United States Government Accountability Office

Report to Congressional Committees

April 2023

SOFTWARE ACQUISITION

Additional Actions Needed to Help DOD Implement Future Modernization Efforts

GAO Highlights

Highlights of GAO-23-105611, a report to congressional committees

April 2023

SOFTWARE ACQUISITION

Additional Actions Needed to Help DOD Implement Future Modernization Efforts

Why GAO Did This Study

DOD has made efforts to modernize its approaches to developing and acquiring software for its software-intensive systems—such as weapon and IT systems. However, it faces challenges executing approaches to rapidly deliver software. The DSB and DIB published reports in 2018 and 2019, respectively, which made recommendations to improve DOD's software practices.

Congress included a provision in statute for GAO to examine DOD's implementation of DSB and DIB recommendations. This report assesses (1) the extent to which DOD addressed DSB and DIB recommendations; and (2) the extent to which DOD is positioned to implement its future software modernization plans.

GAO reviewed DOD documents related to ongoing and future software reform initiatives and interviewed relevant officials. GAO then compared this information to DIB and DSB recommendations and key practices from past GAO work.

What GAO Recommends

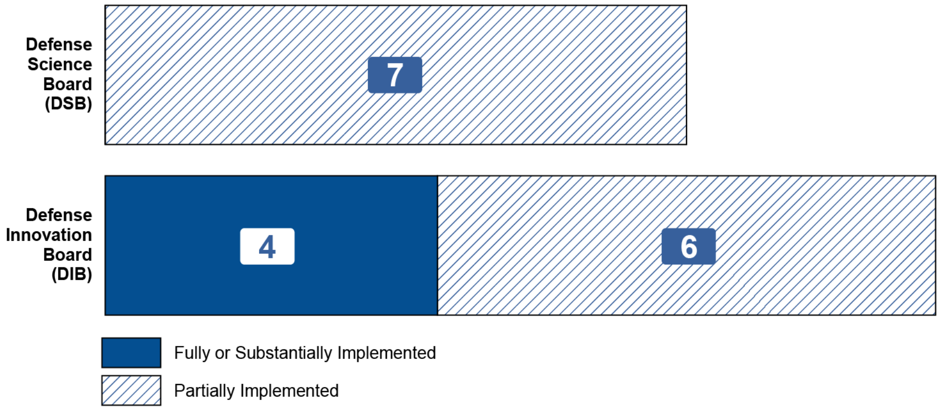
GAO is making seven recommendations, including that DOD finalize implementation plans for future software modernization efforts and develop a software workforce plan. DOD concurred with four recommendations and partially concurred with three recommendations. GAO continues to believe that all of its recommendations are warranted.

View GAO-23-105611. For more information, contact Shelby S. Oakley at (202) 512-4841 or oakleys@gao.gov.

What GAO Found

The Department of Defense's (DOD) response to evolving threats is increasingly determined by its ability to rapidly develop and deploy systems that heavily rely on software, such as weapons or information technology (IT) systems. DOD has taken many steps in the past few years to modernize its approach to developing and acquiring software. DOD's efforts at least partially implement all 17 Defense Science Board (DSB) and Defense Innovation Board (DIB) recommendations, some of which include multiple recommended actions. For example, DOD substantially implemented two DIB recommendations by streamlining software acquisition processes and piloting a new funding approach to deliver software faster.

DOD Has at Least Partially Implemented All of the DIB and DSB Recommendations



Source: GAO analysis of Department of Defense (DOD) information and interviews with DOD officials. | GAO-23-105611

However, for 13 of the 17 recommendations, DOD has yet to take certain actions outlined in the recommendations. For example, while DOD enhanced training for its software workforce, it has yet to establish a cadre of software developers. DOD officials stated that they have addressed the intent of the recommendations and do not plan to fully implement all recommended actions, in part, because certain actions may be impractical or outdated.

DOD has outlined transformational plans to continue software modernization. According to DOD, its plans will require a cohesive department-wide effort that will take time to fully implement. However, DOD has yet to take certain steps recommended by GAO's past work to position itself to effectively implement its planned reforms. For example, DOD has yet to finalize implementation plans for these efforts or conduct strategic planning for its software workforce to ensure it has the needed skillsets to implement reforms. Taking such steps would better position DOD to implement its planned reforms, which are aimed at helping achieve its goal of more rapidly delivering software to its users.

Contents

Tables

Figures

Abbreviations

ATO	authorization to operate
CAPE	Cost Assessment and Program Evaluation
cATO	continuous authorization to operate
CDAO	Chief Digital and Artificial Intelligence Office
CIO	Chief Information Officer
DAU	Defense Acquisition University
DevSecOps	Development, Security, and Operations
DIB	Defense Innovation Board
DOD	Department of Defense
DOT&E	Director, Operational Test and Evaluation
DSB	Defense Science Board
IT	information technology
JCIDS	Joint Capabilities Integration and Development System
Joint Staff	Office of the Chairman of the Joint Chiefs of Staff
NDAA	National Defense Authorization Act
OSD	Office of the Secretary of Defense
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)	Under Secretary of Defense (Comptroller)
USD(R&E)	Under Secretary of Defense for Research and Engineering
RDT&E	research, development, test and evaluation
SSG	Senior Steering Group

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

April 5, 2023

Congressional Committees

The Department of Defense's (DOD) ability to respond to evolving threats and compete with strategic competitors, such as Russia and China, is increasingly determined by its ability to rapidly develop and deploy software-intensive systems, such as weapons and information technology (IT) systems. Sustaining a competitive advantage requires that DOD be able to deliver software-based capabilities faster than its adversaries. Our recent work found that DOD has made numerous efforts to modernize its software acquisition and development approaches over the past several years.[1]

However, we have also highlighted that DOD continues to face challenges in executing modern approaches and rapidly delivering software to users, which senior DOD leaders have acknowledged.[2] According to DOD, software modernization will entail a cohesive department-wide effort that will take time. The department noted in its February 2022 Software Modernization Strategy that this major digital transformation requires significant changes to processes, policies, workforce, technology, and the establishment of partnerships across the department—all of which will require sustained engagement over many years.[3]

The Defense Science Board (DSB) and Defense Innovation Board (DIB) published reports in 2018 and 2019, respectively, that made recommendations to improve DOD's software acquisition and

[1] GAO, *DOD Software Acquisition: Status of and Challenges Related to Reform Efforts*, GAO-21-105298 (Washington, D.C.: Sept. 30, 2021). For the purposes of this report, we refer to DOD's efforts to modernize its software development and acquisition approaches as software modernization efforts.

[2] GAO*, Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, GAO-22-105330 (Washington, D.C.: June 14, 2022); *Weapon Systems Annual Assessment: Challenges to Fielding Capabilities Faster Persist*, GAO-22-105230 (Washington, D.C.: June 8, 2022); and GAO-21-105298.

[3] Department of Defense, *Software Modernization Strategy* (Washington, D.C.: Feb. 2, 2022).

development practices.[4] These recommendations addressed a broad range of themes, including streamlining software acquisition processes, establishing new funding methods, and developing training for the software workforce.

The William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 included a provision for us to examine DOD's implementation of DSB and DIB software modernization recommendations.[5] This report assesses the extent to which DOD (1) has implemented the DSB's and DIB's recommendations; and (2) is positioned to implement future software modernization efforts.

To determine the extent to which DOD has implemented the DSB's and DIB's recommendations, we reviewed DSB's 2018 and DIB's 2019 reports. In addition, we analyzed agency policies, guidance, and other documentation related to software development and acquisition, such as DOD Instruction 5000.02, *Operation of the Adaptive Acquisition Framework* and DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*.[6] We then compared DOD's actions to DSB's and DIB's recommendations.

To determine the extent to which DOD is positioned to implement future software modernization efforts, we reviewed relevant DOD strategies and other documents that outlined future plans, such as reports from DOD to Congress. We compared DOD's planning efforts as described in these documents to selected practices from our prior work associated with the

[4] Department of Defense, Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 3, 2019); and Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington, D.C.: Feb. 14, 2018).

[5] Pub. L. No. 116-283, § 838(a) (2021). We previously addressed additional topics included in Sec. 838: GAO-22-105230 and GAO-21-105298.

[6] Department of Defense, Department of Defense Instruction 5000.02, *Operation of the Adaptive Acquisition Framework* (Jan. 23, 2020) and Department of Defense Instruction 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

implementation of successful agency reforms.[7] For both objectives, we also conducted interviews with officials from the Office of the Secretary of Defense, Office of the Chairman of the Joint Chiefs of Staff (Joint Staff), and the military departments. Appendix I provides additional information on our objectives, scope, and methodology.

We conducted this performance audit from December 2021 to April 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

For years, commercial companies have recognized the value of software for providing new capabilities to consumers. According to the DSB and DIB, the commercial industry has developed leading practices that foster quicker, more cost effective software development, which allows for the speedier delivery of new capability to users and consumers.

DOD has also recognized software as an increasingly critical element for meeting weapon systems' requirements. However, our recent work has highlighted that DOD's software development practices have not kept up with leading industry practices even as software has become increasingly vital to DOD systems.[8] Other recent studies, such as the 2018 DSB and 2019 DIB reports, also found deficiencies in software development and acquisition practices within DOD, such as outdated acquisition processes and delays in delivering software to users.

[7] GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018). In that report, we defined the term "reforms" broadly, to include any organizational changes—such as major transformations, mergers, consolidations, and other reorganizations—and efforts to streamline and improve the efficiency and effectiveness of government operations. The leading practices the report presented were based on our previous work that found the success of agency reforms hinges on the agencies' adherence to key practices for organizational transformations. We selected practices, such as establishing clear outcome-oriented goals and performance measures, as well as involving federal employees and other key stakeholders to develop the proposed reforms, which we found to be most relevant to DOD's software modernization reform effort.

[8] GAO-21-105298.

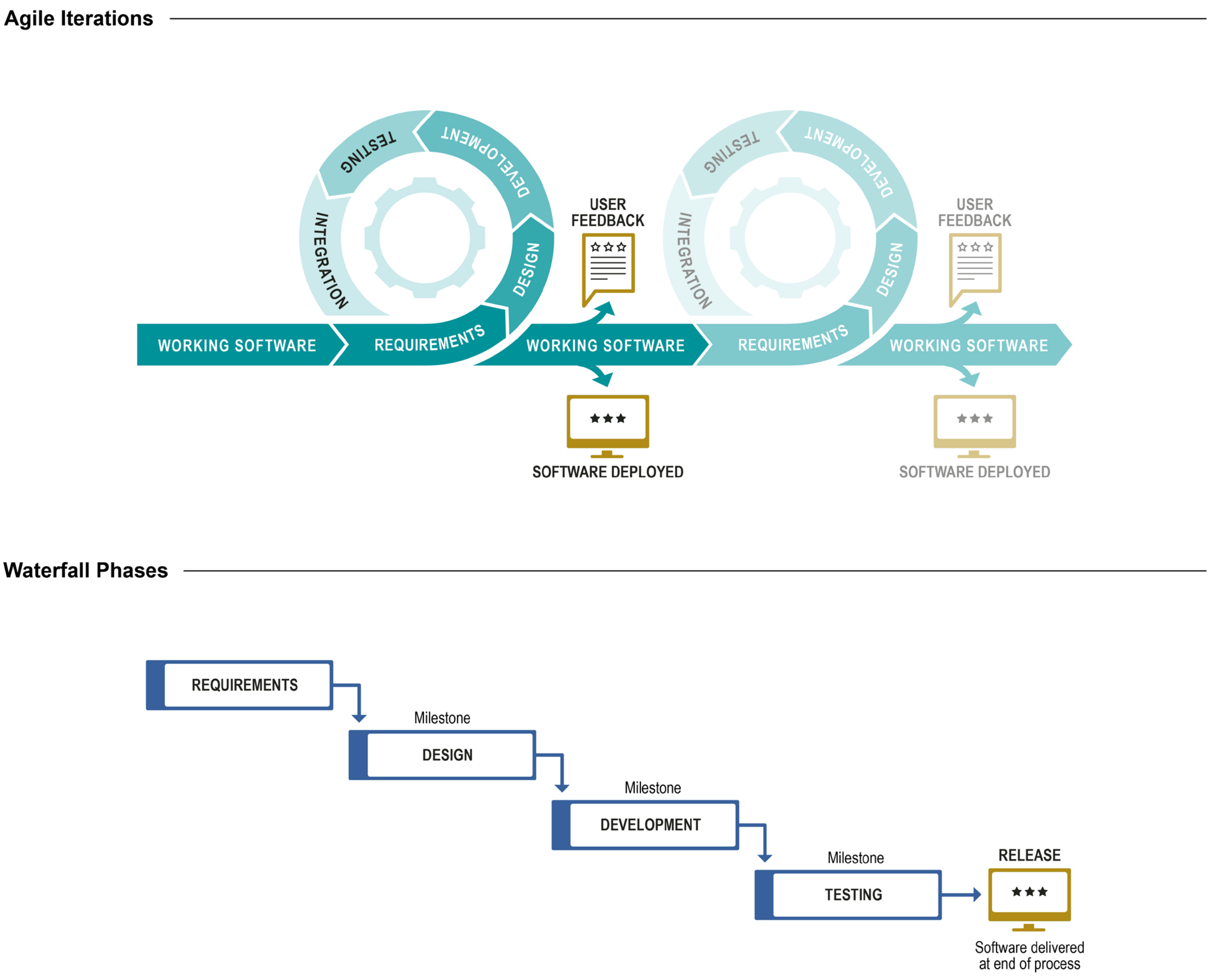
Agile Software Development

Modern approaches to software delivery rely extensively on Agile development. Agile development is a flexible, iterative way of developing software that delivers working capabilities to users earlier than traditional DOD software development processes, known as the waterfall approach.[9] In most instances, adopting Agile methods involves new behaviors and a different mindset, which is a major shift in how an organization operates. For example, Agile practices call for the integration of planning, design, development, and testing into an iterative life cycle to deliver software early and often, ranging from every few days to every 60 to 90 days. The frequent iterations are intended to effectively measure progress toward delivery of the full suite of capabilities, reduce technical and programmatic risk, and be responsive to feedback from stakeholders and users.

In contrast, under the waterfall approach traditionally used by DOD, requirements are established in advance of development, and software is usually delivered as a single completed program at the end of the development cycle. Software development occurs without continual user involvement or feedback, and programs may not be able to modify requirements without cost increases and schedule delays. This software development approach mirrored the development of a DOD hardware system. Figure 1 compares Agile and waterfall approaches for developing software.

[9] GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation,* GAO-20-590G (Washington, D.C.: Sept. 28, 2020).

Figure 1: Comparison of Agile and Waterfall Frameworks for Developing Software



Source: GAO analysis of Department of Defense and U.S. Citizenship and Immigration Services Information. | GAO-23-105611

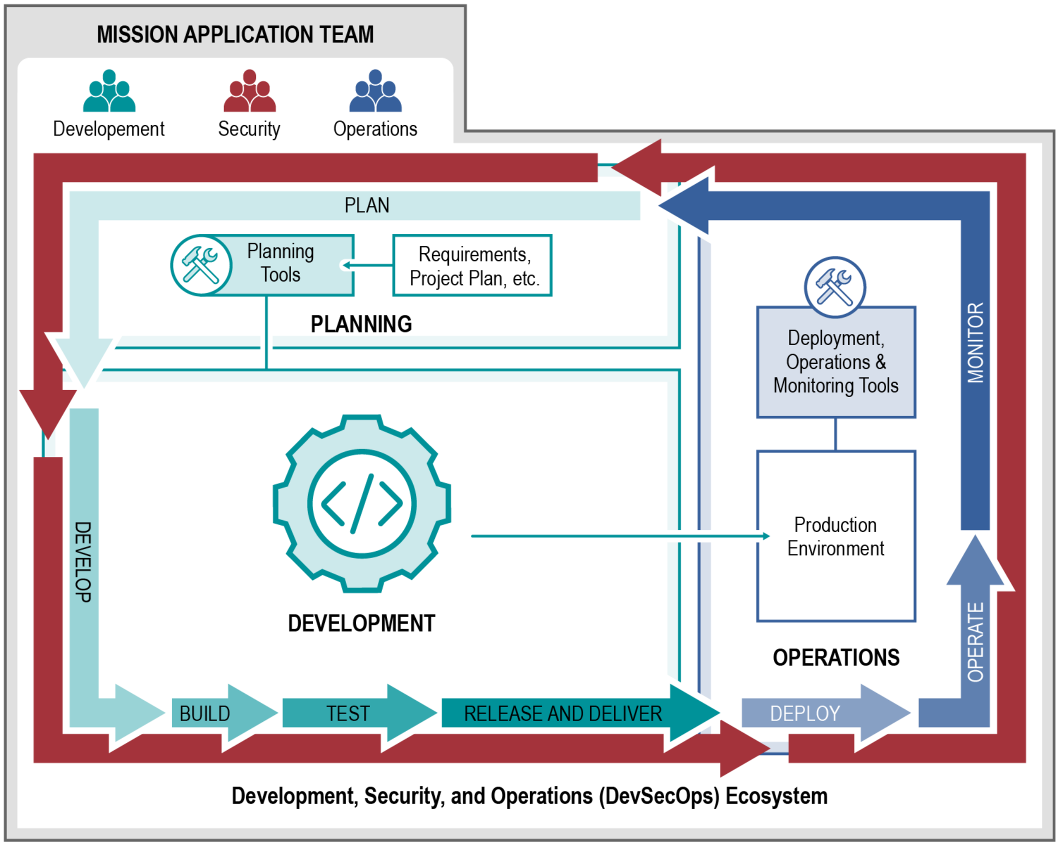
There are numerous frameworks available for Agile programs to use, such as Development, Security, and Operations (DevSecOps), an iterative software development methodology that combines development, security, and operations as key elements in delivering useful capability to the user of the software. These frameworks provide a basic structure to guide projects. Agile, as a concept, is not prescriptive but rather an umbrella term for a variety of iterative software approaches. Each framework is unique and may have its own terminology for processes and artifacts (documents, data, or other information describing what was planned or completed). According to GAO's *Agile Assessment Guide*, when implementing Agile in the federal environment, both government and contractor staff should work together to define the Agile terms and processes to be used for particular programs. The frameworks are not mutually exclusive and can be combined.[10]

DOD's Software Factory Ecosystem

DOD's software factory ecosystem is a collection of tools and processes that support activities throughout the DevSecOps life cycle. Software factories use cloud-based computing to assemble a set of software tools enabling developers, users, and management to work together on a daily tempo. As shown in figure 2, these tools and processes support continuous iterative development through three key phases: planning, development, and operations, with security emphasized throughout each.

