of 25
Assessment during developmental testing	A vulnerability assessment conducted early in the system life cycle intended to identify cybersecurity issues and vulnerabilities, facilitate remediation, and reduce impact on cost, schedule, and performance.	15 of 25
Assessment during operational testing	A vulnerability assessment conducted on production systems that supports the evaluation of system effectiveness, suitability, and survivability.	15 of 25
Component assessment	A test of individual hardware and software components or groups of related components.	14 of 25
Penetration test	A penetration test, which may or may not be conducted as part of a cooperative assessment, is a testing methodology in which independent assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.	13 of 25
Adversarial assessment	A cybersecurity developmental test and evaluation activity that uses realistic threat exploitation techniques in representative operating environments to evaluate a system's cyber survivability and operational resilience in a mission context.	11 of 25
Other[a]		2 of 25

Source: GAO analysis of Department of Defense questionnaire responses (December 2021). | GAO-22-105330

[a]Officials from two programs reported conducting other types of cybersecurity assessments including authority to operate renewals and risk and security impact assessments.

Officials from 24 of the 25 Programs Reported Conducting Required Cybersecurity Testing

DOD Instruction 5000.89[84] requires that DOD major IT program staff complete both developmental and operational cybersecurity testing.[85] Developmental cybersecurity testing and evaluation is intended to identify cybersecurity vulnerabilities before program deployment in order to help facilitate remediation of cybersecurity vulnerabilities and reduce the risk of a negative impact on cost, schedule, or performance. Cybersecurity operational testing evaluates operational programs for effectiveness, suitability, and survivability. However, program staff can perform other developmental and operational cybersecurity assessments.

Officials from 24 of the 25 programs included in our assessment reported conducting either developmental cybersecurity testing, operational cybersecurity testing, or both. Specifically, officials for four of these 24 programs reported conducting only developmental testing, officials for four programs reporting conducting only operational testing, and officials for 16 programs reported conducting both developmental and operational cybersecurity testing. Officials for the one remaining program out of the 25 reported conducting neither developmental nor operational testing. Officials from this program reported that they plan to perform a variety of tests by the end of the second quarter of FY 2024, including cooperative vulnerability and identification assessments and adversarial assessments for developmental testing. They stated that the program is too early in its life cycle to schedule a date for any operational testing. Programs may have conducted certain types of cybersecurity testing and not conducted other types due, in part, to being in different life cycle phases. For example, systems in an earlier life cycle phase may conduct developmental testing but may not be mature enough to conduct operational testing. Table 5 describes the extent to which program

[84]Department of Defense, *Test and Evaluation*, Instruction 5000.89 (Nov. 12, 2020).

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

officials reported conducting developmental and operational cybersecurity testing.

Table 5: Officials from Major DOD IT Business Programs Reported Conducting Developmental and Operational Cybersecurity Testing

Testing phase	Assessment conducted	Assessment definition	Number **of** programs conducting assessments
Developmental testing			20[a] of 25
	Cooperative vulnerability and identification	Cooperative vulnerability identification is a cybersecurity developmental test and evaluation activity that collects data needed to identify vulnerabilities and plan the means to mitigate or resolve them, including system scans, analysis, and architectural reviews.	14 of 25
	Adversarial assessment	An adversarial cybersecurity developmental test is a cybersecurity developmental test and evaluation activity that uses realistic threat exploitation techniques in representative operating environments.	6 of 25
	Other kind of assessment[b]		8 of 25
	No assessments		5 of 25
Operational testing			20[c] of 25
	Cooperative vulnerability and identification	A cooperative vulnerability and penetration assessment examines a system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities.	12 of 25
	Adversarial assessment	An adversarial assessment assesses the ability of a system to support its mission while withstanding cyber threat activity representative of an actual adversary.	8 of 25
	Other kind of assessment[d]		8 of 25
	No assessments		5 of 25
Neither developmental nor operational testing			**1 of 25**

Source: GAO analysis of Department of Defense questionnaire responses (December 2021). | GAO-22-105330

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

[b]Officials from eight programs reported conducting other types of assessments for developmental testing including code scans in the preproduction environment and contractor testing as part of the Agile process.

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

[d]Officials from eight programs reported conducting other types of assessments for operational testing including weekly vulnerability scans in the operational environment and operational testing and evaluation activities.

Officials for 10 of the 25 Programs Provided Plans Addressing ICT Supply Chain Risk Management

NIST Special Publication 800-161,[86] which documents leading government-wide practices, states that implementing consistent, well-documented, repeatable processes for systems engineering, information and communications technology (ICT) security practices, and acquisitions are foundational practices for improving the implementation of ICT supply chain risk management practices. The NIST guidance also calls for including ICT supply chain risk management considerations in system security plans or in a stand-alone supply chain risk management plan for individual systems.

In addition, DOD Instruction 5200.44 directs programs to implement supply chain risk management disciplines to manage the risks to system integrity and trust.[87] However, it does not require programs to include these considerations in system security plans or to develop separate plans for addressing supply chain risk management.

As of February 2022, officials from only 10 of the 25 major IT business programs demonstrated that they had a system security plan that addresses ICT supply chain risk management.[88] Officials from one of the 25 programs reported having a supply chain risk management plan but did not provide supporting documentation to validate that they had such a plan. Program officials from the remaining 14 programs reported not having supply chain plans. Officials from seven of these 14 programs reported that they planned to develop a security plan that would address ICT supply chain risk management by the end of 2022. Officials from the remaining seven programs reported not planning to develop one.

Program officials who reported not having a security plan to address supply chain risk management provided a variety of reasons for not developing such a plan for their programs. For example, officials from two

[86]National Institute of Standards and Technology, *Supply Chain Risk Management for Federal Information Systems and Organizations*, Special Publication 800-161 (April 2015).

[87]Department of Defense, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, Instruction 5200.44 (Nov. 5, 2012, incorporating change 3, Oct. 15, 2018).

[88]We did not evaluate programs' plans for addressing supply chain risk management. GAO currently has an ongoing review focused on assessing DOD's ICT supply chain risk management.

programs do not consider their programs to be ICT programs and did not see a need to develop such a plan. An official from another program stated the program has not created a security plan that addresses supply chain risk because the program uses technology provided by another agency.

According to officials from the office of the DOD CIO, DOD programs follow DOD Instruction 5200.44, which does not require programs to include ICT supply chain risk management considerations in system security plans or to develop separate plans for addressing supply chain risk management.[89] They stated that programs might address supply chain risk management in program protection plans. In addition, the officials acknowledged that ICT supply chain risk management is important, but noted that DOD CIO has focused its recent supply chain risk management efforts on weapons systems. They also stated that smaller programs might be able to rely on the Defense Information Systems Agency for supporting supply chain risk management efforts and added that larger programs will need to obtain dedicated staff to support their supply chain risk management efforts. However, as detailed above, 15 of DOD's major IT programs did not demonstrate that they had a supply chain risk management plan.

Until DOD ensures that these programs address supply chain risk management, whether documented in a stand-alone plan or as part of other program planning documentation, programs are less likely to be able to manage supply chain risks and mitigate threats that could disrupt operations. For example, they are at greater risk of threats such as malware-directed internal reconnaissance[90] and insecure or incomplete data deletion in a multi-tenant environment.[91]

[89]DOD Instruction 5200.44 states that risks to the trust in applicable systems shall be managed throughout the entire life cycle. It further states that risk management includes trusted systems and networks risk management principles and notes that risk management includes processes, tools, and techniques to employ protections that manage risk in the supply chain for components or subcomponent products and services when they are identifiable as having a DOD end-use.

[90]An adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it cannot be detected by externally placed intrusion detection systems.

[91]An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., a cloud computing environment).

DOD Is Taking Steps to Address Associated Challenges

As of December 2021, DOD program officials reported facing a number of challenges associated with the 25 major IT business programs. These officials provided open-ended answers to six questions about the challenges that the programs face.[92]

Officials from six of the 25 programs reported challenges related to budget constraints. An official from one program stated that budget constraints would hamper sustainment efforts and impact its schedule for maintaining software and hardware requirements. An official from another program stated that increasing cybersecurity costs are causing budgets to be focused on that area.

Officials from four programs reported challenges related to changing customer requirements. For example, an official from one program reported that customers make changes throughout the development process, making it difficult for them to keep up with the customer's requirements. In addition, a program official from another program reported that this leaves little time to meet administrative requirements.

Program officials from four programs reported challenges related to keeping up with the DOD's rapidly evolving cybersecurity requirements. For example, an official from one program reported that these changes to cybersecurity requirements can often interrupt current business practices. An official from another program also stated that with these changes often require additional resources allocated to this effort, which may take away resources from other parts of the program.

Lastly, officials from three programs reported issues related to software development and commercial off-the-shelf (COTS) software. One program official reported a challenge associated with not developing additional functionality for their program, and another program official reported that the use of COTS products does not always meet program requirements based on the capabilities of the product.

DOD recognizes the many challenges facing programs as they develop software and are taking steps to help address those challenges. For

[92]These responses were based on GAO analysis of six open-ended questions related to the challenges for each program. These six questions consisted of challenges related to risk ratings, cost and schedule changes, software development, planning, cybersecurity, and supply chain management.

example, as discussed, DOD has implemented a senior steering group to lead department-wide collaboration on software modernization activities. According to the group's December 2021 charter, its scope includes defining better ways to program and budget for software development and delivery and defining better ways to support cybersecurity, cyber survivability, and operational resilience requirements.[93]

In addition, in February 2022, DOD released its software modernization strategy.[94] Among other things, the strategy recognizes the need for DOD to review and modernize its requirements, budget, acquisition, and security processes to take advantage of new software development approaches and technologies. It also includes objectives associated with making software acquisition more Agile and managing COTS software for efficiencies and effectiveness.

DOD Has Begun Addressing the Repeal of the Chief Management Office Position and the Reorganization of Former CMO Responsibilities

The NDAA for FY 2021 eliminated the DOD CMO position, which previously had broad oversight responsibilities for DOD business systems. In September 2021, the Deputy Secretary of Defense directed a broad realignment of the responsibilities previously assigned to the CMO.[95] Table 6 describes selected responsibilities previously assigned to the CMO and identifies the new responsible entities.

[93]Department of Defense, *Software Modernization Senior Steering Group (SSG) Charter* (Dec. 9, 2021).

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

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

Table 6: Selected Responsibilities Previously Assigned to the Chief Management Officer (CMO) and New Responsible Entities, as of September 2021

Responsibility	New responsible entities
Establish a Defense Business Council (DBC), chaired by the CMO and the Department of Defense (DOD) Chief Information Officer (CIO), to provide advice to the Secretary of Defense on developing the defense business enterprise architecture, reengineering DOD business processes, developing and deploying defense business systems, and developing requirements for defense business systems.	Director of Administration and Management (DA&M); Undersecretary of Defense (Comptroller) (USD(C)); and DOD CIO.
Develop and maintain the DOD business enterprise architecture to guide the development of integrated DOD business processes.	DOD CIO
Ensure that each covered defense business system developed, deployed, and operated by DOD: (1) supports efficient business process, (2) is integrated into a comprehensive defense business enterprise architecture, (3) is managed to provide visibility into expenditures, and (4) uses an acquisition and sustainment strategy that prioritizes use of commercial software/business practices.	USD(C) and DOD CIO
Document and maintain common enterprise data, extract data from defense business systems, ensure data is same as data used for financial statements, provide data to DOD components, and ensure consistency of common enterprise data across DOD components.	USD(C) and DOD CIO
Serve as initial approving official for a covered defense business system proceeding into development (or as appropriate production or fielding) for a priority defense business system or a system of a defense agency or field activity or more than one military department.	USD(C) and DOD CIO
Serve as approving official for annual certification for continued development or sustainment of a covered defense business system and provide recommendations to the milestone decision authority for corrective actions.	USD(C) and DOD CIO
Designate priority defense business systems based upon complexity, scope and technical risks, and provide notification of designation to Congress.	USD(C) and DOD CIO
Issue supporting guidance (along with USD(A&S), DOD CIO, and military department CMOs) within respective areas of responsibility for the coordination of, and decision making for, the planning, programming, and control of investments in covered defense business systems.	USD(C) and DOD CIO

Source: GAO analysis of Department of Defense documentation.| GAO-22-105330

In January 2022, officials from DOD's office of the Director of Administration and Management, Office of USD(A&S), and DOD CIO described efforts underway to implement changes associated with the Defense Business Council (DBC), business systems investment management guidance, and the business enterprise architecture. Those efforts are:

- **DBC:** An official from DOD CIO stated that the department held the first DBC meeting under the new tri-chair arrangement in September 2021 and held three more meetings in November and December 2021. 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.

- **Business systems investment management policy and guidance:** An official from DOD CIO stated that the department plans to make minor changes to its defense business systems investment management policy and guidance for the FY23 investment review and approval cycle and plans to make more significant changes for the FY24 review and approval cycle. An official from the office of the USD(A&S) also stated that USD(A&S) plans to make adjustments to acquisition policies and guidance after more significant updates to the business systems investment management guidance are complete. This official noted that USD(A&S) officials are participating in efforts to update the business systems investment management policy and guidance.
- **Business enterprise architecture:** DOD officials stated that the department is reviewing its portfolio management processes and is working to integrate them with the business enterprise architecture and the associated information enterprise architecture. They added that their goal for this calendar year is to establish Office of the Secretary of Defense-level requirements and to better understand what functional owners need to improve how they manage their portfolios.

These officials also stated that while these changes are ongoing, DOD continues to certify and approve covered business system investments on an annual basis consistent with the requirements described in 10 U.S.C. Section 2222. GAO will continue to monitor DOD's efforts to redistribute the roles and responsibilities formerly assigned to the CMO through this series of annual reports mandated under the FY2019 NDAA and a review of reforms to improve DOD's efficiency and effectiveness mandated under the FY 2021 NDAA, as well as through monitoring associated with the DOD business systems modernization and DOD's approach to business transformation high-risk areas.

Conclusions

DOD relies heavily on the use of IT to protect the security of our nation. DOD requested and planned to spend $8.8 billion on its 25 largest IT business systems between FY 2020 and FY 2022. However, since 1995, we have identified DOD's efforts to modernize its business systems as high risk, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments.

For its major IT business programs, DOD identified operational performance metrics consistent with OMB guidance. As a result, programs have taken the initial steps needed to support more effective insight into and oversight of their programs. However, programs reported mixed progress on achieving operational performance metrics on the federal IT Dashboard and others did not fully report performance data to the Dashboard. By reporting incomplete operational performance metric data, DOD limits program accountability. Those data also help stakeholders, federal agencies, and the public understand how programs are performing. As a result, DOD limits the ability of Congress to conduct effective external oversight and the availability of this information for the public.

To DOD's credit, the major IT business programs are taking software development actions that can mitigate risks to cost and schedule and are taking steps to address reported challenges. These actions and other ongoing efforts have the potential to improve how DOD acquires and manages its IT systems. In addition, officials for two of the programs that reported being legacy systems have plans for migrating to a new system and deactivating the legacy system. As a result, these programs are better positioned to successfully migrate their software functionality to new systems.