[10] GAO-20-590G.

Figure 2: The Department of Defense's Software Factory Ecosystem



Source: GAO analysis of Department of Defense information. | GAO-23-105611

- **Planning.** This phase involves activities that help projects manage time, cost, quality, risk and other issues, such as system design, project plan creation, risk analysis, and business requirements gathering.
- **Development.** This phase contains multiple work streams, equipped with tools and workflows to automate activities with minimal human intervention to produce software applications.
- **Operations.** In this phase, software is deployed to the end user. Among other things, operations and security monitoring are performed during this time.

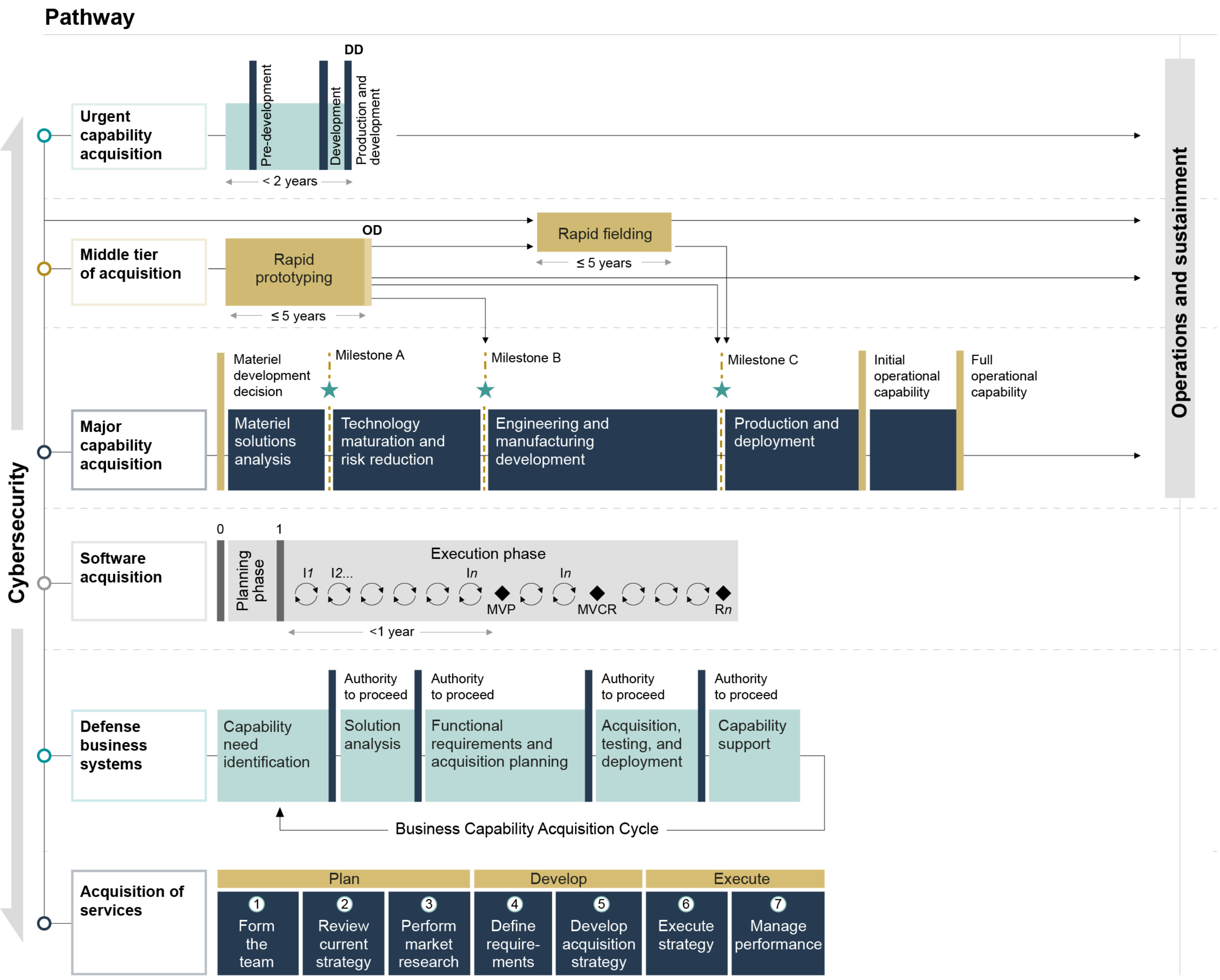
In February 2018, the DSB stated that software factories are a crucial part of iterative development practices, as they allow programs to identify errors and obtain user feedback continuously.

DOD's Adaptive Acquisition Framework and Software Acquisition Pathway

In January 2020, DOD reissued and updated its acquisition policies, emphasizing speed and agility in the acquisition process.[11] The updated instruction established the Adaptive Acquisition Framework, comprised of six acquisition pathways, each tailored to the characteristics and risk profile of the capability being acquired. These six acquisition pathways are intended to, among other things, deliver solutions to the end user in a timely manner (see fig. 3).

[11] Department of Defense, Department of Defense Directive 5000.01, *The Defense Acquisition System* (Sept. 9, 2020) and Department of Defense Instruction 5000.02, *Operation of the Adaptive Acquisition Framework* (Jan. 23, 2020).

Figure 3: DOD's Adaptive Acquisition Framework


Pathway
Urgent capability acquisition
Pre-development
Development
Production and development
DD
< 2 years
Middle tier of acquisition
Rapid prototyping
≤ 5 years
OD
Rapid fielding
≤ 5 years
Major capability acquisition
Materiel development decision
Milestone A
Milestone B
Milestone C
Initial operational capability
Full operational capability
Materiel solutions analysis
Technology maturation and risk reduction
Engineering and manufacturing development
Production and deployment
Software acquisition
0
1
Planning phase
Execution phase
I1
I2...
In
MVP
In
MVCR
Rn
<1 year
Defense business systems
Authority to proceed
Authority to proceed
Authority to proceed
Authority to proceed
Capability need identification
Solution analysis
Functional requirements and acquisition planning
Acquisition, testing, and deployment
Capability support
Business Capability Acquisition Cycle
Acquisition of services
Plan
Develop
Execute
1 Form the team
2 Review current strategy
3 Perform market research
4 Define require-ments
5 Develop acquisition strategy
6 Execute strategy
7 Manage performance
Cybersecurity
Operations and sustainment

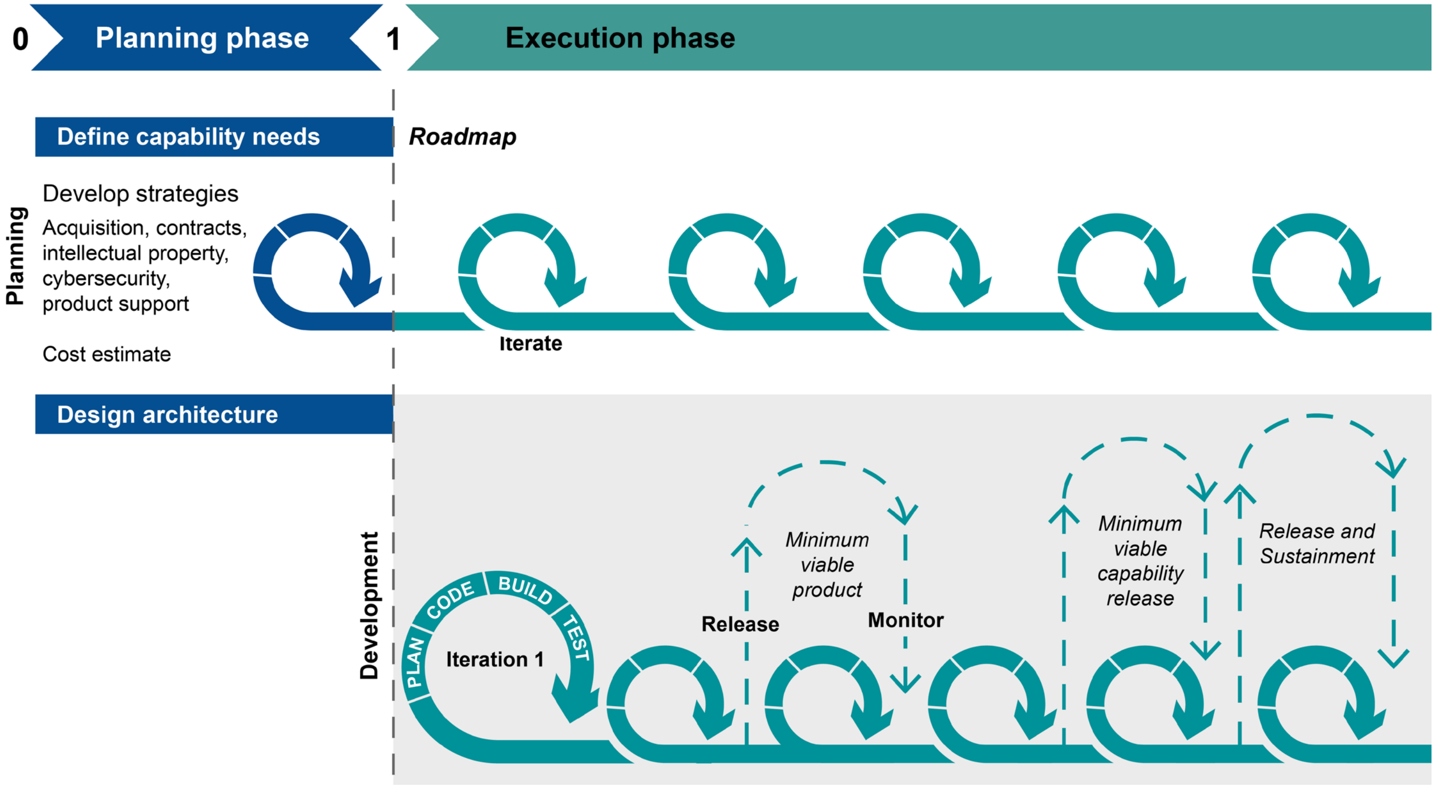
I = Iteration
OD = Outcome determination
DD = Disposition decision

MVCR = Minimum viable capability release
MVP = Minimum viable product
R= Release

Source: GAO analysis of Department of Defense (DOD) data. I GAO-23-105611

One of these pathways, the software acquisition pathway, is intended to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software.[12] Section 800 of the NDAA for Fiscal Year 2020 mandated that DOD develop this pathway.[13] The pathway establishes a framework for software acquisition and development investment decisions that addresses tradeoffs between capabilities, affordability, risk tolerance, and other considerations. It has two phases: planning and execution (see fig. 4).

Figure 4: The Department of Defense's Software Acquisition Pathway



Source: GAO analysis of relevant Department of Defense instructions. | GAO-23-105611

[12] Department of Defense, Department of Defense Instruction, 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

[13] Pub. L. No. 116-92, § 800 (2019).

Using this pathway, small cross-functional teams—users, testers, software developers, and cybersecurity experts—are expected to be able to deliver software rapidly and iteratively to meet user needs. DOD policy encourages program officials to frequently engage with users and deliver new capabilities to operations at least annually.[14] The instruction implemented recommendations we made in 2019 that DOD ensure its software development guidance provides specific, required direction on the timing, frequency, and documentation of user involvement and feedback.[15] Further, in March 2022, we reported that the instruction generally reflected key product development principles used by leading companies.[16]

While the software acquisition pathway offers a number of potential ways to improve DOD's ability to benefit from modern software development approaches, our recent work also shows that DOD is still determining how it will conduct oversight of the pathway. For example, we reported in June 2021 that DOD had yet to collect the data and develop tools it needed to oversee the programs using the pathway.[17]

In September 2021, DOD stated that it had established a software acquisition pathway data collection strategy and shared it with component headquarters and relevant program offices. In addition, DOD stated that it plans to prepare a semiannual reporting template and collect trial submissions from early pathway programs to gain insights, implement suggestions, and improve the template.

Entities Involved in Software Modernization Efforts

The Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Under Secretary of Defense for Research and Engineering (USD(R&E)), and the DOD Chief Information Officer (CIO) are responsible for leading the coordination of software modernization activities, specifically through the Software Modernization Senior Steering Group (SSG). Among other things, the Software Modernization SSG is

[14] Department of Defense, Department of Defense Instruction, 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

[15] GAO, *DOD Space Acquisitions: Including Users Early and Often in Software Development Could Benefit Programs,* GAO-19-136 (Washington D.C.: Mar. 18, 2019).

[16] GAO*, Leading Practices: Agency Acquisition Policies Could Better Implement Key Product Development Principles*, GAO-22-104513 (Washington, D.C.: Mar. 10, 2022).

[17] 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).

intended to promote the adoption of modern software development practices across the department and remove barriers to adoption.

Many other offices within OSD—including Cost Assessment and Program Evaluation (CAPE), and the Director, Operational Test and Evaluation (DOT&E)—as well as Joint Staff, and the military departments also have responsibilities for executing or overseeing certain aspects of software modernization. These organizations are also represented on the Software Modernization SSG, among others.

Examples of selected responsibilities of these offices related to software modernization include:

- **USD(A&S)** establishes software acquisition and sustainment policies, such as DOD's software acquisition pathway instruction.[18]
- **USD(R&E)** establishes policies and advises on all aspects of defense research and engineering and technology development, such as advancing and enabling the rapid transition of software-developed capabilities to acquisition programs of record through research and development and science and technology initiatives.
- **DOD CIO** develops strategy and policy on the operation of DOD information technology, information systems, and cybersecurity, such as co-leading the development of DOD's Software Modernization Strategy.
- **DOT&E** establishes DOD testing policies, including DOD Instruction 5000.89, *Test and Evaluation*, which outlines testing guidance for software acquisition pathway programs.[19]
- **CAPE** establishes policy on cost estimation and analysis, including DOD Instruction 5000.73, *Cost Analysis Guidance and Procedures*, which outlines cost estimation guidance for software acquisition pathway programs.[20]

[18] Department of Defense, Department of Defense Instruction, 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

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

[20] Department of Defense, Department of Defense Instruction, 5000.73, *Cost Analysis Guidance and Procedures* (Mar. 13, 2020).

- Joint Staff develops supplemental guidance for requirements validation and reviews software programs for joint requirements.[21]
- Military departments implement DOD software acquisition policy and, acting through the decision authority, oversee software acquisition pathway programs. In addition, military departments develop supplemental software policies and manage their software workforce.

DSB and DIB Software Modernization Recommendations

DSB Recommendations

Established in 1956, the DSB serves as the Federal Advisory Committee chartered to provide DOD leadership with independent advice and recommendations on science, technology, and acquisition processes, among other things.[22] The DSB is comprised of former senior military and government officials as well as leaders from academia and industry. When necessary, the DOD may establish task forces to support the DSB, such as the task force established to examine the state of DOD's software acquisition. The DSB reports to the USD(R&E), who may act upon the DSB's recommendations.

In February 2018, a DSB task force concluded that DOD can, and should, leverage commercial software development leading practices to its

[21] Joint Staff uses the Joint Capabilities Integration and Development System (JCIDS) process to manage the review and approval of capability requirements documents. The Joint Requirements Oversight Council oversees the process. The Joint Requirements Oversight Council is responsible for assessing joint military capabilities and identifying, approving, and prioritizing gaps in such capabilities to meet requirements in the National Defense Strategy. In addition, the Joint Requirements Oversight Council establishes and approves joint performance requirements that, among other things, ensure interoperability between and among joint military capabilities and are necessary to fulfill capability gaps of more than one armed force or other DOD organization.