However, while major IT business program officials reported conducting a variety of cybersecurity tests, programs did not all have cybersecurity strategies and security plans that address ICT supply chain risk management. Until DOD ensures that programs develop and document approved cybersecurity strategies, programs lack assurance that they are effectively positioned to manage cybersecurity risks and mitigate threats. As a result, programs are at increased risk of adverse impacts on the performance of its systems. Further, until DOD ensures that programs address ICT supply chain risk management, they are less likely to be able to manage supply chain risks and mitigate threats that could disrupt operations. For example, programs are at greater risk of threats such as malware-directed internal reconnaissance.

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

Recommendations

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

The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs report operational performance measures, as appropriate, as part of the department's submission to the federal IT Dashboard. (Recommendation 1)

The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs develop approved cybersecurity strategies, as appropriate. (Recommendation 2)

The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs develop plans that address information and communication technology supply chain risk management, as appropriate. (Recommendation 3)

Agency Comments

DOD provided written comments on a draft of this report. In its comments, the department concurred with our recommendations. The department stated that it is committed to acquisition reform and continual improvement for all of its systems with software-defined capabilities, including business systems. Specifically, it stated that the Office of the DOD CIO plans to redouble its efforts to ensure its largest IT programs report their operational metrics and status in a timely manner via the federal IT Dashboard. In addition, the department stated that it is committed to ensuring that all programs document their cybersecurity strategies and plans. Further, DOD stated that COVID-19 disruptions to supply chains increased its awareness of potential risks associated with inadequate supply chain risk management on its software acquisitions. The department added that, to continue to address this, the Office of the DOD CIO will encourage its IT programs to include these important considerations in the development of program plans. DOD's comments are reproduced in Appendix IV.

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 Under Secretary of Defense for Acquisition and

Sustainment. 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) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

Kevin Walsh
Director, Information Technology and Cybersecurity

List of Committees

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Jon Tester
Chairman
The Honorable Richard C. Shelby
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

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

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

The John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 included a provision for GAO to conduct annual assessments of selected Department of Defense (DOD) IT programs

Appendix I: Objectives, Scope, and Methodology

through March 2023.[1] Our specific objectives for this assessment were to: (1) examine how DOD's portfolio of major IT acquisition business programs has performed; (2) determine the extent to which the department has implemented software development, cybersecurity, and supply chain risk management practices; and (3) describe what actions DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, we initially considered the 27 major IT business programs that DOD had reported to the federal IT Dashboard as of December 2021. We then excluded two of these programs: one program that the department no longer considered a major IT program and one program that it planned to retire before FY 2022. We determined the universe of major IT business programs to be the remaining 25. These included programs that support key areas such as personnel, financial management, health care, and logistics.

To determine how much DOD reported spending on the programs in FY 2020 and planned to spend on these programs between FYs 2021 and 2022, we reviewed the department's FY 2022 submission to the Dashboard.[2] Based on these data, we calculated the total actual and planned expenditures for the programs during the 3-year period. In addition, we obtained programs' operational performance metric data, as

[1]Pub. L. No. 115-232, § 833, 132 Stat. 1636, 1858 (Aug. 13, 2018). This report is a companion to GAO-22-105230, also issued under this mandate, which discusses major DOD IT systems and DOD weapon programs.

[2]According to the federal IT Dashboard, DOD submitted its data on June 22, 2021. GAO obtained the department's major IT portfolio data from the Dashboard on August 26, 2021. As of December 31, 2021, the June 2021 data were the most current data publicly available on the Dashboard.

of December 2021,[3] from the Dashboard, and compared the data to OMB guidance. We also met with officials within DOD's Office of the Chief Information Officer (CIO) to determine reasons why programs were not reporting data in accordance with guidance.[4]

Further, we collected and analyzed key documents, reports, and artifacts pertaining to each program's life-cycle cost and schedule estimates, including acquisition program baseline reports, program schedule and rebaseline documentation,[5] and acquisition strategies, as well as program office responses to a GAO questionnaire we developed and administered to all 25 programs in October 2021. Programs provided their responses between October 2021 and December 2021 and we followed up with programs about their responses through February 2022. The questionnaire included questions about program costs and schedule changes that had occurred since January 2020.

To assess the reliability of the cost data DOD reported on the federal IT Dashboard for the 25 programs, we compared the data to cost information provided by the programs to identify any obvious inconsistencies. In addition, we prepared and sent program summaries to the 10 programs (of the 25) that had the largest planned expenditures over the 3-year period discussed in this report and asked program staff to review the summaries and confirm their accuracy. These program summaries are included in appendix II. To assess the reliability of the operational performance metric data, we met with officials from the office of the DOD CIO to determine whether programs submitted data consistently with DOD instructions. We determined that the budget data and operational performance metrics data were sufficiently reliable for our reporting purposes.

To help ensure the reliability of 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,

[3]GAO obtained DOD's reported operational metrics from the federal IT Dashboard on August 26, 2021. According to the Dashboard, the data was most recently updated as of May 18, 2021.

[4]Office of Management and Budget, *FY22 IT Budget - Capital Planning Guidance*, (Washington, D.C.: Nov. 16, 2020).

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

we conducted pretests of the questionnaire with three programs to ensure that the questions were clear, unbiased, and consistently interpreted. The pretests allowed us to obtain initial program feedback and helped ensure that officials within each program understood the questions. The questionnaire allowed respondents to submit their answers electronically. 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.

For the second objective, we sought information on the software development, cybersecurity, and supply chain risk management plans and practices used by the 25 IT programs via our questionnaire. Our identification of risks and challenges that might impact acquisition outcomes focused on the responses to the questionnaire from the 11 programs that we considered to be actively developing new software functionality. For the purposes of this assessment, we considered programs to be actively developing new software functionality if program officials reported they were actively developing new software functionality, reported they had not yet reached full deployment ATP, or reported a life cycle phase of "other" and indicated they were in the process of migrating functionality to the cloud.[6] We also collected and analyzed key documents pertaining to each of the 25 programs' approaches to cybersecurity and supply chain risk management, including cybersecurity strategies and system security plans. We followed up with officials within DOD's office of the CIO for clarification as to why programs did not provide the strategies and/or security plans. We selected the topics of software development, cybersecurity, and supply chain risk management practices to help ensure consistency with companion work being conducted under this same provision in the NDAA for FY 2019 that focuses on DOD weapon

[6]Of the 11 programs that we considered most likely to be actively developing new software functionality, officials from seven programs reported they were actively developing new software functionality. An official from one program reported that limited deployment ATP was the most recent milestone they had achieved. An official from one other program reported that the most recent milestone the program achieved was acquisition ATP. Officials from the two remaining programs reported a lifecycle phase of "other" and indicated that they were in the process of migrating functionality to the cloud. Officials from the other 14 programs reported that their software development efforts were either intended to sustain existing functionality or involved minor enhancements to a program currently in sustainment or reported that their program had proceeded past full deployment ATP or its equivalent milestone (e.g., capability support). The 11 programs we identified were the ones we expected to most likely be using the more modern approaches to software development discussed in the related section of the report.

programs[7] and to continue developing our body of work intended to improve supply chain cybersecurity across the federal government.[8]

Appendix III also provides additional information about DOD program leadership tenure for the 25 major IT business programs, including for the 11 programs we identified as actively developing new software functionality.

We aggregated program office responses and compared the aggregated information from our questionnaires to relevant guidance and leading practices[9] to identify where there were gaps. In doing so, we identified possible risks and challenges associated with not following guidance and leading practices that may affect acquisition outcomes relative to cost, schedule, and technical performance. We received responses to our program questionnaires from all of the programs we assessed between October and December 2021.

We did not validate all responses provided by the program offices, although we followed up with programs when responses were unclear or inconsistent. Where we discovered discrepancies, we clarified the responses accordingly.