[22] Federal Advisory Committee Act, Pub. L. No. 92-463 (1972) (codified as amended at 5 U.S.C. app. 2). We have previously reported that advisory committees play an important role in informing public policy and government regulations by advising the President and federal agencies on national issues. These committees perform peer reviews of scientific research, develop recommendations on specific policy decisions, identify long-range issues facing the nation, and evaluate grant applications. The committees' advice—on issues ranging from stem cell research and space exploration to tax administration and drug approvals—can enhance the quality and credibility of federal decision-making. See also GAO, *Federal Advisory Committees: Actions Needed to Enhance Decision-Making Transparency and Cost Data Accuracy*, GAO-20-575 (Washington, D.C.: Sept. 10, 2020).

advantage, including on its weapon systems.[23] The DSB study made seven recommendations to DOD. We reported previously that DOD was taking steps to address some of these recommendations.[24] Table 1 provides a list of the seven DSB recommendation topics and the specific recommended actions.

Table 1: GAO Summary of February 2018 DSB Software Modernization Recommendations

Recommendation	Recommended actions
Software factory[a]	• Establish a common list of source selection criteria for evaluating software factories for use throughout the department • Require contractors to demonstrate at least a pass-fail ability to construct a software factory • Review and update source selection criteria every 5 years
Continuous iterative development[b]	• Adopt continuous iterative development best practices for software, including security, throughout the acquisition life cycle • Identify minimum viable product approaches • Delegate acquisition authority to program managers • Require all programs entering system development (Milestone B) to implement iterative processes for acquisition category I, II, and III programs • Identify best practices and incorporate into regular program reviews
Adoption of risk reduction metrics for new programs	• Allow multiple vendors to begin work. After a vendor has demonstrated that work can be done, a down-select should happen. Retain several vendors through development to reduce risk, as feasible • Modernize cost and schedule estimates and measurements and contract with the defense industrial base for work breakdown schedule data to include, among others, staff, cost, and productivity • Build a program-appropriate framework for status estimation
Current and legacy programs in development, production, and sustainment	• Plan for ongoing programs to transition to a software factory and continuous iterative development processes • Require prime contractors for ongoing programs to transition to a hybrid model (i.e., hybrid approach between iterative software development and waterfall) and incorporate continuous iterative development processes into long-term sustainment plans • Make the business case for whether to transition the legacy programs for which development is complete • Provide a quarterly status update on the transition plan for programs to the Under Secretary of Defense for Acquisition and Sustainment • Brief best practices and lessons learned across the military departments from programs that have transitioned successfully to modern software development practices

[23] Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington, D.C.: Feb. 14, 2018).

[24] GAO-21-105298.

Recommendation	Recommended actions
Workforce	• Develop a workforce that is competent and familiar with current software development techniques • Military departments should acquire or access a small cadre of software systems architects with a deep understanding of iterative development • Services acquisition commands should use this cadre early in the acquisition process to formulate acquisition strategy, develop source selection criteria, and evaluate progress • Develop a training curriculum, including software acquisition training, to train this cadre and ensure the program managers of software-intensive programs are knowledgeable about software • Direct the Defense Acquisition University to establish curricula addressing modern software practices • Brief the Under Secretary of Defense for Acquisition and Sustainment at least annually to demonstrate contractors' progress on adopting modern software practices • Hire and train a cadre of modern software acquisition experts from across the military services • Create an iterative development integrated product team with associated training
Software sustainment	• Direct that requests for proposals and contractor selection criteria include elements of the software framework supporting the software factory, including code and document repositories and software tools • Require contractors to provide documentation, such as test files and coding, to DOD • Consider selection of contractors based on the ability of DOD to reconstitute a contractor's software framework and rebuild binaries, re-run tests, procedures, and tools against delivered software and documentation
Independent verification and validation for machine learning[c]	• Establish research and experimentation programs around the practical use of machine learning in defense systems with efficient testing, independent verification and validation, and cybersecurity resiliency and hardening as the primary focus points • Establish a machine learning and autonomy data repository and exchange to collect and share necessary data from and for the deployment of machine learning and autonomy • Create and establish a methodology and best practices for the construction, validation, and deployment of machine learning systems

Source: GAO analysis of Defense Science Board (DSB) information. | GAO-23-105611

Note: Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington, D.C.: Feb. 14, 2018).

[a]Software factories use cloud-based computing to assemble a set of software tools enabling developers, users, and management to work together on a daily tempo.

[b]Continuous iterative development is a way of developing software in small blocks that can be incrementally evaluated by a user community. This incremental approach allows updates and improvements to be rapidly incorporated into the software.

[c]Independent verification and machine learning refers to using machine learning in software systems coupled with independent testing to help monitor the systems.

DIB Recommendations

Established in 2016 under the Federal Advisory Committee Act, the DIB provides independent recommendations to the Secretary of Defense and other senior DOD leaders on emerging technologies and innovative approaches for DOD to adopt.[25] Topics addressed by the DIB include digital modernization, software, and artificial intelligence. The DIB is

[25] Pub. L. No. 92-463 (1972) (codified as amended at 5 U.S.C. app. 2).

comprised of national security leaders, including from academia and the private sector.

When necessary, DOD may establish subcommittees and task forces through which the DIB provides recommendations, such as the subcommittee established to examine DOD's software acquisition and development practices. The DIB reports to the Secretary of Defense and the Deputy Secretary of Defense, who may act upon the DIB's recommendations.

In May 2019, the DIB released a report that emphasized the need for DOD to deploy software quickly, focus on continuous improvement throughout the software life cycle, and develop a workforce to follow modern software development practices.[26] The DIB study made 10 primary recommendations to address statutory, regulatory, and cultural hurdles DIB identified that DOD faces in modernizing its approach to software (see table 2).[27]

Table 2: GAO Summary of May 2019 DIB Software Modernization Recommendations

Recommendation	Recommended actions
New acquisition pathway	Establish one or more new acquisition pathways for software that prioritize continuous integration and delivery of working software in a secure manner, with continuous oversight from automated analytics
New appropriation category	Create a new appropriation category for software capability delivery that allows software to be funded as a single budget item, with no separation between research, development, test and evaluation, production, and sustainment
Security considerations	Make security a first-order consideration for all software-intensive systems
Software features	Shift from the use of rigid lists of requirements for software programs to desired features and required characteristics to avoid requirements creep, overly ambitious requirements, and program delays
Digital infrastructure	Establish and maintain digital infrastructure within the Department of Defense (DOD) and the military departments that enables rapid deployment of secure software to the field, and incentivize its use by contractors

[26] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 872(a) (2017). This section required the Secretary of Defense to direct the DIB to conduct a study on streamlining software development and acquisition regulations: Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Washington, D.C.: May 3, 2019).

[27] The DIB made a total of 26 software modernization recommendations to DOD. For the purposes of this report, we focused on the 10 primary recommendations, which DIB stated should be implemented first. There are 16 further recommendations—which we refer to as secondary recommendations—that DIB states are for DOD to implement once it has made sufficient progress on the primary recommendations.

Recommendation	Recommended actions
Automated testing and evaluation	Create, implement, support, and use fully automatable approaches to testing and evaluation, including security
Authorization to operate (ATO)[a] reciprocity	Create a mechanism for ATO reciprocity within and between programs, the military departments, and other DOD agencies to enable sharing of software platforms, components, and infrastructure, and rapid integration of capabilities
Source code access	Require access to source code, software frameworks, and development toolchains—with appropriate intellectual property rights—for DOD-specific code, enabling full security testing and rebuilding of binaries from source
Organization of development groups	Create software development units in each military department consisting of military and civilian personnel who develop and deploy software to the field using DevSecOps practices[b]
Acquisition workforce and training	Expand the use of training programs for leadership and program managers that provide insight into modern software development and the authorities available to enable rapid acquisition of software

Source: GAO analysis of Defense Innovation Board (DIB) information. | GAO-23-105611

Note: Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Washington, D.C.: May 3, 2019). The DIB made a total of 26 software modernization recommendations to DOD. For the purposes of this report, we focused on the 10 primary recommendations which the DIB stated should be implemented first. There are 16 further recommendations—which we refer to as secondary recommendations—that DIB states are for DOD to implement once it has made sufficient progress on the primary recommendations.

[a]The National Institute of Standards and Technology defines ATO as the official management decision given by a senior federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls. Continuous authorization, otherwise known as continuous authorization to operate, encompasses validating the quality and security of the software development platform, process, and platform team. It couples ATO with automation to produce real-time and continuous evidence, verifying the defensive posture of the platform and resulting software in real-time.

[b]Development, Security, and Operations (DevSecOps) is an iterative software development methodology that combines development, security, and operations as key elements in delivering useful capability to the user of the software.

Past GAO Work on Successful Implementation of Reform Efforts

Our prior work—including reports on leading practices on organizational mergers and transformations, collaboration, government streamlining and efficiency—shows that following certain change management practices helps to improve the likelihood of successful reforms.[28] Examples of practices associated with successful reforms identified by our prior work include:

- **Goals and outcomes of reforms.** Our prior work shows that establishing a mission-driven strategy and identifying specific desired outcomes to guide that strategy are critical to achieving intended results.

[28] GAO-18-427. A list of related GAO work is included in appendix I of GAO-18-427.

- **Process for developing reforms.** Our prior work shows that involving employees and key stakeholders is critical to developing reforms.
- **Implementing reforms.** Our prior work shows that incorporating change management practices improves the likelihood of successful reforms. We have also found that fully implementing major transformations can span several years and must be carefully and closely managed.
- **Strategically managing the federal workforce.** Our prior work has found that at the heart of any serious change management initiative are the people—because people define the organization's culture, drive its performance, and embody its knowledge base.

DOD's Efforts to Date At Least Partially Implement All DSB and DIB Recommendations

DOD has taken many steps to facilitate programs' ability to modernize software development and acquisition in recent years, which at least partially implemented all 17 DSB and DIB recommendations. DOD, however, has not implemented all recommended actions. DOD officials told us that, while they are not required to implement these actions because the DSB and DIB are federal advisory boards, they expect they may implement some of them through future software modernization efforts. These officials told us that, in other cases, they have determined that implementing the recommended actions would be impractical.

DOD Has Partially Implemented Most DSB and DIB Recommendations

Defense Science Board

As shown in table 3, DOD has taken steps that partially address each of the DSB's seven recommendations but has not implemented all specific recommended actions for any of the recommendations.

Table 3: GAO Analysis of DOD Implementation of DSB Software Modernization Recommendations

GAO summary of DSB recommendations	Implementation of specific actions
Evaluate software factories in source selection	◐
Adopt continuous iterative development best practices	◐
Adopt risk reduction metrics for new programs	◐

GAO summary of DSB recommendations	Implementation of specific actions
Transition current and legacy programs in development, production, and sustainment to continuous iterative development	◐
Begin workforce hiring and upskilling	◐
Review software sustainment documentation in source selection	◐
Independently verify and validate for machine learning	◐

Legend: ◐ = partially implemented.

Source: GAO analysis of Defense Science Board (DSB) report, Department of Defense (DOD) documents, and interviews with DOD officials. | GAO-23-105611

Notes: Defense Science Board*, Final Report of the Defense Science Board Task Force on the Design and Acquisition of Software for Defense Systems* (February 2018). If DOD took steps to implement some, but not most or all of the specific recommended actions, the recommendation was scored as partially implemented. We did not identify any DSB recommendations for which DOD had fully or substantially implemented all recommended actions or for which DOD had not taken any steps to implement recommended actions.

The following examples highlight actions taken by DOD that align with the DSB's recommendations as well as specific recommended actions DOD has not implemented.

Evaluate software factories in source selection. The DSB recommended several actions related to software factories, such as (1) establishing a common list of source selection criteria for evaluating software factories for use throughout DOD and (2) requiring that contractors demonstrate at least a pass-fail ability to construct a software factory to be considered minimally viable for a proposal. DOD has taken steps to address the recommended actions, but has not fully addressed them. For example, in August 2019, DOD published the *Enterprise DevSecOps Reference Design*, which establishes guidance for program managers on the DevSecOps ecosystem and life cycle, and applications.[29] The reference design includes some guidance to assess agency and vendor software factories.[30] However, use of the guidance is

[29] Department of Defense, *Enterprise DevSecOps Reference Design* (Aug. 12, 2019). The primary purpose of this document is to furnish a logical description of the key design components and processes to provide a repeatable reference design that can be used as a concrete example for a DOD DevSecOps software factory. DOD has also developed, and plans to develop, additional reference designs for its DevSecOps ecosystem.

[30] DOD has also taken related actions by establishing 29 software factories capable of delivering modern software at all phases of the software life cycle, including at least one software factory in each military department, such as the Department of the Air Force's Platform One and Kessel Run, the Navy's Forge, and Army's Software Factory.

not required and the guidance does not address whether it should be used as criteria during source selection.

Transition current and legacy programs in development, production, and sustainment to continuous iterative development. The DSB recommended several actions related to transitioning programs to continuous iterative development. These include having ongoing development programs plan to transition to a software factory and continuous iterative development and briefing best practices and lessons learned across the military departments. DOD has taken steps to address the recommended actions. For example, DOD established policies and guidance related to continuous iterative development for programs within the software acquisition pathway, including a process for new and legacy programs to enter the pathway.[31] DOD has also provided opportunities for programs to provide feedback and lessons learned about the adoption of modern software development practices. For instance, in February 2020, DOD published the *Agile Software Acquisition Guidebook*. The guidebook covers topics that programs should consider when transitioning to Agile practices as well as iterative development lessons learned from DOD's Agile pilots.

However, DOD has not implemented some of the specific recommended actions. For example, DOD officials stated that they do not intend to direct prime contractors to transition to a hybrid model and adopt continuous iterative development within current contracts, as recommended by the DSB. Officials noted, however, that they agree with the intent of the recommendation and that contractors who propose modern practices for future programs will likely be more competitive than contractors proposing a legacy model.

Begin workforce hiring and upskilling. The DSB recommended several actions related to workforce hiring and upskilling, such as establishing training curricula on modern software practices as well as acquiring and maintaining a small cadre of software systems architects with a deep understanding of iterative development. DOD has taken steps to address the recommended actions. For example, the Office of the USD(A&S) collaborated with the Defense Acquisition University (DAU) to establish

[31] Department of Defense, Department of Defense Instruction 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020). According to the instruction, current acquisition programs may elect to transition to the software acquisition pathway. In these instances, programs are to obtain approval for a transition approach that includes tailored processes, reviews, and documentation to effectively deliver software capabilities.

training in Agile and DevSecOps methods for DOD software development and acquisition staff, including DOD leadership. In addition, the military departments have also expanded or are planning to expand training opportunities on software intensive systems and practices. For example, the Air Force Institute of Technology provides DevSecOps courses for leadership, including program managers. However, additional work remains for DOD to implement all of the specific recommended actions. For instance, DOD has yet to develop a software cadre or training for that cadre. DOD has also yet establish a special software acquisition workforce fund, as recommended by the DSB.

Appendix II further details the implementation status of each DSB recommendation.

Defense Innovation Board

DOD has taken steps that fully or substantially implement four of the DIB's 10 recommendations and partially implement the remaining six recommendations (see table 4).

Table 4: GAO Analysis of DOD Implementation of DIB Software Modernization Recommendations

GAO summary of DIB recommendations	Implementation of specific actions
Create a new acquisition pathway for software	●
Create a new appropriation category for software	●[a]
Prioritize security considerations	●
Shift from system requirements to software features	◐
Use digital infrastructure to enable rapid deployment	◐
Use automated testing and evaluation approaches	◐
Create Authorization to Operate reciprocity between programs, services, and DOD agencies[b]	◐
Use source code access to enable security testing	◐
Use organic development groups to develop and deploy software	◐
Provide acquisition workforce training for leadership and program managers	●

Legend: ● = fully or substantially implemented; ◐ = partially implemented.

Source: GAO analysis of Defense Innovation Board (DIB) report, Department of Defense (DOD) documents, and interviews with DOD officials. | GAO-23-105611

Notes: Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 3, 2019). If DOD took steps to implement most or all of the specific actions and sub-actions, the recommendation was scored as fully or substantially implemented. If DOD took steps to implement some, but not most of the specific actions and sub-actions, the recommendation was scored as partially implemented. We did not identify any recommendations that DOD had not taken any steps to implement.

[a]While the Software and Digital Technology Pilot Program has not been made permanent, any further action to do so would require congressional action.

[b]The National Institute of Standards and Technology defines Authorization to Operate as the official management decision given by a senior official or officials to authorize operation of an information system and to accept the risk to operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.

The following examples highlight actions taken by DOD that align with DIB's recommendations as well as specific recommended actions DOD has not implemented.

Create a new acquisition pathway for software. The DIB recommended that DOD establish one or more new acquisition pathways for software that prioritize continuous integration and delivery of working software in a secure manner, with continuous oversight from automated analytics. DOD has addressed the recommendation. For example, in response to a legislative requirement, DOD established a pathway for the timely acquisition of software capabilities by using an iterative approach to software development.[32] DOD's policy for the software acquisition pathway provides opportunities for new and existing programs to join the pathway but does not require its use. Each program following the pathway must develop and track a set of metrics—using automated tools to the maximum extent practicable—to assess and manage, among other things, the performance, progress, speed, and quality of the software development, and the ability to meet users' needs. As of March 2023, there were 49 programs using the pathway.