To address the third objective, we reviewed actions DOD has taken to implement previously identified legislative and policy changes that could affect its IT acquisitions.[10] Specifically, we reviewed information previously provided by DOD about the department's plans to implement these changes and requested status updates, including on DOD's efforts

[7]GAO-22-105230.

[8]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

[9]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Cybersecurity Test and Evaluation Guidebook* Version 2.0, Change 1, (Washington, D.C.: Feb. 10, 2020); Department of Defense, *Operation of the Defense Acquisition System*, Instruction 5000.02T (Washington, D.C.: Jan. 7, 2015); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 [incorporating change 2 (Jan. 24, 2020)] (Washington, D.C.: Feb. 2, 2017); NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015); Department of Defense, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, Instruction 5200.44 (Nov. 5, 2012, Incorporating Change 3, Oct. 15, 2018).

[10]The previously identified legislative and policy changes are discussed in GAO-21-351.

to finalize strategies for its business system and software acquisition pathways; to implement modern approaches to software development such as transitioning to Agile; and to reorganize former CMO responsibilities throughout the department. The objective focused on DOD's efforts to reorganize former CMO responsibilities, while updates to other efforts are addressed either in the report background or will be addressed in ongoing GAO assessments.

To understand and assess the potential implementation of these changes, we reviewed policies, plans, and guidance provided by DOD; reports that DOD submitted to Congress; and internal program documentation. In addition, we interviewed officials within DOD's Office of the CIO, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, and Office of the Under Secretary of Defense for Acquisition and Sustainment. We also coordinated with the GAO team conducting a companion assessment examining major defense acquisition programs that was conducted under this same provision of the NDAA for FY 2019.[11]

We conducted this performance audit from July 2021 to June 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[11]GAO-22-105230.

Appendix II: Program Summaries

This appendix provides summaries for 10 of the 25 Department of Defense (DOD) major IT business programs included in our review. These 10 represented the programs that DOD reported as having the greatest actual and planned expenditures from fiscal year (FY) 2020 through FY 2022. Each summary provides a program description, describes essential information about the program, such as the lead DOD component and the acquisition pathway, and provides an overview of actual and planned expenditures and software development practices. Programs are listed in order of largest to smallest actual and planned expenditures.

Defense Health Agency – Department of Defense Healthcare Management System Modernization

Program description

DOD established DOD Healthcare Management System Modernization to acquire and field a configurable and scalable modernized electronic health record system to replace DOD legacy healthcare systems with an off-the-shelf electronic health record system intended to enable improved sustainability, flexibility, interoperability, and continuity of care.

Program essentials (as reported by program officials in November 2021)

Lead DOD component: Office of the Secretary of Defense

Program owner: Defense Health Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Limited deployment authority to proceed (ATP) (April 2020)

Next planned milestone: Full deployment ATP (Date is to be determined in coordination with the milestone decision authority)

Year investment began: 2014

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

CIO evaluation rating: 3 - Medium risk

Tables 7-9 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 7: Department of Defense Healthcare Management System's Fiscal Year 2020 through Fiscal Year 2022 Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	275.241	298.059	573.3
2021	385.715	334.024	719.739
2022	588.684	391.544	980.228
Total	**1249.64**	**1023.63**	**2273.27**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 8: Department of Defense Healthcare Management System's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	0 years, 10 months	3
Program executive	1 year, 10 months	4
Milestone decision authority	3 years, 1 month	3

Source: GAO analysis of DOD Healthcare Management System's questionnaire response, as of November 2021 | GAO-22-105330.

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

Software development practices	Program response
Software development approach	Agile, mixed, DevSecOps
Software releases to date	5
Planned releases	10
Average time between releases	4 to 6 months
Uses a software factory	No
Uses continuous iterative development	Yes

Delivery of minimum viable product	Yes

Source: GAO analysis of DOD Healthcare Management System's questionnaire response, as of November 2021. | GAO-22-105330.

Department of the Navy – Navy Enterprise Resource Planning

Program description

The Navy Enterprise Resource Planning Program is the Department of the Navy's financial system of record. The system is intended to streamline the Navy's business operations, focused on financial and supply chain management.

Program essentials (as reported by Navy Enterprise Resource Planning program officials in October 2021)

Lead DOD component: Department of the Navy

Program owner: Department of the Navy

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Full-rate production (full deployment decision) (December 2013)

Next planned milestone: Program is in sustainment

Year investment began: 2004

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

CIO evaluation rating: 4 - Moderately low risk

Tables 10-12 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 10: Navy Enterprise Resource Planning's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	0	365.129	365.129
2021	0	405.757	405.757
2022	0	445.736	445.736
Total	**0**	**1216.622**	**1216.622**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 11: Navy Enterprise Resource Planning's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	2 years and 2 months	4
Program executive	1 year and 5 months	4
Milestone decision authority	0 years and 9 month	3

Source: GAO analysis of Navy Enterprise Resource Planning's questionnaire response, as of October 2021. | GAO-22-105330

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

Software development practices	Program response
Software development approach	Agile, incremental, mixed, DevSecOps
Software releases to date	76 (quarterly releases)
Planned releases	>2 (major releases)
Average time between releases	1 to 3 Months
Uses a software factory	No
Uses continuous iterative development	Yes
Delivery of minimum viable product	Yes

Source: GAO analysis of Navy Enterprise Resource Planning's questionnaire response, as of October 2021. | GAO-22-105330

Department of the Army – Global Combat Support System-Army

Program description

Global Combat Support System-Army is intended to provide functional services to the business enterprise mission areas. The system is focused on property book, supply operations, tactical maintenance, and enterprise

aviation logistics, along with associated logistics management and tactical finance functionality.

Program essentials (as reported by Global Combat Support System-Army program officials in November 2021)

Lead DOD component: Department of the Army

Program owner: Department of the Army

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support ATP (March 2018)

Next planned milestone: Program baseline is in capability support, with an Increment 2 Aviation Log being in a limited deployment ATP (4th quarter 2022)

Year investment began: 2002

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

CIO evaluation rating: 5 - Low risk

Tables 13-15 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 13: Global Combat Support System-Army's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	66.419	248.672	315.091
2021	73.444	210.146	283.59
2022	64.01	160.981	224.991
Total	**203.873**	**619.799**	**823.672**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 14: Global Combat Support System-Army's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	2 years and 2 months	4
Program executive	1 year and 5 months	4
Milestone decision authority	0 years and 9 month	3

Source: GAO analysis of Global Combat Support System-Army's questionnaire response, as of November 2021. | GAO-22-105330

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

Software development practices	Program response
Software development approach	Incremental, mixed, DevOps, DevSecOps
Software releases to date	59
Planned releases	4 major quarterly and 8 minor per year
Average time between releases	1 to 3 months
Uses a software factory	No
Uses continuous iterative development	Yes
Delivery of minimum viable product	Yes

Source: GAO analysis of Global Combat Support System-Army's questionnaire response, as of November 2021. | GAO-22-105330

Department of the Army – General Fund Enterprise Business System

Program description

The General Fund Enterprise Business System is the 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 (as reported by General Fund Enterprise Business System program officials in October 2021)

Lead DOD component: Department of the Army

Program owner: Department of the Army

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support ATP

Next planned milestone: None

Year investment began: 2005

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

CIO evaluation rating: 5 - Low risk

Tables 16-18 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 16: General Fund Enterprise Business System's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	42.029	127.874	169.903
2021	12.486	154.913	167.399
2022	14.587	137.678	152.265
Total	**69.102**	**420.465**	**489.567**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 17: General Fund Enterprise Business System's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	3 years, 4 months	3
Program executive	1 year, 5 months	6
Milestone decision authority	0 years, 8 months	12

Source: GAO analysis of General Fund Enterprise Business System's questionnaire response, as of October 2021. | GAO-22-105330

Table 18: General Fund Enterprise Business System's Reported Software Development Approaches

Software development practices	Program response
Software development approach	Agile, waterfall, incremental, mixed, DevOps
Software releases to date	176
Planned releases	186
Average time between releases	1 to 3 months
Uses a software factory	No
Uses continuous iterative development	Yes
Delivery of minimum viable product	Yes

Source: GAO analysis of General Fund Enterprise Business System's questionnaire response, as of October 2021. | GAO-22-105330

Air Force – Defense Enterprise Accounting and Management System

Program description:

Defense Enterprise Accounting and Management System is intended to enable the integration of all Air Force financial information to produce accurate and timely financial statements to support accurate budget forecasting and allow for the retirement of some legacy systems.

Program essentials (as reported by Defense Enterprise Accounting and Management System program officials in October 2021)

Lead DOD component: U.S Air Force

Program owner: U.S Air Force

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Full deployment ATP (January 2021)

Next planned milestone: Capability support (1st quarter 2023)

Year investment began: 2003

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

CIO evaluation rating: 2 - Moderately high risk

Tables 19-21 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 19: Defense Enterprise Accounting and Management System's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars			
Fiscal year	**Development, modernization, and enhancement (DME) expenditures**	**Operations and sustainment (O&S) expenditures**	**Total expenditures (DME + O&S)**
2020	48.584	56.987	105.571
2021	47.403	80.036	127.439
2022	141.203	0	141.203
Total	**237.19**	**137.023**	**374.213**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 20: Defense Enterprise Accounting and Management System's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	1 year and 5 months	7
Program executive	5 years and 5 months	2
Milestone decision authority	acting, position is vacant	3

Source: GAO analysis of Department of Defense Enterprise Accounting and Management System's questionnaire response, as of October 2021. | GAO-22-105330

Table 21: Defense Enterprise Accounting and Management System's Reported Software Development Approaches

Software development practices	**Program response**
Software development approach	Agile, DevSecOps
Software releases to date	304
Planned releases	Releases on a 3 week or 12 week iteration
Average time between releases	Less than 1 month
Uses a software factory	No
Uses continuous iterative development	No
Delivery of minimum viable product	Yes

Source: GAO analysis of Department of Defense Enterprise Accounting and Management System's questionnaire response, as of October 2021. | GAO-22-105330

Department of the Navy – Navy Maritime Maintenance Enterprise Solution

Program description

Navy Maritime Maintenance Enterprise Solution is intended to consolidate overlapping application functionality and databases, data centers, and

infrastructure for ship and submarine maintenance into a fully integrated enterprise solution resulting in reduced costs to Navy.

Program essentials (as reported by Navy Maritime Maintenance Enterprise Solution program officials in November 2021)

Lead DOD component: Department of the Navy

Program owner: Department of the Navy

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

Last milestone achieved: Capability support ATP (2012)

Next planned milestone: Capability support ATP

Year investment began: 1990

Year investment is estimated to reach the end of its useful life: 2050

CIO evaluation rating: 4 - Moderately low risk

Tables 22-24 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 22: Navy Maritime Maintenance Enterprise Solution's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	8.975	98.319	107.294
2021	14.563	98.246	112.809
2022	10.618	106.853	117.471
Total	**34.156**	**303.418**	**337.574**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 23: Navy Maritime Maintenance Enterprise Solution's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	6 years and 1 month	2
Program executive	1 year and 5 months	1
Milestone decision authority	0 years and 3 month	2

Source: GAO analysis of Navy Maritime Maintenance Enterprise Solution's questionnaire response, as of November 2021 | GAO-22-105330

Table 24: Navy Maritime Maintenance Enterprise Solution's Reported Software Development Approaches

Software development practices	Program response
Software development approach	Agile, waterfall, incremental, mixed, DevOps, DevSecOps, other[a]
Software releases to date	N/A
Planned releases	N/A
Average time between releases	1 to 3 months
Uses a software factory	No
Uses continuous iterative development	Yes
Delivery of minimum viable product	Yes

Source: GAO analysis of Navy Maritime Maintenance Enterprise Solution's questionnaire response, as of November 2021. | GAO-22-105330

[a]Portions of the portfolio are still continuing to use other development approaches.

Defense Health Agency – Defense Enrollment Eligibility Reporting System

Program description

Defense Enrollment Eligibility Reporting System is the Department of Defense's authoritative data repository for all workforce, personnel benefits, eligibility, and military health care system enrollment information.

Program essentials (as reported by Defense Enrollment Eligibility Reporting System program officials in November 2021)

Lead DOD component: Under Secretary of Defense for Personnel and Readiness / Defense Human Resources Activity / Defense Manpower Data Center

Program owner: Under Secretary of Defense for Personnel and Readiness / Defense Human Resources Activity / Defense Manpower Data Center

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Deliver capabilities (1980's)

Next planned milestone: Deliver capabilities

Year investment began: 1979

Year investment is estimated to reach the end of its useful life: 2031

CIO evaluation rating: 3 - Medium risk

Tables 25-27 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 25: Defense Enrollment Eligibility Reporting System's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	0	98.188	98.188
2021	0	104.314	104.314
2022	0	68.974	68.974
Total	**0**	**271.476**	**271.476**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 26: Defense Enrollment Eligibility Reporting System's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	4 years and 6 months	3
Program executive	5 years and 0 months	2
Milestone decision authority	10 years and 0 months	Prior to July 18, 2017 it was Under Secretary of Defense for Personnel and Readiness. The milestone decision authority is the Assistant Secretary of Defense for Acquisitions and the role has always been in the Office of the Secretary of Defense Acquisitions office.

Source: GAO analysis of Department of Defense Enrollment Eligibility Reporting System's questionnaire response, as of November 2021. | GAO-22-105330

Table 27: Defense Enrollment Eligibility Reporting System's Reported Software Development Approaches

Software development practices	Program response
Software development approach	Agile, waterfall
Software releases to date	No more than 4 per year
Planned releases	Average 4 per year
Average time between releases	1 to 3 months
Uses a software factory	No
Uses continuous iterative development	No
Delivery of minimum viable product	No

Source: GAO analysis of Department of Defense Enrollment Eligibility Reporting System's questionnaire response, as of November 2021. | GAO-22-105330

Defense Logistics Agency – Distribution Standard System

Program description

The Distribution Standard System is the Defense Logistics Agency's standard automated system for distributing Department of Defense materiel. Distribution Standard System is intended to provide global service and worldwide support to the warfighter, peacekeepers, and to federal and civilian customers.

Program essentials (as reported by program officials in November 2021)

Lead DOD component: Department of Defense-Military Programs

Program owner: Defense Logistics Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support ATP

Next planned milestone: Distribution Standard System continues to be in Production, Deployment, and Sustainment and plans as it conducts technical refreshes to support capabilities.

Year investment began: 1999

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

CIO evaluation rating: 3 – Medium risk

Tables 28-30 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 28: Distribution Standard System's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	0	49.079	49.079
2021	20	77.348	97.348
2022	11.134	109.717	120.851
Total	**31.134**	**236.144**	**267.278**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 29: Distribution Standard System's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	4 years and 6 months	2
Program executive	1 year and 11 months	2
Milestone decision authority	7 years and 9 months	2

Source: GAO analysis of Distribution Standard System's questionnaire response, as of November 2021. | GAO-22-105330

Table 30: Distribution Standard System's Reported Software Development Approaches

Software development practices	Program response
Software development approach	Agile, incremental, mixed
Software releases to date	80
Planned releases	92
Average time between releases	4 to 6 months
Uses a software factory	Yes
Uses continuous iterative development	Yes
Delivery of minimum viable product	Yes

Source: GAO analysis of Distribution Standard System's questionnaire response, as of November 2021. | GAO-22-105330

Defense Logistics Agency – Enterprise Business System

Program description

The Enterprise Business System is intended to provide business capabilities enabling supply chain management for energy and non-energy commodities, including enterprise procurement and property.