Create a new appropriation category for software. The DIB recommended the creation of a new appropriation category for software capability delivery that allows software to be funded as a single budget item that could be used for the purposes of research, development, test, and evaluation (RDT&E), production, and sustainment. DOD has substantially addressed the recommendation. In December 2020, the Consolidated Appropriations Act of 2021 established the Software and Digital Technology Pilot Program.[33] The Office of the USD(A&S), in collaboration with the Under Secretary of Defense (Comptroller) (USD(C)), engaged Congress to establish the pilot. The act provides for certain programs to use RDT&E funding appropriated in that act for

[32] Pub. L. No. 116-92, § 800(a) (2019); Department of Defense Instruction 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

[33] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 8131(a) (2020).

procurement and sustainment activities.[34] Traditionally, software development programs have funded RDT&E, procurement, and sustainment activities through distinct appropriation categories. This pilot is intended to provide additional funding flexibility for software programs, particularly those using modern software development methods, such as iterative testing.

DOD does not plan for the pilot to be a permanent solution to software funding issues. Rather, DOD views the pilot as an opportunity to test whether the use of a single appropriation category enables modern software development practices. DOD intends to use the pilot for several years and work with Congress to implement a long-term solution based on lessons learned from the pilot. The pilot originally included eight programs. In May 2022, DOD officials told us that Congress has not approved recent requests to include additional pilot programs. However, DOD continues to collect data on the pilot programs to understand the effect of this funding mechanism on software development programs. As explained in the Joint Explanatory Statement accompanying the Consolidated Appropriations Act, 2023, the Secretary of Defense is encouraged to refrain from submitting additional pilot programs in future budget submissions until DOD has demonstrated its ability to collect data on performance improvements resulting from the pilot program.[35]

Use digital infrastructure to enable rapid deployment. The DIB recommended that DOD establish and maintain digital infrastructure within DOD and the military departments that enables rapid deployment of secure software to the field and incentivize its use by contractors. DOD has taken action to address the recommendation but has not fully implemented it.

DOD issued policy and guidance related to establishing and operating digital infrastructure, such as networks and software factories. For example, DOD's September 2019 *Enterprise DevSecOps Reference*

[34] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 8131(a). Subsequent appropriations acts included substantively similar language, but new initiatives under The Software and Digital Technology Pilot program were not included. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, § 8119(b) and Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 8107(b) (2022).

[35] 168 Cong. Rec. S7819, S8174 (Dec. 20, 2022) (joint explanatory statement to the Consolidated Appropriations Act, 2023, div. C, Dept. of Defense Appropriations Act, 2023).

Design provides programs with modern software development techniques that consider security and operations throughout, such as automated, iterative testing that begins earlier in the process.[36] In addition, this guidance encourages programs to use software factories. DOD has also issued guidance related to the department's cloud infrastructure, intended to provide users and systems with secure internet access to and from unclassified cloud environments. According to DOD officials, each military department has established a cloud environment.

However, additional work remains related to establishing and maintaining digital infrastructure, as outlined in DOD's key strategy documents. For example, while not yet achieved, DOD's February 2022 Software Modernization Strategy establishes several goals:

- accelerating the DOD enterprise cloud environment;
- transitioning from disparate cloud efforts to an integrated cloud portfolio;
- establishing a DOD-wide software factory ecosystem;
- leveraging established software factories; and
- scaling the services across the department.

Appendix III further details the implementation status of each DIB recommendation.[37]

DOD Plans to Implement Some but Not All Remaining Recommended Actions

Officials from the Office of the USD(A&S) stated that they have addressed the intent of the recommendations from the DSB and DIB reports and do not plan to implement all of the specific recommended

[36] Department of Defense, *Enterprise DevSecOps Reference Design* (Aug. 12, 2019). The primary purpose of this document is to furnish a logical description of the key design components and processes to provide a repeatable reference design that can be used as a concrete example for a DOD DevSecOps software factory. DOD has also developed, and plans to develop, additional reference designs for its DevSecOps ecosystem.

[37] For more information on DOD's efforts to address DIB's secondary recommendations, see appendix IV.

actions.[38] According to DOD officials, the department is not required to implement specific actions recommended in the reports because DSB and DIB are federal advisory committees.[39]

DOD officials told us that department-wide actions over the last several years have focused on encouraging—rather than requiring—programs to adopt modern software development and acquisition practices. Officials explained that this approach mitigates challenges with implementing the DSB and DIB recommendations that arose, in part, because older programs were less able to automate security and testing in a way that aligned with modern software development methods.

DOD officials told us they still plan to implement some specific recommended actions through their planned future software modernization efforts. For example, DOD plans additional actions to address DSB's recommendation that the military departments acquire or access a small cadre of software development professionals with a deep understanding of iterative development processes and practices. According to officials from the Office of the USD(A&S), further planning to implement this part of the recommendation is underway in response to a provision in the NDAA for Fiscal Year 2022.[40]

In other cases, DOD officials told us they chose not to implement the actions for specific reasons, such as the recommended actions being impractical. For example, they noted that DOD does not plan to fully implement the DSB's recommendation on transitioning programs to continuous iterative development. Specifically, DSB recommended that

[38] Section 868(a) of the National Defense Authorization Act for Fiscal Year 2019 states that DOD shall commence implementation of DSB's recommendations within 18 months of enactment of the Act, with certain exceptions, including delayed and nonimplementation. Pub. L. No. 115-232, § 868(a) (2019). The section states that the Secretary of Defense may opt to not implement a recommendation if the Secretary provides to the congressional defense committee the reason for nonimplementation and a summary of alternative actions. Pub. L. No. 115-232, § 868(b)(2). In April 2020, DOD submitted a report to Congress describing plans to implement DSB recommendations.

[39] Federal Advisory Committee Act, Pub. L. No. 92-463 (1972) (codified as amended at 5 U.S.C. app. 2). As noted above, advisory committees play an important role in informing public policy and government regulations by advising the President and federal agencies on national issues. GAO, Federal Advisory Committees: Actions Needs to Enhance Decision-Making Transparency and Cost Data Accuracy, GAO-20-575 (Washington, D.C.: Sept. 10, 2020).

[40] Pub. L. No. 117-81 § 836(a) (2021). This provision requires the USD(A&S) to establish a cadre of personnel who are experts in software development, acquisition, and sustainment to improve the effectiveness of related programs or activities at DOD.

prime contractors—within contract constraints—transition from waterfall to a more iterative software development approach, using a hybrid approach, if necessary, and incorporate iterative development into a long-term sustainment plan. Officials from the Office of the USD(A&S) stated that they do not intend to direct contractors to take these actions because it is unrealistic to do so for a large number of contracts. These officials added that programs can make assessments of individual contracts once they have an understanding of modern software development practices.

DOD's software modernization efforts are still underway, and, moving forward, DOD is focused on continuing efforts in the areas DSB and DIB emphasized. DOD officials stated that, as the department continues its software modernization efforts, they expect that additional actions recommended by DSB and DIB will be implemented. However, these officials also noted that certain steps recommended by DIB may become outdated as time passes and technology changes.

DOD Is Not Fully Positioned to Implement Future Software Modernization Efforts

DOD has outlined planned actions to continue its software modernization efforts across the department but has yet to incorporate certain key practices our prior work shows could help DOD implement these actions successfully.[41] While DOD's planning incorporated some elements of most of the practices we assessed, we identified gaps in the implementation of several of them.

DOD Plans Outline Transformational Future Software Modernization Efforts

DOD senior leadership has repeatedly emphasized the importance of ongoing software modernization efforts and the need for the department to take further actions. In a February 2022 memorandum approving the DOD Software Modernization Strategy, the Deputy Secretary of Defense stated that achieving faster delivery of software capabilities requires the combined focus of DOD senior leadership and significant changes in policies, technologies, processes, and workforce.

[41] Appendix V includes additional detail on the practices we used to assess DOD's preparation to implement future software modernization efforts.

DOD has detailed its plans for future software modernization efforts in three key department-wide strategies.[42]

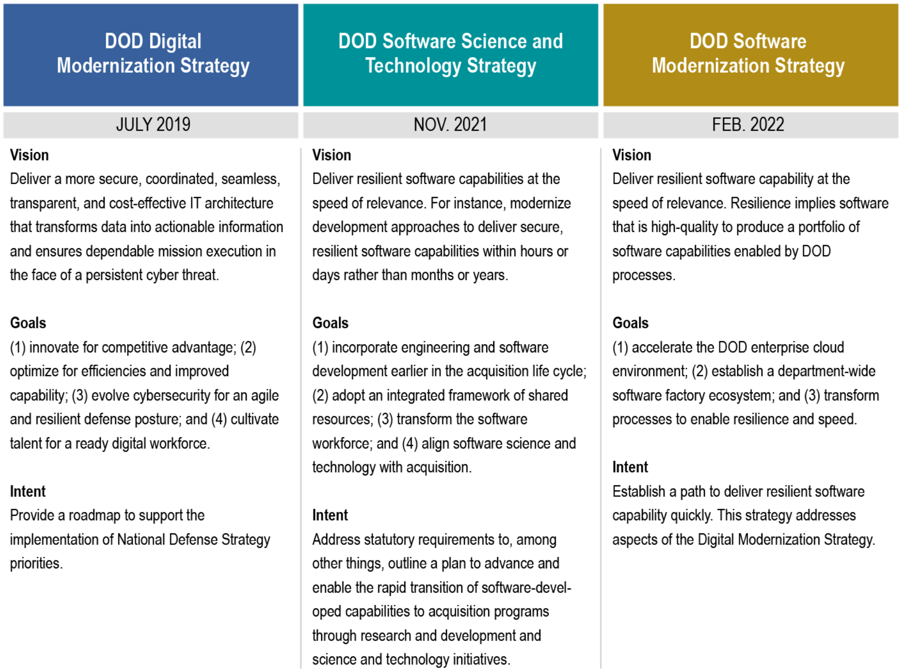
- ***Digital Modernization Strategy.*** Published in July 2019, this strategy supports implementation of the 2018 National Defense Strategy lines of effort involving cloud, artificial intelligence, command, control and communications, as well as cybersecurity.
- ***Software Modernization Strategy.*** Published in February 2022, this strategy is one of a set of sub-strategies of the Digital Modernization Strategy. The strategy provides a framework of technologies, approaches, and processes that must be addressed to modernize software delivery, such as adoption of DevSecOps, process and policy transformation, and workforce.
- ***Software Science and Technology Strategy.*** Published in November 2021 in response to a requirement in the NDAA for Fiscal Year 2020, this strategy is intended to guide strategic thinking within DOD to advance and enable the rapid transition of software-developed capabilities to acquisition programs through research and development and science and technology initiatives.[43] According to an official from the Office of the USD(R&E), the goals of this strategy align with the Software Modernization Strategy, but the Software Science and Technology Strategy is focused on the research and development of critical technologies while the Software Modernization Strategy aims to achieve faster delivery of software capabilities in support of DOD priorities.

Together, these strategies document the breadth of DOD's future software modernization efforts. Each plan includes a discussion of the department's vision and goals relevant to the scope of the plan (see fig. 5).

[42] Department of Defense, *Software Modernization Strategy* (Washington, D.C.: Feb. 2, 2022); Department of Defense, *Software Science and Technology Strategy* (Washington, D.C.: November 2021); and Department of Defense, *Department of Defense Digital Modernization Strategy*: *DOD Information Resource Management Strategic Plan Fiscal Years 2019–2023* (July 12, 2019).

[43] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92 § 255(b) (2019).

Figure 5: Visions, Goals, and Intent of the Department of Defense's (DOD) Key Software Modernization Strategies



DOD Digital Modernization Strategy	DOD Software Science and Technology Strategy	DOD Software Modernization Strategy
JULY 2019	NOV. 2021	FEB. 2022
Vision Deliver a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat.	**Vision** Deliver resilient software capabilities at the speed of relevance. For instance, modernize development approaches to deliver secure, resilient software capabilities within hours or days rather than months or years.	**Vision** Deliver resilient software capability at the speed of relevance. Resilience implies software that is high-quality to produce a portfolio of software capabilities enabled by DOD processes.
Goals (1) innovate for competitive advantage; (2) optimize for efficiencies and improved capability; (3) evolve cybersecurity for an agile and resilient defense posture; and (4) cultivate talent for a ready digital workforce.	**Goals** (1) incorporate engineering and software development earlier in the acquisition life cycle; (2) adopt an integrated framework of shared resources; (3) transform the software workforce; and (4) align software science and technology with acquisition.	**Goals** (1) accelerate the DOD enterprise cloud environment; (2) establish a department-wide software factory ecosystem; and (3) transform processes to enable resilience and speed.
Intent Provide a roadmap to support the implementation of National Defense Strategy priorities.	**Intent** Address statutory requirements to, among other things, outline a plan to advance and enable the rapid transition of software-developed capabilities to acquisition programs through research and development and science and technology initiatives.	**Intent** Establish a path to deliver resilient software capability quickly. This strategy addresses aspects of the Digital Modernization Strategy.

Source: GAO analysis of DOD documentation | GAO-23-105611

The plans further define each goal through objectives or focus areas. For example:

- To achieve its goal of establishing a department-wide software factory ecosystem, DOD outlines five key objectives in its Software Modernization Strategy, such as advancing DevSecOps through enterprise providers and accelerating software deployment with continuous authorization.
- To achieve its goal of transforming the software workforce, DOD outlines five focus areas in its Software Science and Technology Strategy—training and investing in data science, artificial intelligence, machine learning, and software engineering as well as cultivating a software engineering workforce.

According to DOD, these future software modernization efforts are expected to require sustained effort to fully implement. For example, DOD's Software Modernization Strategy states that software modernization is a continuous journey where success requires action and a shift in mindset and culture. In addition, Office of the USD(A&S) and DOT&E officials said that it will take time to develop and encourage the adoption of Agile software practices across the department and establish supporting infrastructure, such as training the software development, acquisition, and cybersecurity workforce in modern software methods.

DOD Has Yet to Fully Implement Key Practices to Facilitate Future Software Modernization Plans

In its preparation to implement future software modernization efforts, DOD fully or substantially followed two of six, partially followed three, and has yet to implement one of six selected practices that our prior work shows can help agencies implement transformative changes.[44] While DOD incorporated some elements of these four practices, we found gaps in the implementation of each.

DOD Involved a Range of Stakeholders and Engaged Employees to Facilitate Implementation

DOD has substantially followed key practices related to involving employees and key stakeholders, and employee engagement.

Involving employees and key stakeholders. DOD took steps or developed plans to involve Congress, key stakeholders, such as the private sector, and employees in developing software modernization reforms. Our prior work shows that involving employees and key stakeholders helps facilitate goals, incorporate insights, and increase acceptance of transformation change.[45] Examples of DOD's related efforts include:

- **Software acquisition pathway.** DOD has continuously involved employees in developing and refining aspects of the software acquisition pathway. OSD established a working group that collaborates with the military departments and other DOD organizations to shape policies and guidance related to the implementation of the pathway, according to officials from the Office of the USD(A&S). Additionally, the Office of the USD(A&S) continues to iteratively deploy guidance to aid programs transitioning to the pathway, including regularly updating policy and guidance and resources for the software acquisition pathway on DOD's Adaptive Acquisition Framework website. Officials from the Office of the USD(A&S) noted that these resources incorporate lessons learned and are intended to aid the software workforce in effectively delivering

[44] GAO-18-427. Appendix I provides additional information on how we selected the practices on which we evaluated DOD's efforts.

[45] GAO-18-427.

and acquiring software through the pathway. They added that they also consult directly with programs considering the pathway and plan to continue to do so as the pathway evolves.

- **Software and Digital Technology Pilot Program.** In December 2020, the Consolidated Appropriations Act of 2021 established the Software and Digital Technology Pilot program.[46] The Office of the USD(A&S), in collaboration with the Office of the USD(C), engaged Congress to help establish the pilot program.[47] Office of the USD(C) officials told us they proposed the single appropriation category to Congress after receiving initial support from within DOD. They noted that they continue to engage with Congress regarding proposals to expand the pilot, which began in fiscal year 2021. However, Congress has yet to approve any additional programs to date. DOD intends to execute the pilot for several years and subsequently work with Congress to implement a long-term funding solution.[48]
- **Ignite initiatives.** According to officials from the Office of the USD(A&S), they established initiatives—which DOD refers to as ignite initiatives—with a goal of transforming functions such as requirements, cost estimating, and test and evaluation processes for software. The officials said that these initiatives include representatives from Joint Staff, OSD, and the military departments to provide input on policies, processes, and culture to enable modern software delivery.

DOD has also involved industry stakeholders in developing reforms. For example, DOD collaborated with industry to develop the Continuous Iterative Development Measurement Framework, which is a comprehensive set of metrics to evaluate vendor software factories.

[46] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 8131(a) (2020).

[47] As previously described in this report, the Software and Digital Technology Pilot enables certain software-intensive programs to conduct RDT&E, procurement, and sustainment activities for identified pilot programs with a single RDT&E appropriation. DOD intends for the pilot program to provide more funding flexibility for software programs, particularly those using modern software development methods, such as iterative testing. Traditionally, software development programs have funded RDT&E, procurement, and sustainment activities through distinct appropriation categories. See Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 8131(a) (2021).

[48] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 8131(a). As noted above, new initiatives under the Software and Digital Technology Pilot program were not included in subsequent appropriations acts. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, § 8119(b) (2022) and Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 8107(b) (2022).