Program essentials (as reported by Enterprise Business System program officials in November 2021)

Lead DOD component: Defense Logistics Agency

Program owner: Defense Logistics Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Capability support ATP (May 2019)

Next planned milestone: Capability support ATP (2nd quarter 2022)

Year investment began: 2000

Year investment is estimated to reach the end of its useful life: 2025

CIO evaluation rating: 5 - Low risk

Tables 31-33 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 31: Enterprise Business System's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	6.933	70.487	77.42
2021	6.418	81.408	87.826
2022	0	118.994	118.994

Total	**13.351**	**270.889**	**284.24**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 32: Enterprise Business System's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	5 years and 0 months	3
Program executive	2 years and 0 months	4
Milestone decision authority	2 years and 0 months	5

Source: GAO analysis of Department of Enterprise Business System's questionnaire response, as of November 2021. | GAO-22-105330

Table 33: Enterprise Business System's Reported Software Development Approaches

Software development practices	Program response
Software development approach	Agile, waterfall, incremental, DevOps
Software releases to date	33
Planned releases	67
Average time between releases	4 to 6 months
Uses a software factory	Yes
Uses continuous iterative development	Yes
Delivery of minimum viable product	Yes

Source: GAO analysis of Department of Enterprise Business System's questionnaire response, as of November 2021. | GAO-22-105330

Defense Logistics Agency – Defense Agencies Initiative

Program description

The Defense Agencies Initiative is intended to transform the budget, finance, and accounting operations of most DOD defense agencies in order to achieve accurate and reliable financial information in support of financial accountability and effective and efficient decision-making throughout the defense agencies. Defense Agencies Initiative is a critical part of the department's effort to modernize the defense agencies' financial management capabilities.

Program essentials (as reported by Defense Agencies Initiative program officials in October 2021)

Lead DOD component: Defense Logistics Agency

Program owner: Defense Logistics Agency

Acquisition pathway: Defense business systems acquisition

Last milestone achieved: Limited deployment ATP(s) (August 2021)

Next planned milestone: Limited deployment ATP(s) (August 2022)

Year investment began: 2007

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

CIO evaluation rating: 3 - Medium risk

Tables 34-36 describe key information about the program, including actual and planned expenditures, leadership tenure, and reported software development practices.

Table 34: Defense Agencies Initiative's Reported Fiscal Year 2020 through Fiscal Year 2022 Costs Actual and Planned Expenditures

Millions of dollars

Fiscal year	Development, modernization, and enhancement (DME) expenditures	Operations and sustainment (O&S) expenditures	Total expenditures (DME + O&S)
2020	21.116	66.073	87.189
2021	20.537	58.144	78.681
2022	32.254	72.497	104.751
Total	**73.907**	**196.714**	**270.621**

Source: Program information reported by DOD to the Office of Management and Budget's federal IT Dashboard (June 2021). | GAO-22-105330

Table 35: Defense Agencies Initiative's Reported Leadership and Tenure

Title	Years and months in position	Number of people who have held this position over the past 10 years
Program manager	1 year and 0 months	3
Program executive	1 year and 11 months	2
Milestone decision authority	7 years and 9 months	2

Source: GAO analysis of Department of Defense Agencies Initiative's questionnaire response, as of October 2021. | GAO-22-105330

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

Software development practices	Program responses
Software development approach	Incremental

Software releases to date	4
Planned releases	7 annual releases
Average time between releases	10 to 12 months
Uses a software factory	No
Uses continuous iterative development	No
Delivery of minimum viable product	Yes

Source: GAO analysis of Department of Defense Agencies Initiative's questionnaire response, as of October 2021. | GAO-22-105330

Appendix III: Program Leadership Tenure

Program officials representing the 25 Department of Defense (DOD) major IT business programs included in our review reported on the amount of time current (as of December 2021) program managers, program executive officers, and milestone decision authorities had held those positions. In addition, program officials reported the number of individuals that had held those positions over the last 10 years. Table 37 summarizes DOD program leadership turnover for the 25 major IT business programs and table 38 summarizes the same information for the 11 programs we identified as actively developing new software functionality.[1]

Table 37: Program Leadership Turnover for DOD's 25 Major IT Business Programs

Title	Average time working with program	Median time working with program	Average number of individuals in the position	Median number of individuals in the position
Program manager	2 years and 5 months	2 years and 2 months	4	4
Program executive	2 years and 8 months	1 year and 10.5 months	3	3
Milestone decision authority	2 years and 11 months	1 year and 11 months	2.9	3

Source: GAO analysis of Department of Defense questionnaire responses (December 2021). | GAO-22-105330

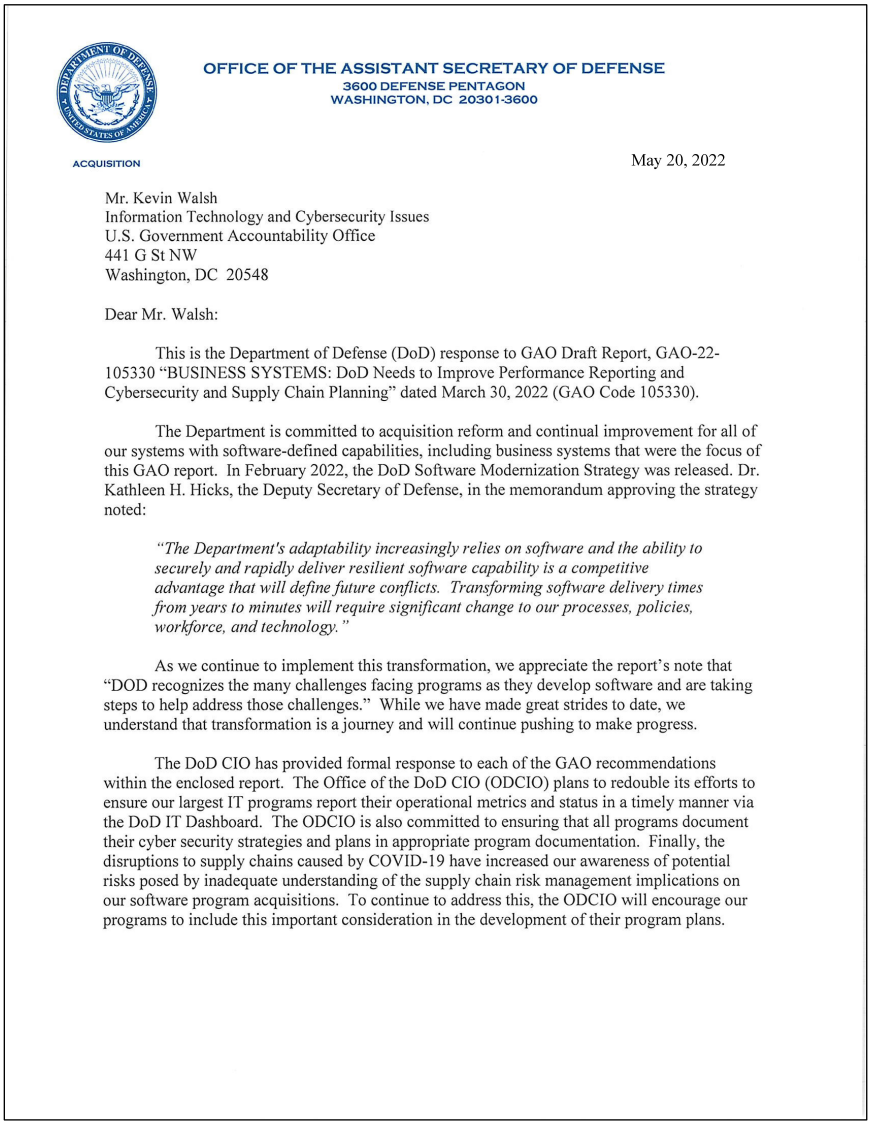
[1]For the purposes of this assessment, we considered programs most likely to be actively developing new software functionality if program officials reported they were actively developing new software functionality, reported they had not yet reached full deployment ATP, or reported a life cycle phase of "other" and indicated they were in the process of migrating functionality to the cloud. Of the 11 programs that we identified, officials from seven programs reported they were actively developing new software functionality. An official from one program reported that limited deployment ATP was the most recent milestone they had achieved. An official from one other program reported that the most recent milestone the program achieved was acquisition ATP. Officials from the two remaining programs reported a lifecycle phase of "other" and indicated that they were in the process of migrating functionality to the cloud. Officials from the other 14 programs reported that their software development efforts were either intended to sustain existing functionality or involved minor enhancements to a program currently in sustainment or reported that their program had proceeded past full deployment ATP or its equivalent milestone (e.g., capability support). The 11 programs we identified were the ones we expected to most likely be using the more modern approaches to software development discussed in the related section of the report.

Table 38: Program Leadership Turnover for DOD's 11 Major IT Business Programs Developing Software

Title	Average time working with program	Median time working with program	Average number of individuals in the position	Median number of individuals in the position
Program manager	1 year and 10 months	1 year and 6 months	3.6	3
Program executive	3 years and 4 months	2 years and 11.5 months	2.4	2
Milestone decision authority	3 years and 6 months	2 years and 10 months	2.6	2

Source: GAO analysis of Department of Defense questionnaire responses (December 2021). | GAO-22-105330

Appendix IV: Comments from the Department of Defense



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

ACQUISITION

May 20, 2022

Mr. Kevin Walsh
Information Technology and Cybersecurity Issues
U.S. Government Accountability Office
441 G St NW
Washington, DC 20548

Dear Mr. Walsh:

This is the Department of Defense (DoD) response to GAO Draft Report, GAO-22-105330 "BUSINESS SYSTEMS: DoD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning" dated March 30, 2022 (GAO Code 105330).

The Department is committed to acquisition reform and continual improvement for all of our systems with software-defined capabilities, including business systems that were the focus of this GAO report. In February 2022, the DoD Software Modernization Strategy was released. Dr. Kathleen H. Hicks, the Deputy Secretary of Defense, in the memorandum approving the strategy noted:

"The Department's adaptability increasingly relies on software and the ability to securely and rapidly deliver resilient software capability is a competitive advantage that will define future conflicts. Transforming software delivery times from years to minutes will require significant change to our processes, policies, workforce, and technology."

As we continue to implement this transformation, we appreciate the report's note that "DOD recognizes the many challenges facing programs as they develop software and are taking steps to help address those challenges." While we have made great strides to date, we understand that transformation is a journey and will continue pushing to make progress.

The DoD CIO has provided formal response to each of the GAO recommendations within the enclosed report. The Office of the DoD CIO (ODCIO) plans to redouble its efforts to ensure our largest IT programs report their operational metrics and status in a timely manner via the DoD IT Dashboard. The ODCIO is also committed to ensuring that all programs document their cyber security strategies and plans in appropriate program documentation. Finally, the disruptions to supply chains caused by COVID-19 have increased our awareness of potential risks posed by inadequate understanding of the supply chain risk management implications on our software program acquisitions. To continue to address this, the ODCIO will encourage our programs to include this important consideration in the development of their program plans.

The Department appreciates the opportunity to comment on the Draft Final Report. My point of contact for this effort is Mr. Sean P. Brady, (732) 673-5858.

Sincerely,

Tanya M. Skeen
Acting Assistant Secretary of Defense for Acquisition

Enclosure:
As stated

2

GAO DRAFT REPORT DATED MARCH 31, 2022
GAO-22-105330 (GAO CODE 105330)

"BUSINESS SYSTEMS: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs report operational performance measures, as appropriate, as part of the department's submission to the federal IT Dashboard.

DoD RESPONSE: DoD concurs with Recommendation 1.

DoD is already required to report major investments, including major IT business systems, operational performance metrics to the Federal IT Dashboard per the OMB A-11 and Capital Planning Guidance. In addition, DoD releases specific IT budget guidance that requires Components to report operational performance metrics for major IT investments.

RECOMMENDATION 2: The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs develop approved cybersecurity strategies, as appropriate.

DoD RESPONSE: DoD concurs with Recommendation 2.

The DoD CIO, in conjunction with the Undersecretary of Defense for Acquisition and Sustainment (A&S) is working to ensure business programs develop Cybersecurity strategies that demonstrate that they are effectively positioned to manage cybersecurity risks and mitigate threats.

The DoD CIO has recently reviewed and approved Cybersecurity Strategies (CSS) for several of the major business systems covered in GAO-22-105330. The Army, and the Navy have adopted, and/or adapted, the DoD CIO's, June 24, 2021, Cybersecurity Outline and Guidance for developing CSS. The office of the DoD CIO continues to provide online guidance at:

https://www.dau.edu/cop/pm/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/pm/DAU%20Sponsored%20Documents/CYBERSECURITY%20STRATEGY%20OUTLINE%20and%20GUIDANCE.docx&action=default&DefaultItemOpen=1

The DOD CIO is currently updating the CSS governing issuance, DoD Instruction 8580.01, *Information Assurance in the Defense Acquisition System (DAS),* to reflect the USD (A&S) comprehensive revision of the DAS, known as the Adaptive Acquisition Framework (AAF). The DoD CIO update to the DoDI 8580.01 will deliver updated cybersecurity guidance

to the development, operations, and sustainment of DoD business systems following AAF pathways.

The DoD Instruction 5000.75, *Business Systems Requirements and Acquisition*, identifies the DoD CIO as the approval authority for Business Category (BCAT) 1 systems in development or sustainment. Legacy business systems have and shall be held to current cybersecurity standards as are other mission critical or mission essential IT systems.

RECOMMENDATION 3: The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs develop plans that address information and communication technology supply chain risk management, as appropriate.

DoD RESPONSE: DoD concurs with Recommendation 3.

Although Components are not yet required to maintain their own information and communications technology supply chain risk management (ICT SCRM) policies, the Department has already laid a foundation for this forthcoming requirement, which will become effective when NIST SP 800-53 revision 5 is adopted. Additionally, the Department is in the process of enhancing Risk Management Framework (RMF) guidance for the SCRM family of controls, with tailoring guidance for Components' implementation.

Nonetheless, related metrics have been in place within the current Cyber Hardening Scorecard since 2019, with the Services (and DISA) reporting quarterly on relevant objectives. Each Component has a SCRM Policy that is approved, regularly reviewed, requires automated continuous monitoring, covers all acquisition programs, requires use of a SCRM approved products list, addresses simplified acquisitions and purchase card acquisition, and defines the key stakeholders, roles, and responsibilities for ICT SCRM Policy. Along with the ICT-SCRM policy metric, each Component reports on the presence (or absence) of a cyber-SCRM specific funding line.

Enterprise-wide policies for acquisition of IT/ICT in DoDI 5000.82, ACQUISITION OF INFORMATION TECHNOLOGY (IT), which includes Defense Business Systems (Figure 1, AAF), directs the assessment of supply chain risk as part of the required implementation of DoDI 5200.44, PROTECTION OF MISSION CRITICAL FUNCTIONS TO ACHIEVE TRUSTED SYSTEMS AND NETWORKS (TSN). Additionally, DoDI 5000.90, CYBERSECURITY FOR ACQUISITION DECISION AUTHORITIES AND PROGRAM MANAGERS provides detailed policy for program managers to "deliberately harden the supply chain commensurate with the risk to national security" (paragraph 3.4, CYBERSECURITY IN THE SUPPLY CHAIN). Table 1, SCRM Actions by Risk Tolerance level, provides succinct policy for acquisitions ranging from simplified procurements, to capability/engineered acquisition with very low risk tolerance.