DOD also has plans to involve additional stakeholders in future reforms, such as by partnering with industry to improve contracting processes and ensure access to enterprise cloud services. Two of DOD’s key strategies establish goals and objectives related to working with industry, such as on cloud capabilities. For example, the Digital Modernization Strategy states that DOD will partner with industry to securely deliver cloud capabilities in alignment with mission requirements to achieve its goals. Further, the Software Modernization Strategy notes that DOD must partner with industry to improve contracting processes for cloud services, including a range of enterprise contracts that leverages existing acquisition success while avoiding duplication.

Employee engagement. DOD has taken several actions to sustain and strengthen employee engagement for its future software modernization reforms, such as educating employees, conducting targeted outreach, and forming working groups. Our past work emphasizes the importance of this step because people define the organization’s culture and drive its performance.[49] Examples of DOD’s efforts to engage employees include:

- DOD has communicated with employees on software modernization reform efforts. For example, the Office of the USD(A&S) performed outreach to and developed guidance for individual program offices to facilitate their transition to modern software approaches. OSD offices also offered training, such as through conferences and webinars, to educate the workforce on modern software approaches and why and how DOD needs to fundamentally transform the way it develops and acquires software.
- DOD and the military departments encourage participation in software communities of practice to share best practices and lessons learned on modern software approaches.
- According to an official from the Office of the USD(R&E), the office continuously engages with software factory stakeholders, such as the Office of the USD(A&S), DOD CIO, and software acquisition programs, at formal presentations and forums to understand what support software factories need from OSD organizations. These discussions include working with programs to help eliminate barriers for software factories.
- The Software Modernization SSG established an Action Officer Working Group that includes representatives from across DOD

[49] GAO-18-427.

organizations and the military departments to help coordinate future software modernization initiatives.

DOD Developed Outcome-Oriented Goals but Has Yet to Establish Performance Measures

DOD has partially followed a key practice related to establishing goals and outcomes. Our past work has found that agencies should establish clear outcome-oriented goals to help identify what they are trying to achieve with their reform efforts and should establish performance measures to assess the extent to which they are meeting their goals.[50] DOD's key department-wide strategies for software modernization establish clear outcome-oriented goals and objectives that align with DOD's mission and strategic plans, such as the National Defense Strategy.[51] For example:

- DOD's Digital Modernization Strategy outlines a goal to preserve and expand the U.S. military's competitive advantage against adversaries. This goal depends on the United States' ability to deliver technology faster, a theme throughout the 2018 National Defense Strategy. Specifically, the National Defense Strategy notes that continuously delivering performance with affordability and speed is a defense objective.
- DOD's Software Modernization and Science and Technology strategies state that software modernization requires the department to transform its software workforce to adopt the appropriate technical skills, such as equipping software engineers, developers, and testers with modern tool sets, processes, and capabilities. These efforts align with cultivating workforce talent, as discussed in the 2018 National Defense Strategy. Specifically, the National Defense Strategy notes that cultivating a lethal force relies on the ability of warfighters and others in DOD's workforce to integrate new capabilities, adapt warfighting approaches, and change business practices to achieve mission success. The Software Modernization Strategy states that DOD's workforce must understand its role in delivering software, streamline processes, push for automation, and better leverage technology.

However, DOD has yet to establish performance measures to assess progress toward its goals. According to DOD officials, the department is developing implementation plans that are expected to include

[50] GAO-18-427.

[51] In October 2022, DOD released the department's updated National Defense Strategy. For the purposes of this report, we review the 2018 National Defense Strategy because it was in place when DOD's strategies were developed.

performance measures.[52] Specifically, officials told us the Software Modernization Strategy implementation plan will include performance measures to assess progress against priority tasks, which track to outcome-oriented goals. DOD officials noted in November 2022 that the Software Modernization Strategy implementation plan is in draft and is expected to be published in the second quarter of fiscal year 2023. The Software Science and Technology Strategy states that its implementation plan will, among other things, establish and define metrics for outcome-oriented goals. According to DOD officials, the Software Science and Technology Strategy implementation plan is being drafted, with an estimated publication date in the first or second quarter of calendar year 2023.

While its plans to include performance measures in implementation plans are a positive step, DOD has yet to identify the steps it will take to develop effective measures. We have previously identified key attributes of successful performance measures, such as linkage to an agency's goals, which help organizations track the progress they are making and assess whether performance is meeting expectations (see appendix VI). DOD's key strategies do not establish any guidelines for the characteristics of performance measures to be developed. DOD officials noted they had yet to determine the particular measures they would use to assess progress against outcome-oriented goals because the plan is still in draft. As DOD finalizes implementation plans for its future software modernization efforts, ensuring that key attributes of successful performance measures are included, as appropriate, will help guarantee that DOD is well positioned to assess progress against outcome-oriented goals. In turn, the ability to assess progress will help DOD course correct, if necessary, to reach the desired software modernization outcomes.

DOD Established an Implementation Team but Has Yet to Fully Identify Resources or Responsibilities

DOD has partially followed a key practice related to leadership focus and attention. Our prior work shows that providing leadership for transformational reforms includes several things, such as establishing a dedicated implementation team with sufficient resources, designating leaders responsible for implementation, and holding those leaders accountable.[53] DOD has established an implementation team but has yet

[52] DOD officials told us that they did not develop an implementation plan for the Digital Modernization Strategy. Rather than a single implementation plan, DOD developed sub-strategies, including the Software Modernization and Software Science and Technology strategies, which expand on the themes of the Digital Modernization Strategy.

[53] GAO-18-427.

to identify the resources needed to lead DOD's software modernization efforts or fully determine how it will hold department leaders engaged in these efforts accountable.

Dedicated implementation team with capacity to manage reforms. DOD has established a dedicated implementation team to manage its software modernization reform process. The Software Modernization SSG is the main governance body that oversees and leads the implementation of software modernization reforms across DOD, including activities supporting the Software Modernization Strategy.

While DOD officials told us that individual working groups are assessing the requirements to execute key areas of the Software Modernization Strategy, DOD has yet to take steps to determine whether the Software Modernization SSG as a whole will have the capacity and resources necessary to lead software modernization activities. The Software Modernization SSG relies on its members from OSD organizations, the Joint Staff, and the military departments to identify the resources each member organization is able to devote to support software modernization implementation. DOD officials noted that these entities must balance their own ongoing organizational commitments with available staffing and resources to support software reform efforts.

Identifying needed staffing and resources for DOD's dedicated implementation team could help DOD ensure that the Software Modernization SSG can effectively carry out its leadership role in implementing software modernization efforts.

Assigning leadership roles and responsibilities and holding leaders accountable. DOD's current planning documentation broadly assigns high-level leadership responsibility for implementing software modernization reforms. For example, DOD's Software Modernization SSG is tri-chaired by senior representatives from Offices of the USD(A&S), USD(R&E), and DOD CIO. These organizations are tasked with leading collaboration with other DOD organizations and the military departments as well as making decisions related to DOD's software modernization activities. Additional membership of the Software Modernization SSG includes representatives from across DOD, including DOT&E, CAPE, Joint Staff, and the military departments. These organizations and departments are to provide representation in all efforts pertaining to modern software development and delivery.

DOD’s Software Modernization Strategy states that software modernization requires a cohesive departmental effort that involves various DOD organizations. The strategy states that implementation success depends heavily on partnerships and collaboration across the department given the role and pervasiveness of software across mission capabilities and supporting infrastructure. Further, the Deputy Secretary of Defense’s February 2022 memorandum approving the strategy stated that all offices and personnel are expected to provide the necessary support for software modernization.[54]

However, DOD has yet to fully develop an approach to hold accountable the many leaders who will need to be involved in implementing software modernization reforms. This is in part because DOD has yet to fully identify in key documents what entities will be involved in executing software modernization efforts and what their specific responsibilities will entail. For example, DOD’s current planning documentation, including the Software Modernization and Software Science and Technology strategies, do not address the specific responsibilities of OSD offices with leadership roles or of the military departments and other organizations involved in implementation.

According to DOD officials, once issued, the Software Modernization Strategy implementation plan will identify an Office of Primary Responsibility to support key lines of effort. For example, individual DOD organizations and military departments will be responsible for implementing modern software practices, such as cloud computing and DevSecOps, at the program- and component-levels. The Software Modernization SSG is expected to monitor the efforts of these organizations. Office of the USD(A&S) officials noted that software modernization at DOD relies heavily on the DOD organizations and military departments.

While assigning lead offices is an important step in implementation planning, this approach, as described by DOD, does not ensure that DOD will fully identify the specific roles and responsibilities of leaders involved in transformational software reforms. Until DOD fully identifies the roles and responsibilities for these leaders, DOD will likely be challenged to hold them accountable for implementation.

[54] Department of Defense, Deputy Secretary of Defense, *Department of Defense Software Modernization* (Washington, D.C.: Feb 2. 2022).

DOD Is Developing Implementation Plans but Has Yet to Identify Data Collection Methods for Monitoring Progress

DOD has yet to implement a key practice related to managing and monitoring implementation. Our prior work emphasizes the importance of developing an implementation plan with key milestones and deliverables and putting in place processes to collect the needed data and evidence to effectively measure the reforms' outcome-oriented goals.[55] DOD is in the process of developing implementation plans for its key strategies, although these plans have been delayed from their original planned release dates. Further, DOD has yet to describe how the department plans to collect the data necessary to measure progress in achieving strategic goals.

Developing implementation plans. According to DOD officials, the implementation plans they are developing for the Software Modernization and Software Science and Technology strategies are expected to include key milestones and deliverables to track implementation progress.[56] For example, DOD officials told us that the Software Modernization Strategy implementation plan will include a governance structure to assess, reprioritize, and track progress toward goals, such as measureable deliverables and milestones per activity outlined in strategic goals.

However, DOD has yet to publish these plans and has already delayed its anticipated completion dates for the Software Modernization Strategy. The February 2022 approval memorandum from the Deputy Secretary of Defense for the Software Modernization Strategy directed the delivery of an implementation plan within 180 days, which would have been in August 2022.[57] The planned completion date for this plan has now slipped to the second quarter of fiscal year 2023. According to a DOD official, delays in publishing the implementation plan are due to the need for additional time for internal coordination among DOD leadership to clear for publication. Further, DOD officials told us that the Software Science and Technology Strategy implementation plan is expected to be published after the Software Modernization Strategy implementation plan to, in part, ensure that the goals outlined in both plans align. Given the

[55] GAO-18-427.

[56] DOD's Software Modernization Strategy is a subset of DOD's Digital Modernization Strategy. DOD officials told us they do not plan to develop a separate implementation plan for the Digital Modernization Strategy.

[57] Department of Defense, Deputy Secretary of Defense, *Department of Defense Software Modernization* (Washington, D.C.: Feb 2. 2022).

importance of these plans in helping to manage and monitor implementation, it is essential that DOD finalizes them in a timely manner.

Processes and data to measure effectiveness of reforms. DOD has yet to describe how the department plans to collect the data necessary to effectively assess its progress against performance measures. According to DOD officials, the department plans to collect data to measure performance and expects to analyze it in Advana—DOD's enterprise data platform. However, DOD officials have yet to fully identify the methods they plan to use to collect data across the department or specify how they plan to use the data collected, in part, because DOD's data collection efforts related to software modernization to date have focused on the software acquisition pathway.

DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*, requires pathway programs to report data to assess and manage program performance and progress, such as average lead time and value assessment rating. However, software acquisition pathway program metrics and reporting requirements apply to a selected group of programs out of many in the department that are developing or acquiring software.[58] Further, the software acquisition pathway is one component of DOD's software modernization efforts outlined in department-wide software strategies and does not represent the breadth of planned software modernization efforts.

Developing implementation plans for the Software Modernization and the Software Science and Technology strategies and establishing processes to collect the necessary data and evidence will help DOD ensure it is well positioned to measure progress toward implementing its goals.

DOD Has Yet to Conduct Strategic Planning for Its Software Workforce

DOD has partially followed a key practice related to strategic workforce planning. Our prior work has found that agencies should complete this planning to ensure they have the needed resources and capacity to successfully execute reforms.[59] DOD has taken initial steps to identify its software workforce, a crucial effort that must be completed prior to conducting strategic workforce planning. However, it has yet to determine whether it has the needed workforce resources and capacity to successfully execute planned software modernization reforms.

[58] As of March 2023, there were 49 programs using the software acquisition pathway.

[59] GAO-18-427.

According to DOD, a workforce skilled in modern software development practices is fundamental to carrying out software modernization efforts. DOD's Software Modernization Strategy states that modern software practices require a shift in DOD's workforce and that developing, training, and recruiting that workforce are critical elements of software modernization. Both DOD's Software Science and Technology and Digital Modernization strategies identify transforming DOD's software workforce as a key goal.

Identifying the software workforce. DOD is taking initial steps to identify the makeup of its current software workforce. According to officials from the Office of the USD(A&S), determining the composition of the software workforce, such as identifying DOD professionals that currently make up the software workforce and the additional roles that would be needed to successfully adopt department-wide reforms, has been a challenge. A 2020 RAND study noted that DOD lacks a workforce model that properly supports a software acquisition workforce, such as an official software career field or a system for identifying or tracking software professionals in the department.[60] This study included a recommendation for the department to identify who is in the software acquisition workforce and presented options for DOD to track and manage this workforce.

In July 2021, the department established the Digital Talent Management Forum, which aims to identify and define key software engineering roles needed for modern software delivery, according to DOD officials.[61] These officials noted that the forum is supporting DOD CIO's efforts to expand the DOD Cyber Workforce Framework to include software engineering and software testing roles in the framework's database.[62]

[60] RAND Corporation, *Software Acquisition Workforce Initiative for the Department of Defense* (Santa Monica, Calif.: 2020).

[61] According to DOD officials, the Digital Talent Management Forum is co-chaired by the Offices of the USD(A&S) and USD(R&E). The group includes more than 60 representatives across DOD, including DOD CIO, the Office of the Under Secretary of Defense for Personnel and Readiness, and military departments.

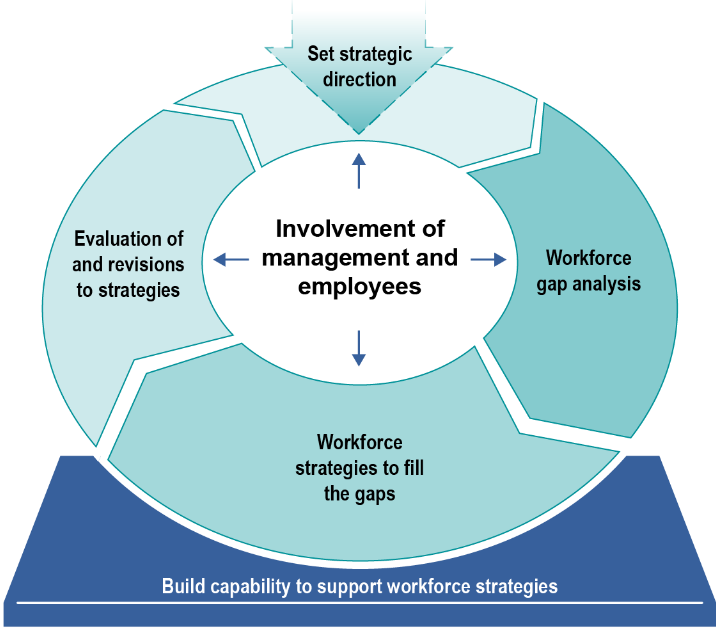
[62] The DOD Cyber Workforce Framework is intended to establish DOD's standard lexicon based on the work an individual is performing, not position titles or occupational series, among other things. According to DOD officials, the Digital Talent Management Forum is leveraging the DOD Cyber Workforce Framework to expand workforce functional areas to include software, data science, and artificial intelligence. When approved, DOD plans to combine the software-related work roles with the data science and artificial intelligence work roles in an expanded DOD Cyber Workforce Framework tool.

An official from the Office of the Under Secretary of Defense for Personnel and Readiness explained that, through this effort, the department is working to collect data to identify software professionals across DOD's workforce, such as those performing software functions that may not be captured in a job title or occupational series. The official noted that identifying the software workforce is currently a challenge for DOD because software professionals work across many occupational series. Once DOD captures the data, officials expect it will provide department-wide information on the software workforce composition, expertise, and skill sets. DOD officials said this data capture effort is expected to take about 12 to 18 months. The resulting insight into the composition of its software workforce should help DOD determine what resources are needed to support software modernization reforms.

Conducting strategic workforce planning. While identifying the workforce is a critical step, it is only the first step in a longer process to ensure that DOD will have the workforce it needs to execute its software modernization reforms. Key principles for strategic workforce planning in our prior work state that this planning should address two critical needs: 1) aligning an organization's human capital program with its current and emerging mission and programmatic goals and 2) developing long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals.[63] Figure 6 illustrates the strategic workforce planning process.

[63] GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

Figure 6: Strategic Workforce Planning Process


Set strategic direction
Involvement of management and employees
Evaluation of and revisions to strategies
Workforce gap analysis
Workforce strategies to fill the gaps
Build capability to support workforce strategies

Source: GAO-04-39 | GAO-23-105611

DOD has yet to determine how it will execute this broader strategic workforce planning process for its software modernization efforts. DOD officials acknowledged that data collection is only the first step in conducting workforce planning. They noted that once software workforce professionals are properly identified in personnel data, DOD can conduct a workforce capability assessment. However, officials noted that DOD is still in the early stages of these identification efforts. Similarly, an Office of the Under Secretary of Defense for Personnel and Readiness official noted that DOD is currently focused on elements that must be in place before strategic workforce planning can begin, such as determining the critical skills and competencies the software acquisition workforce needs to achieve programmatic results.