Text of Appendix IV: Comments from the Department of Defense

ACQUISITION
OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

May 20, 2022

Mr. Kevin Walsh
Information Technology and Cybersecurity Issues
U.S. Government Accountability Office
441 G St NW Washington, DC 20548

Dear Mr. Walsh:

This is the Department of Defense (DoD) response to GAO Draft Report, GAO-22-105330 "BUSINESS SYSTEMS: DoD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning" dated March 30, 2022 (GAO Code 105330).

The Department is committed to acquisition reform and continual improvement for all of our systems with software-defined capabilities, including business systems that were the focus of this GAO report. In February 2022, the DoD Software Modernization Strategy was released. Dr. Kathleen H. Hicks, the Deputy Secretary of Defense, in the memorandum approving the strategy noted:

"The Department's adaptability increasingly relies on software and the ability to securely and rapidly deliver resilient software capability is a competitive advantage that will define future conflicts. Trans.forming software delivery times from years to minutes will require significant change to our processes, policies, worliforce, and technology. "

As we continue to implement this transformation, we appreciate the report's note that "DOD recognizes the many challenges facing programs as they develop software and are taking steps to help address those challenges." While we have made great strides to date, we understand that transformation is a journey and will continue pushing to make progress.

The DoD CIO has provided formal response to each of the GAO recommendations within the enclosed report. The Office of the DoD CIO (ODCIO) plans to redouble its effo1ts to ensure our largest IT programs report their operational metrics and status in a timely manner via the DoD IT Dashboard. The ODCIO is also committed to ensuring that all programs document their cyber security strategies and plans in appropriate program documentation. Finally, the disruptions to supply chains caused by COVID-19 have increased our awareness of potential risks posed by inadequate understanding of the supply chain risk management implications on our software program acquisitions. To continue to address this, the ODCIO will encourage our programs to include this important consideration in the development of their program plans.

The Department appreciates the opportunity to comment on the Draft Final Report. My point of contact for this effort is Mr. Sean P. Brady, (732) 673-5858.

Sincerely,
Acting Assistant Secretary of Defense for Acquisition

Enclosure:

As stated

2

GAO DRAFT REPORT DATED MARCH 31, 2022

GAO-22-105330 (GAO CODE 105330)

"BUSINESS SYSTEMS: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning"

DEPARTMENT OF DEFENSE COMMENTS

TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs report operational performance measures, as appropriate, as part of the department's submission to the federal IT Dashboard.

DoD RESPONSE: DoD concurs with Recommendation 1.

DoD is already required to report major investments, including major IT business systems, operational performance metrics to the Federal IT Dashboard per the OMB A-11 and Capital Planning Guidance. In addition, DoD releases specific IT budget guidance that requires Components to report operational performance metrics for major IT investments.

RECOMMENDATION 2: The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs develop approved cybersecurity strategies, as appropriate.

DoD RESPONSE: DoD concurs with Recommendation 2.

The DoD CIO, in conjunction with the Undersecretary of Defense for Acquisition and Sustainment (A&S) is working to ensure business programs develop Cybersecurity strategies that demonstrate that they are effectively positioned to manage cybersecurity risks and mitigate threats.

The DoD CIO has recently reviewed and approved Cybersecurity Strategies (CSS) for several of the major business systems covered in GAO-22-105330. The Army, and the Navy have adopted, and/or adapted, the DoD CIO's, June 24, 2021, Cybersecurity Outline and Guidance for developing CSS. The office of the DoD CIO continues to provide online guidance at:

https://www.dau.edu/cop/pm/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/pm/DAU%20Sponsored%20Documents/CYBERSECURITY%20STRATEGY%20OUTLINE%20and%20GUIDANCE.docx&action=default&DefaultItemOpen=1

The DOD CIO is currently updating the CSS governing issuance, DoD Instruction 8580.01, Information Assurance in the Defense Acquisition System (DAS), to reflect the USD (A&S) comprehensive revision of the DAS, known as the Adaptive Acquisition Framework (AAF). The DoD CIO update to the DoDI 8580.01 will deliver updated cybersecurity guidance to the development, operations, and sustainment of DoD business systems following AAF pathways.

The DoD Instruction 5000.75, Business Systems Requirements and Acquisition, identifies the DoD CIO as the approval authority for Business Category (BCAT) 1 systems in development or sustainment. Legacy business systems have and shall be held to current cybersecurity standards as are other mission critical or mission essential IT systems.

RECOMMENDATION 3: The Secretary of Defense should direct the Chief Information Officer to ensure that major IT business programs develop plans that address information and communication technology supply chain risk management, as appropriate.

DoD RESPONSE: DoD concurs with Recommendation 3.

Although Components are not yet required to maintain their own information and communications technology supply chain risk management (ICT SCRM) policies, the Department has already laid a foundation for this forthcoming requirement, which will become effective when NIST SP 800-53 revision 5 is adopted. Additionally, the Department is in the process of enhancing Risk Management Framework (RMF) guidance for the SCRM family of controls, with tailoring guidance for Components' implementation.

Nonetheless, related metrics have been in place within the current Cyber Hardening Scorecard since 2019, with the Services (and DISA) reporting quarterly on relevant objectives. Each Component has a SCRM Policy that is approved, regularly reviewed, requires automated continuous monitoring, covers all acquisition programs, requires use of a SCRM approved products list, addresses simplified acquisitions and purchase card acquisition, and defines the key stakeholders, roles, and responsibilities for ICT SCRM Policy. Along with the ICT-SCRM policy metric, each Component reports on the presence (or absence) of a cyber-SCRM specific funding line.

Enterprise-wide policies for acquisition of IT/ICT in DoDI 5000.82, ACQUISITION OF INFORMATION TECHNOLOGY (IT), which includes Defense Business Systems (Figure 1, AAF), directs the assessment of supply chain risk as part of the required implementation of DoDI 5200.44, PROTECTION OF MISSION CRITICAL FUNCTIONS TO ACHIEVE TRUSTED SYSTEMS AND NETWORKS (TSN). Additionally, DoDI 5000.90, CYBERSECURITY FOR ACQUISITION DECISION AUTHORITIES AND PROGRAM MANAGERS provides detailed policy for program managers to “deliberately harden the supply chain commensurate with the risk to national security” (paragraph 3.4, CYBERSECURITY IN THE SUPPLY CHAIN). Table 1, SCRM Actions by Risk Tolerance level, provides succinct policy for acquisitions ranging from simplified procurements, to capability/engineered acquisition with very low risk tolerance.

Error! No text of specified style in document.

GAO Contact

Kevin Walsh at (202) 512-6151 or walshk@gao.gov

Appendix V: GAO Contact and Staff Acknowledgments

Staff Acknowledgments

Principal contributors to this report were Michael Holland (Assistant Director), Tyler Mountjoy (Analyst in Charge), Chris Businsky, Garret Chan, Richard Sayoc, Priscilla Smith, Andrew Weiss, and Marshall Williams. Other key contributors included Jordan Adrian, Bea Alff, Tommy Baril, Lauri Barnes, Nicole Burkart, Lorraine Ettaro, Nathan Foster, Jennifer Franks, Jennifer Leotta, Anne McDonough, Melissa Melvin, Shelby Oakley, Monica Perez-Nelson, Scott Pettis, Brandon Sanders, Hai Tran, 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, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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