Strategic workforce planning for software modernization efforts is likely to take a number of years and will need to involve the coordinated efforts of management, employees, and key stakeholders across DOD. Developing a department-wide strategic workforce plan for DOD's software workforce—including strategies tailored to address gaps in the critical skills and competencies—will help position DOD to execute next steps in this planning process and achieve future software modernization goals.[64]

Conclusions

DOD has made numerous efforts to modernize its software acquisition and development approaches in recent years, but much work remains in this crucial area. DOD's recently-issued software strategies include ambitious goals that are essential to moving from early adoption of modern software practices by selected programs to a lasting, department-wide transformation. Meeting these goals will improve DOD's ability to keep pace with strategic competitors, such as Russia and China.

As DOD begins to translate its goals into action, incorporating key change management practices identified in our past work will help senior leadership oversee continued progress towards software transformation. For example, taking action to develop meaningful performance measures, establish data collection strategies for measuring performance, and finalize implementation plans can help DOD track progress towards achieving and implementing software modernization goals. Moreover, establishing a sufficiently-resourced implementation team and delineating roles and responsibilities associated with software modernization efforts can help ensure that leaders have the resources they need to implement reforms and are held accountable for achieving them.

Further, building a workforce—with critical skills and competencies—that can implement these reforms is foundational to all of DOD's planned actions. Until DOD determines when and how it will conduct effective workforce planning for its software workforce, its ability to implement its planned actions and meaningfully transform its software acquisition practices as intended remains in question.

Recommendations for Executive Action

We are making the following seven recommendations to DOD:

The Secretary of Defense should ensure that, as the Software Modernization SSG and other relevant entities develop performance measures for future software modernization efforts, these measures incorporate GAO's key attributes of successful performance measures, to

[64] We have consistently reported in our High-Risk List that skills gaps within the federal workforce persist. See 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); *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 6, 2019); and *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

the extent appropriate, to track progress towards achieving agency goals. (Recommendation 1)

The Secretary of Defense should direct the USD(A&S), USD(R&E), and DOD CIO to identify the resources needed, such as staffing and funding, to lead DOD's software acquisition and development reform efforts, and to address any related deficiencies these officials identify. (Recommendation 2)

The Secretary of Defense should fully identify roles and responsibilities for leaders throughout the department for carrying out reforms included in key software strategies. (Recommendation 3)

The Secretary of Defense should ensure the USD(A&S), USD(R&E), and DOD CIO finalize an implementation plan that includes key milestones and deliverables to track progress on implementing the Software Modernization Strategy. (Recommendation 4)

The Secretary of Defense should ensure the USD(R&E) finalizes an implementation plan that includes key milestones and deliverables to track progress on implementing the Software Science and Technology Strategy. (Recommendation 5)

The Secretary of Defense should direct the USD(A&S), USD(R&E), and DOD CIO to establish processes to collect the data necessary to effectively measure progress against outcome-oriented goals related to software modernization efforts. (Recommendation 6)

The Secretary of Defense should ensure that, once the software workforce is identified, the USD(A&S), the Under Secretary of Defense for Personnel and Readiness, and other relevant entities, use that information to develop a department-wide strategic workforce plan that identifies strategies tailored to address gaps in the critical skills and competencies needed to achieve software modernization goals. (Recommendation 7)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. In written comments provided by DOD (reproduced in appendix VII), DOD concurred with four recommendations and partially concurred with three.

DOD concurred with our first, third, fourth and fifth recommendations. If effectively implemented, DOD's planned actions to address our first, fourth, and fifth recommendations related to performance measures and implementation plans should address the intent of our recommendations. With regard to our third recommendation to identify roles and responsibilities for reform leaders, however, the steps outlined in DOD's written comments are not likely to fully address challenges that we identified in the report. DOD stated that it plans to identify an Office of Primary Responsibility in its Software Modernization Strategy implementation plan. In the report, we acknowledge that assigning lead offices is an important element in implementation planning. Yet, DOD's stated approach does not ensure that DOD will fully identify the specific roles and responsibilities of leaders involved in transformational software reforms. Until DOD fully identifies the roles and responsibilities for these leaders, DOD will likely be challenged to hold officials in charge of DOD's transformation accountable for implementation.

DOD partially concurred with our second recommendation to identify needed resources, including staffing and funding to lead software modernization efforts and to address any identified deficiencies. Specifically, DOD stated that the Software Modernization SSG—DOD's software modernization implementation team—is supported by OSD teams, which balance ongoing commitments with available resources. DOD also stated that its software modernization efforts will rely heavily on the military departments and DOD organizations rather than on a centrally funded OSD approach. Further, DOD stated that each of the key software modernization activities is directed by a representative from an Office of Primary Responsibility to ensure that sufficient resources are available, among other things.

We acknowledge that the military departments and DOD components will have a significant role in the resourcing and execution of software modernization activities and are not recommending that the department adopt a centrally funded OSD approach. Further, we understand that planned Offices of Primary Responsibility are to lead aspects of DOD's Software Modernization Strategy implementation plan and ensure that military department and component resources are available for these efforts, among other things. However, as stated in the report, identifying necessary resources and addressing any related deficiencies for DOD's dedicated implementation team could help DOD ensure that the Software Modernization SSG, in its leadership role, can effectively guide a coordinated effort to achieve a cohesive, department-wide software modernization transformation. This includes adequate resources to oversee the Offices of Primary Responsibility as they coordinate execution of the Software Modernization Strategy.

DOD partially concurred with our sixth recommendation to establish processes to collect data to measure progress against software modernization goals. DOD stated that the draft Software Modernization Strategy implementation plan identifies tasks for collecting key metrics to inform enterprise-level trends. In addition, DOD noted that progress against goals will be measured, such as through quantitative or qualitative data, or other means as appropriate. DOD added that individual program execution progress and delivery reporting data will be determined and reviewed by the appropriate component decision authority in support of their oversight responsibilities. We agree that different types of data will likely be appropriate for oversight and different organizational levels. Accordingly, DOD's plan to identify tasks for collecting key metrics and data to assess progress against software modernization goals, if fully implemented, would address our recommendation.

DOD partially concurred with our seventh recommendation to develop a department-wide strategic workforce plan to facilitate achievement of software modernization goals. DOD stated that the DOD CIO developed and approved new software work roles for incorporation into DOD's Cyber Workforce Framework, in coordination with relevant offices. Further, DOD stated that the Office of the USD(A&S) plans to work with the Office of the Under Secretary of Defense for Personnel and Readiness to develop a targeted strategic workforce plan that will address any identified skills or competency gaps. We believe DOD's plan to develop a strategic workforce plan that addresses identified skill or competency gaps in DOD's software workforce, if fully implemented, would address our recommendation.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Defense. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or oakleys@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 key contributions to this report are listed in appendix VIII.

Shelby S. Oakley

Shelby S. Oakley
Director, Contracting and National Security Acquisitions

List of Committees

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

The Honorable Jon Tester
Chair
The Honorable Susan Collins
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

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

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

Appendix I: Objectives, Scope, and Methodology

This report assesses the extent to which the Department of Defense (DOD) (1) has implemented recent Defense Science Board (DSB) and Defense Innovation Board (DIB) software modernization recommendations; and (2) is positioned to implement future software modernization efforts.

To determine the extent to which DOD has implemented recent DSB and DIB recommendations, we reviewed DSB's 2018 and DIB's 2019 reports, including DSB's seven recommendations and DIB's 10 primary recommendations to DOD.[1] In addition, we reviewed certain software-related provisions in the National Defense Authorization Acts (NDAA) for Fiscal Years 2018 through 2022 to identify relevant statutory requirements.[2] For example, Section 800(a) of the NDAA for Fiscal Year 2020 directed DOD to develop the software acquisition pathway.[3] We also reviewed agency policies and guidance, such as DOD Instruction 5000.02, *Operation of the Adaptive Acquisition Framework*, and DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*, and reports to Congress, including DOD's 2020 report to Congress on the implementation of DSB recommendations.[4]

We compared the information we collected about DOD's software modernization efforts to DSB and DIB's recommendations to analyze the extent to which DOD implemented each recommendation, such as fully or substantially or partially implemented. Multiple analysts reviewed the evidence related to each recommendation to determine the extent to which DOD implemented the recommendations and held discussions to resolve any disagreements. We assessed a recommendation as being

[1] In May 2019, the DIB made 26 total software modernization recommendations to DOD. For the purposes of this report, we focused on the 10 primary recommendations, which DIB stated should be implemented first. There are a further 16 recommendations—which we refer to as secondary recommendations—that DIB states are for DOD to implement once it has made sufficient progress on the primary recommendations. For more information on DOD's efforts to address DIB's secondary recommendations, see appendix IV.

[2] Pub. L. No. 115-91 (2017); Pub. L. No. 115-232 (2018); Pub. L. 116-92 (2019); Pub. L. No. 116-283 (2021); Pub. L. No. 117-81 (2021).

[3] Pub. L. No. 116-92, § 800(a) (2019).

[4] Department of Defense, Department of Defense Instruction 5000.02, *Operation of the Adaptive Acquisition Framework* (Jan. 23, 2020); and Department of Defense, Department of Defense Instruction 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

fully or substantially implemented if DOD took actions that addressed most or all aspects of the recommendation. We assessed a recommendation as being partially implemented if DOD took actions that addressed some, but not most, aspects of the recommendation. We did not identify any recommendations that DOD had not taken any steps to implement.

To determine the extent to which DOD is positioned to implement future software modernization efforts, we assessed DOD's efforts against selected practices identified in our prior work as being associated with successful agency reform efforts. Our prior work identifies 12 subcategories of change management practices.[5] We focused our assessment on six of the 12 subcategories—(1) establishing goals and outcomes; (2) involving employees and key stakeholders; (3) leadership focus and attention; (4) managing and monitoring; (5) employee engagement; and (6) strategic workforce planning. We selected key questions for those practices that we determined were most relevant to implementing DOD's future software modernization efforts.[6]

To obtain information about DOD's positioning to implement its future software modernization efforts, we analyzed strategy documents, such as DOD's February 2022 Software Modernization Strategy and November 2021 Software Science and Technology Strategy. This enabled us to identify DOD's future software modernization plans. We also interviewed DOD officials about their planning and implementation efforts.[7] Multiple analysts reviewed the evidence related to each selected practice from our past work drawn from the documents and interviews described above and below and independently rated DOD as having either fully or substantially followed, partially followed, or not followed each practice. The analysts then met to resolve any differences. We assessed a practice as fully or substantially followed if DOD took actions that addressed most or all aspects of the selected key questions we examined for the practice. We assessed a practice as partially followed if DOD took actions that

[5] GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018).

[6] We did not include six subcategories that we determined were less relevant for the purposes of our assessment. For example, one focuses on the costs related to workforce reduction strategies, but DOD's software modernization efforts do not include workforce reduction changes.

[7] Department of Defense, *Software Modernization Strategy* (Washington, D.C.: Feb. 2, 2022); and Department of Defense, *Software Science and Technology Strategy* (Washington, D.C.: November 2021).

addressed some, but not most, aspects of the selected key questions we examined for the practice. We assessed a practice as not followed if DOD had yet to take action that addressed aspects of the selected key questions we examined for the practice.

For both objectives, we interviewed officials from DOD's Office of the Secretary of Defense, including: the Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the Under Secretary of Defense for Research and Engineering, Office of the Under Secretary of Defense for Personnel and Readiness, Under Secretary of Defense (Comptroller), DOD Office of the Chief Information Officer, Director, Operational Test & Evaluation, and the Office of Cost Assessment and Program Evaluation.

We also interviewed officials from the Office of the Chairman of the Joint Chiefs of Staff (Joint Staff), military department officials, such as from the Office of the Assistant Secretary of the Air Force for Acquisition, Technology & Logistics, Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology), and the Office of the Assistant Secretary of the Navy for Research, Development and Acquisition, as well as officials from Defense Acquisition University and the DSB.[8]

During these interviews, we discussed topics such as the current status of DOD's implementation of DSB and DIB recommendations as well as the focus of DOD's software modernization efforts and the challenges encountered. We also discussed DOD's planning and implementation of the agency's future software modernization efforts.

We conducted this performance audit from December 2021 to April 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[8] We did not interview DIB officials because the DIB was in a strategic pause at the time of this review, according to DOD officials. In addition, we did not interview DIB or DSB study members because study members were not readily available for interview as they were no longer affiliated with the DIB, DSB, or DOD.

Appendix II: Assessment of Department of Defense (DOD) Implementation of Defense Science Board (DSB) Software Modernization Recommendations

Table 5 shows the status of DOD's implementation of DSB's recommended actions, including key stakeholders.

Table 5: Department of Defense (DOD) Implementation of Defense Science Board (DSB) Software Modernization Recommendations

Recommendation and key stakeholders	Status	Implementation details
Software factory[a] 1. Establish a common list of source selection criteria for evaluating software factories for use throughout the department. 2. Contractors should have to demonstrate at least a pass-fail ability to construct a software factory to be considered minimally viable. 3. Criteria should be reviewed and updated every 5 years. **Key stakeholders** Under Secretary of Defense for Research and Engineering (USD(R&E)) Defense Digital Service Software Engineering Institute[b] Military departments	◐	DOD has provided guidance related to assessing software factories during the source selection process but has yet to establish a common list of source selection criteria for evaluating software factories for use throughout the department. In August 2019, DOD published the Enterprise DevSecOps[c] Reference Design, which establishes guidance for program managers on the DevSecOps ecosystem and life cycle as well as applications. The reference design includes some guidance to assess agency and vendor software factories. According to Office of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) officials, the reference design is to be updated every 6 months. However, use of the guidance is not required and the guidance does not address whether it should be used as criteria during source selection. DOD officials noted that standardizing criteria across each entity that has developed a DevSecOps pipeline is impractical. According to an Office of the USD(R&E) official, DOD has begun to take further action on this specific recommended action, but doing so has been a challenge. For example, the Office of the USD(R&E) funded studies to determine how related aspects of source selection for software can be improved. Yet, the official noted that these efforts will require pilots and test cases that must be conducted and reviewed prior to taking specific action to implement recommended source selection improvements. As of November 2022, the Office of the USD(R&E) has yet to develop a plan for executing pilots and test cases. DOD has yet to require contractors to demonstrate at least a pass-fail ability to construct a software factory to be considered minimally viable or require source selection criteria related to software factories to be reviewed or updated every 5 years. DOD has taken related actions by establishing 29 software factories, including at least one software factory in each military department, such as the Department of the Air Force's Platform One and Kessel Run, the Navy's Forge, and Army's Software Factory.

Recommendation and key stakeholders	Status	Implementation details
Continuous iterative development 1. Adopt continuous iterative development best practices for software, including through sustainment, and evaluation, including security. 2. Identify minimum viable product approaches and delegate acquisition authority to program managers to provide motivation to do minimum viable products. 3. Require all programs entering Milestone B to implement iterative processes for acquisition category I, II, and III programs. 4. Identify best practices and incorporate into regular program reviews. **Key stakeholders** Office of the Chairman of the Joint Chiefs of Staff (Joint Staff) Military departments	◐	DOD has taken steps to adopt continuous iterative development best practices for programs using its software acquisition pathway. In October 2020, DOD published DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*. The instruction establishes policy to facilitate rapid and iterative delivery of software capability to DOD. For example, the software acquisition pathway provides a framework and guidance for adopting iterative development best practices. Included within the instruction is guidance for pathway programs to define the minimum viable product.[d] Specifically, the pathway directs the program manager and sponsor to use an iterative process to define the minimum viable product.[e] Further, DOD has identified minimum viable product approaches through its *Enterprise DevSecOps Reference Design*, which is directed to DOD programs utilizing DevSecOps software factories to deliver applications to end users. The guidance states that developing a minimum viable product is a best practice for critical business needs to gain user feedback. Further, according to Joint Staff officials, Joint Staff assists programs in developing minimum viable product values in requirements documentation. DOD has yet to require major defense acquisition programs entering Milestone B to implement iterative processes.[f] DOD policies and guidance related to continuous iterative development are largely targeted to programs using the software acquisition pathway and DevSecOps processes, and do not require all software-intensive systems to implement iterative processes. For example, DOD Instruction 5000.85, *Major Capability Acquisition* —which establishes policy and procedures for major defense acquisition programs as well as other programs categorized as acquisition category I, major systems, usually categorized as acquisition category II, and other programs, such as acquisition category III programs—does not require major capability acquisition pathway programs to implement iterative software development processes. Officials explained that they encourage programs to transition to software factories and continuous iterative development, but DOD does not require programs to do so. The military departments have not directed substantial changes to program reviews to account for continuous iterative development best practices.

Recommendation and key stakeholders	Status	Implementation details
Adopt risk reduction metrics for new programs 1. Allow multiple vendors to begin work. A down-select should happen after at least one vendor has proven they can do the work, and programs should retain several vendors through development to reduce risk, as feasible. 2. Modernize cost and schedule estimates and measurements. They should evolve from a pure source line of code approach to historical comparisons as a measurement and should adopt the National Reconnaissance Office approach of contracting with the defense industrial base for work breakdown schedule data to include staff, cost, and productivity. 3. Build a program-appropriate framework for status estimation. **Key stakeholders** USD(R&E) Cost Assessment and Program Evaluation (CAPE) Military departments	◐	DOD has not taken action to require multiple vendors to begin work prior to down-selecting vendors. Officials from the Office of the USD(A&S) told us they do not plan to direct programs to take a specific approach to source selection. DOD has taken some steps to modernize cost and schedule estimates and measurements. In March 2020, DOD published DOD Instruction 5000.73, *Cost Analysis Guidance and Procedures*. The instruction establishes policy for conducting cost estimation and analysis at DOD. According to the instruction, CAPE provides independent cost estimates for software acquisition pathway programs before programs enter the execution phase. In addition, the instruction generally contains cost estimation guidance for software programs, including a discussion of risk. For example, all cost estimates must include a discussion of risk, potential effects of risk on program cost and schedule as well as risk mitigation approaches. CAPE officials also stated they have updated the Software Resources Data Report—which collects technical and cost data on software development, maintenance, and enterprise resource planning development efforts—to collect metrics on Agile software methods. Further, DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*, states that programs will continue to update cost estimates during both phases of the software acquisition pathway. The software acquisition pathway also requires programs to develop and track program-appropriate metrics to assess and manage program status, including performance, progress, and speed. The Office of the USD(A&S) also developed guidance for software acquisition pathway programs on metrics for process efficiency, software quality, software development progress, and cost metrics, among others. However, DOD's actions related to establishing cost and schedule estimates and other metrics are largely targeted to programs using the software acquisition pathway and have yet to address all software-intensive systems.

Recommendation and key stakeholders	Status	Implementation details
Current and legacy programs in development, production, and sustainment 1. For ongoing development programs, plan to transition to a software factory and continuous iterative development. 2. Defense prime contractors should transition execution to a hybrid model, within the constraints of their current contracts. Defense prime contractors should incorporate continuous iterative development into a long-term sustainment plan. 3. Provide a quarterly status update to the USD(A&S) on the transition plan for programs. 4. For legacy programs where development is complete, make the business case for whether to transition the program. 5. Programs that have transitioned successfully to modern software development practices are to brief best practices and lessons learned across the military departments. **Key stakeholders** USD(A&S) Military departments	◐	DOD has not required ongoing development programs to transition to modern software development approaches. According to Office of the USD(A&S) officials, DOD's efforts have focused on encouraging—not requiring—programs to adopt to modern software development approaches. To encourage programs to transition to modern approaches, DOD established policies and guidance for current programs within the software acquisition pathway as well as new and legacy programs planning to transition to the pathway. For example, according to DOD Instruction 5000.87, current acquisition programs may elect to transition to the software acquisition pathway. In these instances, programs are to obtain approval for a transition approach that includes tailored processes, reviews, and documentation to effectively deliver software capabilities. DOD officials stated that they do not intend to direct prime contractors to transition to a hybrid model and adopt continuous iterative development within current contracts because it is unrealistic to do so. However, officials also stated that they agree with the intent of the recommendation and that contractors who propose modern practices for future programs will likely be more competitive than contractors proposing a legacy model. DOD has also not required military departments to provide quarterly updates to the Office of the USD(A&S) on program transition plans. DOD has not required legacy programs to make a business case for whether to transition the program. As noted above, DOD's efforts have focused on encouraging—not requiring—programs to adopt to modern software development approaches. DOD has provided opportunities for programs to provide feedback and lessons learned about the adoption of modern software development practices. For example, in February 2020, DOD published the *Agile Software Acquisition Guidebook*. The guidebook covers topics that programs should consider when transitioning to Agile practices as well as Agile and iterative development lessons learned from DOD's Agile pilots.

Recommendation and key stakeholders	Status	Implementation details
Workforce 1. Develop workforce competency and familiarity of current software development techniques. To do so, military departments should acquire or access a small cadre of software systems architects with a deep understanding of iterative development. Service acquisition commands should use this cadre early in the acquisition process to formulate acquisition strategy, develop source selection criteria, and evaluate progress. 2. Develop a training curriculum to create and train this cadre and ensure the program managers of software-intensive programs are knowledgeable about software and with software acquisition training. 3. Direct Defense Acquisition University (DAU) to establish curricula addressing modern software practices. 4. Chief Executive Officers of DOD prime contractors should brief the USD(A&S) at least annually to demonstrate progress on adapting modern software practices, including corporations' proficiencies in establishing effective software factories. 5. Establish a special software acquisition workforce fund modeled after the Defense Acquisition Workforce Development Fund to hire and train a cadre of modern software acquisition experts across the military departments. 6. Program managers should create an iterative development integrated product team with associated training. **Key stakeholders** USD(A&S) USD(R&E) DAU Military departments	◐	According to Office of the USD(A&S) officials, planning for implementation of a software cadre is underway in response to a provision in the NDAA for Fiscal Year 2022.[g] DOD has not taken action to develop training curriculum for the software cadre. The Office of the USD(A&S) collaborated with DAU to develop training for leadership and software professionals. DAU has hired multiple Agile and DevSecOps professionals and developed training programs to educate DOD's acquisition workforce. DAU officials stated that they have also partnered with commercial providers to bring additional training opportunities to the workforce. The Office of the USD(A&S) also worked with DAU to develop and execute a training pilot for software acquisition personnel and those in related supporting disciplines to enhance familiarity and expertise in unique aspects of software. According to Office of the USD(A&S) officials, DAU also offers training courses specifically targeted at DOD senior leadership, such as a workshop for senior leadership on modern software methods and a course focusing on security in a DevSecOps environment. DOD has not required Chief Executive Officers of DOD prime contractors to regularly brief the USD(A&S) on progress on adapting modern software practices. DOD has not taken action to establish a special software acquisition workforce fund. The military departments have not directed program managers to create an iterative development integrated product team with associated training. More generally, however, the military departments have expanded or are planning to expand training opportunities on software intensive systems and practices. For example, the Air Force Institute of Technology provides DevSecOps courses for leadership, including program managers. Further, Army officials stated that, in partnership with the Air Force, they are piloting four learning paths in modern software practices, such as related to cloud computing and DevSecOps.

Recommendation and key stakeholders	Status	Implementation details
Software sustainment 1. Requests for proposals and selection criteria should specify basic elements of the software framework supporting the software factory, including code and document repositories, test infrastructure, software tools, check-in notes, code provenance, and reference and working documents informing development, test, and deployment. 2. Provide documentation, test files, coding, application programming interfaces, design documents, results of fault, performance tests conducted using the framework, and tools developed during the development, as well as the software factory framework. 3. Selection preference should be granted based on the ability of DOD to reconstitute the software framework and rebuild binaries, re-run tests, procedures, and tools against delivered software, and documentation. **Key stakeholder** USD(R&E)	◐	DOD has yet to take action directing requests for proposals and selection criteria to specify elements supporting the software factory as well as for DOD to give preference to contractors based on DOD's ability to reconstitute the software framework, among other things. According to DOD officials, DOD's *Enterprise DevSecOps Reference Design* includes some guidance to assess agency and vendor software factories, which can be used during the source selection process. DOD officials noted that it is not practical to implement a one-size-fits-all approach to source selection. DOD issued guidance for programs using the software acquisition pathway related to source code access. For example, DOD Instruction 5000.87 states that programs using the pathway are to develop intellectual property strategies that identify and describe delivery of license rights for all software and related materials to meet operational, cybersecurity, and supportability requirements. The strategy is to include delivery of materials necessary to operate, integrate, test, debug, and deploy software, including source code, scripts, and datasets. In addition, DOD established enterprise DevSecOps capabilities and services available to all acquisition programs using or planning to use DevSecOps, such as ensuring government access to required software development artifacts, including code, scripts, scanners, compilers, and tools. This is done by providing government owned and operated cloud development environments in which development and integrated can be performed. DOD has also identified additional planned steps to supplement action taken in this area. According to DOD's February 2022 Software Modernization Strategy, DOD must ensure appropriate data access and appropriate data rights to develop, maintain, and protect software. For example, the strategy states that DOD should partner with industry to create intellectual property strategies that better balance return on investment for DOD and the contractor. Additionally, 10 U.S.C. § 4576(a) requires DOD to consider, to the maximum extent practicable, that it ensure access to source code, among other software related materials, when the department negotiates the acquisition of noncommercial software.[h] As of January 2022, DOD was proposing to amend the Defense Federal Acquisition Regulation Supplement to require access to source code, among other materials, to implement these requirements. DOD has not taken action to require selection preferences based on the ability of DOD to reconstitute the software framework and rebuild binaries, re-run tests, procedures, and tools against delivered software, and documentation. Officials from the Office of the USD(A&S) told us they do not plan to direct programs to take a specific approach to source selection.

Recommendation and key stakeholders	Status	Implementation details
Independent verification and validation for machine learning 1. Establish research and experimentation programs around the practical use of machine learning in defense systems with efficient testing, independent verification and validation, and cybersecurity resiliency and hardening as the primary focus points. 2. Establish a machine learning and autonomy data repository and exchange along the lines of the U.S. Computer Emergency Readiness Team to collect and share necessary data from and for the deployment of machine learning and autonomy. 3. Create and promulgate a methodology and best practices for the construction, validation, and deployment of machine learning systems, including architectures and test harnesses. **Key stakeholders** USD(R&E) Defense Advanced Research Projects Agency Software Engineering Institute	◐	DOD has taken steps to establish research and experimentation programs around the use of machine learning in defense systems. For example, March 2021, DOD established the Joint Common Foundation, a cloud-enabled platform that leverages DevSecOps practices and allows DOD customers to develop, test, integrate, and prototype artificial intelligence and machine learning software. This includes sharing and reusing data, software, and tools. DOD has also taken steps to establish a machine learning and autonomy data repository and exchange. For example, the Joint Common Foundation also includes information and source code management repositories that allow users to view information on the platform and access and migrate source code into a centralized repository. DOD plans additional future efforts in these areas. In February 2022, DOD established the Chief Digital and Artificial Intelligence Office (CDAO). CDAO aims to accelerate DOD’s adoption of data, analytics, and artificial intelligence across the department. CDAO integrated the Joint Artificial Intelligence Center, Defense Digital Services, the Chief Data Officer, and Advana, DOD’s enterprise data platform. Among other things, CDAO is tasked with leading DOD’s data, analytics, and artificial intelligence-related strategy and policy; enabling the development of digital and artificial intelligence-enabled solutions across DOD; and providing a cadre of experts to address challenges in these areas. Moving forward, CDAO aims to provide enterprise-level infrastructure and services that enable efforts to advance adoption of data, analytics, and artificial intelligence, to include an expanded and more accessible enterprise data repository and data catalogue with designated authoritative data sources, common data models for enterprise, and joint use cases. Further, in June 2022, DOD published the Responsible Artificial Intelligence Strategy and Implementation Pathway. This strategy defines a framework for DOD use of artificial intelligence and directs DOD’s strategic approach in areas, such as governance, acquisition, and workforce. For example, the strategy establishes a goal of building, training, and equipping an artificial intelligence workforce. DOD has yet to take action to promulgate a methodology and best practices for the construction, validation, and deployment of machine learning systems.

Legend: ◐ = partially implemented.

Source: GAO analysis of DSB report and DOD documents and interviews with DOD officials. | GAO-23-105611

Note: Based on our assessment of documentation and discussion with DOD officials, we assessed a recommendation as being partially implemented if DOD took actions that addressed some, but not most, aspects of the recommendation. We did not identify any recommendations that DOD had fully or substantially addressed nor any that DOD had not taken any steps to address.

[a] Software factories, which are equipped with a set of tools, process workflows, scripts, and environments, are used to deliver software by automating activities in the development, build, test, release, and deliver phases.

[b] The Software Engineering Institute is a DOD Federally Funded Research and Development Center that focuses on software engineering, cybersecurity, and artificial intelligence.

[c] According to DOD, Development, Security, and Operations (DevSecOps) is a software engineering culture and practice that aims at unifying software development, security, and operations. The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of software development.

[d] The minimum viable product is an early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on. Insights from minimum viable products help shape scope, requirements, and design.

[e] Sponsors are the individuals that hold the authority and advocate for needed user capabilities and associated resource commitments.

[f] Major defense acquisition programs are those identified by DOD or that have a dollar value for all increments estimated to require eventual total expenditure for research, development, test, and evaluation of more than $525 million, or for procurement of more than $3.065 billion, in fiscal year 2020 constant dollars. DOD Instruction 5000.85, Major Capability Acquisition (Aug. 6, 2020) (incorporating change 1, Nov. 4, 2021). See also 10 U.S.C. § 4201. The text of this statute was previously codified at title 10, section 2430(a)(1) of the U.S. Code until it was transferred on January 1, 2022.

[g] National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, § 836(a).

[h] 10 U.S.C. § 4576(a)(1).

Appendix III: Assessment of Department of Defense (DOD) Implementation of Defense Innovation Board (DIB) Software Modernization Recommendations

Table 6 shows the status of DOD's implementation of DIB's recommended actions, including key stakeholders.[1]

Table 6: Department of Defense (DOD) Implementation of Defense Innovation Board (DIB) Software Modernization Recommendations

Recommendation and key stakeholders	Status	Implementation details
New acquisition pathway Establish one or more new acquisition pathways for software that prioritize continuous integration and delivery of working software in a secure manner, with continuous oversight from automated analytics K**ey stakeholders** Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) Under Secretary of Defense (Comptroller) (USD(C)) Cost Assessment and Program Evaluation (CAPE) Director, Operation Test and Evaluation (DOT&E) Under Secretary of Defense for Research and Engineering (USD(R&E)) Office of the Chairman of the Joint Chiefs of Staff (Joint Staff) Military departments	●	In October 2020, DOD published DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*. The instruction establishes policy to facilitate rapid and iterative delivery of software capability to DOD. Pathway programs require software teams to use modern iterative software development methodologies, tools, and techniques, such as DevSecOps, which aims to, among other things, shift security to the beginning of the application life cycle.[a] In addition, pathway programs are to incorporate continuous automated testing and evaluation, resiliency, and cybersecurity. Each program following the pathway must develop and track a set of metrics—using automated tools to the maximum extent practicable—to assess and manage, among other things, the performance, progress, speed, and quality of the software development, and the ability to meet users' needs. As of March 2023, there were 49 programs participating in the software acquisition pathway.

[1] In May 2019, the DIB made 26 total software modernization recommendations to DOD. Sixteen of these recommendations (we refer to these as secondary recommendations) are for DOD to implement after action on the other 10 (we refer to these as primary recommendations) are solidly underway. Appendices III and IV detail the implementation status of each recommendation with steps taken and the steps remaining. In addition, for the purposes of this report, we focused on DIB's primary recommendations because DIB emphasized the urgency of implementing these recommendations. DSB did not make a similar distinction, so we included all DSB recommendations. For more information on DOD's efforts to address DIB's secondary recommendations, see appendix IV.

Recommendation and key stakeholders	Status	Implementation details
New appropriation category Create a new appropriation category for software capability delivery that allows software to be funded as a single budget item, with no separation between research, development, test and evaluation (RDT&E), production, and sustainment **Key stakeholders** USD(A&S) USD(C) CAPE Military departments	●	The Office of the USD(A&S), in collaboration with the Office of the USD(C), CAPE, and the military departments, proposed a framework—based on the DIB recommendation—for a pilot program. The Consolidated Appropriations Act, 2021 established the pilot and provides that DOD's appropriations for RDT&E in that Act may be used for expenses for agile RDT&E; procurement; and operations and maintenance for approved pilot programs. DOD's goal for the pilot program is to determine whether the use of a single appropriation category facilitates modern Agile practices.[b] As of August 2022, there were eight pilot programs. DOD plans to execute the pilots for several years and work with Congress to implement a long-term funding solution. According to DOD officials, Congress has not approved recent requests to include additional pilot programs, but DOD continues to collect data on the pilot programs to understand the impact on software development programs.
Security considerations Make security a first-order consideration for all software-intensive systems, recognizing that security-at-the-perimeter is not enough **Key stakeholders** USD(A&S) DOD Chief Information Officer (CIO) DOT&E Defense Digital Service Military departments	●	DOD established policies and guidance related to cybersecurity for programs within the software acquisition pathway. According to DOD Instruction 5000.87, pathway programs require software teams to use modern iterative software development methodologies and tools and techniques, such as DevSecOps, which aims to, among other things, shift security to the beginning of the application lifecycle. In addition, pathway programs are to incorporate continuous automated testing and evaluation, resiliency, and cybersecurity. For programs outside of the pathway, the DevSecOps Reference design encourages the transition from legacy software practices to modern software methods when appropriate. In addition, section 4 of DOD Instruction 8510.01, Risk Management Framework for DOD Systems, issued in July 2022, describes a department-wide approach to cybersecurity risk governance that applies to all systems. While DOD has made substantial progress developing cybersecurity policy and guidance, how programs implement this guidance moving forward will be critical to DOD's success in this area.

Recommendation and key stakeholders	Status	Implementation details
Software features Shift from the use of rigid lists of requirements for software programs to a list of desired features and required interfaces or characteristics to avoid requirements creep, overly ambitious requirements, and program delays **Key stakeholders** USD(A&S) Joint Staff Military departments	◐	DOD established policies and guidance related to capability requirements definition for programs within the software acquisition pathway. DOD Instruction 5000.87 defines capability needs and performance requirements for pathway programs. The instruction notes that programs within the pathway are not subject to DOD's Joint Capabilities Integration and Development System (JCIDS); rather, software development is to be done in collaboration with end users to ensure, among other things, that it is delivered to address user needs.[c] Under the pathway, programs are to capture high-level operational needs, including capabilities, features, and interoperability needs in requirements documents. According to Joint Staff officials , being less rigid with requirements will be a challenge for the organization. They noted, however, that they collaborated with the Office of the USD(A&S) to ensure that software acquisition programs have the flexibility to avoid over-specifying requirements. However, DOD policies and guidance relevant to this recommendation are largely targeted to programs using the software acquisition pathway and do not address software-intensive systems using other acquisition pathways. In June 2022, we reported that nearly all of DOD's costliest weapon programs, many of which are developing substantial amounts of software, are using pathways other than the software acquisition pathway.[d]
Digital infrastructure Establish and maintain digital infrastructure within DOD and the military services that enables rapid deployment of secure software to the field, and incentivize its use by contractors **Key stakeholders** USD(A&S) DOD CIO USD(C) Military departments	◐	As of August 2022, DOD has established 29 software factories across the department, such as the Department of the Air Force's Platform One and Kessel Run, the Navy's Forge, and the Army's Software Factory.[e] DOD has also published guidance for enabling cloud DevSecOps software factories. For example, in July 2021, DOD published its Cloud Native Access Point Reference Design, which established guidance for the Cloud Native Access Point (CNAP). CNAP provides secure authorized access to DOD resources in a commercial cloud environment by DOD users. According to Office of the USD(A&S) officials, each of DOD's military services have established cloud environments, such as the Army's Cloud Account Management Optimization, Navy's Commercial Cloud Services, and Air Force's Cloud One. However, additional work remains for DOD to establish and maintain digital infrastructure, as outlined in DOD's key strategy documents. For example, while not yet achieved, DOD's February 2022 Software Modernization Strategy establishes a goal of accelerating the DOD enterprise cloud environment, transitioning from disparate cloud efforts to integrated cloud portfolio, and establishing a DOD-wide software factory ecosystem, leveraging established software factories and scaling the services across the department. Further, DOD's November 2021 Software Science and Technology Strategy states that work remains in refining contract incentives. In June 2022, we found that DOD had addressed 11 of 14 Office of Management and Budget requirements in its Federal Cloud Computing Strategy. We reported that addressing the remaining requirements will help DOD realize the benefits of cloud computing.[f]

Recommendation and key stakeholders	Status	Implementation details
Automated testing and evaluation Create, implement, support, and use fully automatable approaches to testing and evaluation, including security **Key stakeholders** DOT&E USD(A&S) Military departments	◐	DOD established policies and guidance related to automated testing and evaluation. For example, DOD Instruction 5000.87 states that software development will incorporate continuous automated testing and evaluation, resiliency, and cybersecurity by using automation to the maximum extent practicable. For programs using the software acquisition pathway, cybersecurity is expected to be addressed from program inception and throughout a program's lifecycle by continually assessing and measuring cybersecurity preparedness and responsiveness, identifying and addressing risks, and executing mitigation actions. Further, DOT&E published DOD Instruction 5000.89, *Test and Evaluation*, which establishes policy and procedures for test and evaluation across DOD's Adaptive Acquisition Framework. The instruction includes certain requirements related to automated testing. DOT&E officials also stated that DOT&E staff, in coordination with the Office of the USD(R&E), drafted a guidebook to accompany the instruction. The guidebook is expected to include guidance about the implementation, support, and use of fully automatable approaches to test and evaluation. However, additional work remains for DOD to implement, support, and use fully automated approaches to testing and evaluation. DOD policies and guidance relevant to this recommendation are largely targeted to programs using the software acquisition pathway, and have yet to address all software-intensive systems. For example, the procedures related to automated testing and evaluation described in DOD Instruction 5000.89 are targeted towards programs within the software acquisition pathway even though software-intensive systems may be developed using other pathways. Further, in May 2022, DOT&E officials said that DOT&E was in the process of standing up multi-disciplinary research teams to initiate the development of automatable approaches to test and evaluation.
Authorization to Operate (ATO) reciprocity[g] Create a mechanism for ATO reciprocity within and between programs, the military services, and other DOD agencies to enable sharing of software platforms, components, and infrastructure, and rapid integration of capabilities across platforms, systems, and the military services **Key stakeholders** DOD CIO USD(A&S) Defense Information Systems Agency Military departments	◐	In July 2022, DOD issued DOD Instruction 8510.01, Risk Management Framework for DOD Systems. Among other things, the instruction provides guidance on system authorization decision reciprocity for DOD, including sharing system to system connections across authorization boundaries and decisions for shared services within the department. In addition, in February 2022, DOD's Office of the Secretary of Defense (OSD) issued a memorandum to senior DOD leadership directing DOD CIO to coordinate and publish guidance on the necessary steps to allow systems to operate under a continuous ATO (cATO) state. However, additional work remains for DOD to establish ATO reciprocity across the department. For example, DOD has yet to publish guidance for cATO. According to Office of the USD(A&S) officials, employing cATO is a high priority, but it will take time to implement the policies, processes, and technical enablers for cATO. Officials noted that DOD's Software Modernization Senior Steering Group (SSG)—chartered to guide and facilitate the adoption of modern software practices across DOD—frequently discusses cATO implementation. Further, Office of the USD(A&S) officials said that enterprise resources are being evaluated within DOD CIO, the Office of the USD(R&E), and testing communities to speed responsive and robust tools to implement cATO across DOD.

Recommendation and key stakeholders	Status	Implementation details
Source code access Require access to source code, software frameworks, and development toolchains—with appropriate intellectual property rights—for DOD-specific code, enabling full security testing and rebuilding of binaries from source **Key stakeholders** USD(A&S) DOD CIO Military departments	◐	DOD issued guidance for programs using the software acquisition pathway related to source code access. For example, DOD Instruction 5000.87 states that pathway programs are to develop intellectual property strategies that identify and describe delivery of license rights for all software and related materials to meet operational, cybersecurity, and supportability requirements. The strategy is to include delivery of materials necessary to operate, integrate, test, debug, and deploy software, including source code, scripts, and datasets. However, DOD's policy to date on source code access does not address programs using pathways other than the software acquisition pathway. In addition, DOD has identified additional steps it needs to take in this area. According to DOD's February 2022 Software Modernization Strategy, DOD must ensure appropriate data access and appropriate data rights to develop, maintain, and protect software. For example, DOD should partner with industry to create intellectual property strategies that better balance return on investment for DOD and the contractor. Further, 10 U.S.C. § 4576(a) requires DOD to consider, to the maximum extent practicable, ensuring access to source code, among other software related materials, as the department negotiates the acquisition of noncommercial software.[h] As of January 2022, DOD was proposing to amend the Defense Federal Acquisition Regulation Supplement to implement these requirements.
Organic development groups Create software development units in each military service consisting of military and civilian personnel who develop and deploy software to the field using DevSecOps practices **Key stakeholders** USD(A&S) Under Secretary of Defense for Personnel and Readiness Military departments	◐	DOD established 29 software factories across the department—such as the Department of the Air Force's Platform One and Kessel Run, the Navy's Forge, and Army's Software Factory. Software factories include personnel across various specialized teams, including development and security teams, to develop and deploy software. However, these software factories do not address certain elements envisioned by DIB, such as a separate career track for software development and the use of commercial best practices for recruitment of talented personnel.

Recommendation and key stakeholders	Status	Implementation details
Acquisition workforce training Expand the use of training programs for leadership and program managers that provide insight into modern software development and the authorities available to enable rapid acquisition of software **Key stakeholders** USD(A&S) DOD CIO Military departments	●	The Office of the USD(A&S) collaborated with the Defense Acquisition University (DAU) to develop training for leadership and software professionals. According to an April 2020 DOD report to Congress, DAU has hired multiple Agile and DevSecOps professionals and developed training programs to educate DOD's acquisition workforce. DAU officials stated that they have also partnered with commercial providers to bring additional training opportunities to the workforce. The Office of the USD(A&S) also worked with DAU to develop and execute a training pilot for software acquisition personnel and those in related supporting disciplines to enhance familiarity and expertise in unique aspects of software. According to Office of the USD(A&S) officials, DAU also offers training courses specifically targeted at DOD senior leadership, such as a workshop for senior leadership on modern software methods and a course focusing on security in a DevSecOps environment. Further, in response to a provision in the National Defense Authorization Act for Fiscal Year 2020, DOD developed a strategy to address software training and management for software acquisition professionals and software developers, among others.[i]

Legend: ● = fully or substantially implemented; ◐ = partially implemented.

Source: GAO analysis of DIB report and DOD documents and interviews with DOD officials. | GAO-23-105611

Note: Based on our assessment of documentation and discussion with DOD officials, we assessed a recommendation as being fully or substantially implemented if DOD took actions that addressed most or all aspects of the recommendation. We assessed a recommendation as being partially implemented if DOD took actions that addressed some, but not most, aspects of the recommendation. We did not identify any recommendations that DOD had not taken any steps to address.

[a] According to DOD, DevSecOps is a software engineering culture and practice that aims at unifying software development, security, and operations. The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of software development.

[b] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 8131(a). Subsequent appropriations acts included substantively similar language, but new initiatives under the Software and Digital Technology Pilot program were not included. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, § 8119(b) (2022) and Consolidated Appropriations Act, 2023, Publ. L. No. 117-328, § 8107(b) (2022).

[c] DOD's Joint Staff uses the JCIDS process to manage the review and approval of capability requirements documents. The Joint Requirements Oversight Council oversees the process. The Joint Requirements Oversight Council is responsible for assessing joint military capabilities, and identifying, approving, and prioritizing gaps in such capabilities to meet requirements in the National Defense Strategy. In addition, the Joint Requirements Oversight Council establishes and approves joint performance requirements that, among other things, ensure interoperability between and among joint military capabilities and are necessary to fulfill capability gaps of more than one armed force or other DOD organization.

[d] GAO, *Weapon System Annual Assessment: Challenges to Fielding Capabilities Faster Persist*, GAO-22-105230 (Washington, D.C.: June 8, 2022).

[e] Software factories, which are equipped with a set of tools, process workflows, scripts, and environments, are used to deliver software by automating activities in the development, build, test, release, and deliver phases.

[f] GAO, *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization*, GAO-22-104070 (Washington, D.C.: June 29, 2022).

[g] The National Institute of Standards and Technology defines ATO as the official management decision given by a senior official or officials to authorize operation of an information system and to explicitly accept the risk to operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of

security and privacy controls. Continuous authorization, otherwise known as continuous authorization to operate, encompasses validating the quality and security of the software development platform, process, and platform team. It couples ATO with automation to produce real-time and continuous evidence, verifying the defensive posture of the platform and resulting software in real-time.

[h] 10 U.S.C. § 4576(a).

[i] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 862.

Appendix IV: Department of Defense (DOD) Implementation of Defense Innovation Board (DIB) Secondary Software Modernization Recommendations

The table below provides information about DOD's implementation of DIB's secondary recommended actions, including key stakeholders and examples of implementation reported by DOD.[1] DOD reported that it is in the process of implementing each of the recommendations. DOD officials provided examples—as of October 2022—of actions taken to date and planned future actions related to these recommendations (see table 7).

Table 7: Completed and Planned Department of Defense (DOD) Actions Related to the Implementation of Defense Innovation Board (DIB) Software Modernization Secondary Recommendations, as Reported by DOD

Recommendation and key stakeholders	Examples of related actions reported by DOD	Examples of future related actions reported by DOD
Metrics for cost assessment and performance estimates Require cost assessment and performance estimates for software programs (and software components of larger programs) of appropriate type be based on metrics that track speed and cycle time, security, code quality, and functionality **Key stakeholders** Cost Assessment and Program Evaluation (CAPE)	DOD established cross-government working groups to discuss and develop the use of software cost and performance metrics and updated its system for reporting software data to include metrics that support cost estimation and performance for Agile software development programs.	DOD plans to continue discussions with industry on appropriate software cost assessment and performance estimates, which may lead to further refinement of cost estimation and performance metrics for DOD's software data reporting system.
Simplify laws and policies Refactor and simplify Title 10, Defense Federal Acquisition Regulation Supplement, and DOD Instructions 5000.02, *Operation of the Defense Acquisition System* and 5000.75, *Business Systems Requirements and Acquisition* to remove statutory, regulatory, and procedural requirements that generate delays for acquisition, development, and fielding of software while adding requirements for continuous (automated) reporting of cost, performance (against updated metrics), and schedule **Key stakeholders** Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))	DOD reissued DOD Instruction 5000.02, *Operation of the Adaptive Acquisition Framework*, which describes six different acquisition pathways, including software acquisition and defense business systems pathways. The instruction allows program managers to tailor regulatory requirements based on program needs, such as developing and coordinating documentation not needed to manage the program. DOD also issued DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*, to be used by programs to rapidly and continuously develop and deliver software and tailor requirements and reporting.	DOD plans to continuously improve the software acquisition pathway and DOD processes going forward consistent with the department's Software Modernization Strategy.

[1] In May 2019, the DIB made 26 total software modernization recommendations to DOD. DIB described 10 of these recommendation as primary recommendations and stated that DOD should start implementing them first. It described the additional 16 recommendations (we refer to these as secondary recommendations) as recommendations that can provide further improvements for DOD to implement after action on the primary recommendations are solidly underway. See Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Washington, D.C.: May 3, 2019).

Recommendation and key stakeholders	Examples of related actions reported by DOD	Examples of future related actions reported by DOD
Streamlined processes for business systems Create streamlined authorization and appropriation processes for defense business systems that use commercially available products with minimal (source code) modification **Key stakeholders** USD(A&S)	DOD engaged Congress to establish a Software and Digital Technology Pilot program. The Consolidated Appropriations Act, 2021 provides that DOD's appropriations for research, development, test, and evaluation (RDT&E) in that act may be used for expenses for Agile RDT&E, procurement, and operations and maintenance for identified pilot programs.[a] The goal of the pilot program is to determine whether the use of a single appropriation category facilitates modern Agile practices. The pilot—which includes two defense business system programs—will help DOD to understand the effect of the use of a single appropriation category on software-intensive programs. DOD officials noted that the pilot program is demonstrating that a single appropriation category adds flexibility and speed in acquiring technologies. In January 2020, DOD reissued DOD Instruction 5000.75, *Business System Requirements and Acquisitions*, which states that when DOD acquires business systems it is to minimize the need for customizing commercial products to the maximum extent practicable.	DOD plans to continue to monitor actions related to the defense business system authorization and appropriation processes for potential adoption and implementation. For example, DOD plans to review the results of the ongoing Planning, Programming, Budgeting, and Execution commission to identify additional improvements to streamline these processes for defense business systems in the future.
Enduring capability Plan, budget, fund, and manage software development as an enduring capability that crosses program elements and funding categories, removing cost and schedule triggers associated with hardware-focused regulations and processes **Key stakeholders** CAPE	DOD engaged Congress to establish the Software and Digital Technology Pilot program, which allows use of certain RDT&E appropriations for procurement, and operations and maintenance activities for approved pilot programs, as mentioned above. The department is testing the use of a single appropriation category to understand its effect on software-intensive programs.[a] DOD officials noted that the pilot program is demonstrating that a single appropriation category adds flexibility and speed in acquiring technologies. DOD also established DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway*, to be used by programs to rapidly and continuously develop and deliver software. According to DOD officials, the software acquisition pathway can help eliminate cost and schedule breaches common with hardware acquisition programs.	DOD plans to continue efforts to expand the Software and Digital Technology Pilot program and refine the guidance on the software pathway. For example, according to officials, DOD has requested congressional approval for additional programs to provide further insight and inform the department of long-term solutions for funding software acquisitions.

Recommendation and key stakeholders	Examples of related actions reported by DOD	Examples of future related actions reported by DOD
Portfolio management Replace the Joint Capabilities Integration and Development System (JCIDS), Planning, Programming, Budgeting, and Execution, and Defense Federal Acquisition Regulation Supplement with a portfolio management approach to software programs, assign an office in each military department that uses direct identification of warfighter needs to determine allocation priorities for software capabilities **Key stakeholders** Office of the Chairman of the Joint Chiefs of Staff (Joint Staff) USD(A&S)	Joint Staff updated the JCIDS manual and the Chairman of the Joint Chiefs of Staff Instruction 5123.01H, *Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System*, to align with the software acquisition pathway.	DOD plans to continue efforts to evaluate processes, such as Planning, Programming, Budgeting, and Execution in support of the software acquisition pathway.
Prioritize modern software development methods Prioritize secure, iterative, collaborative development for selection and execution of new software development programs (and software components of hardware programs), especially those using commodity hardware and operating systems **Key stakeholders** DOD Chief Information Officer (CIO)	The Software Modernization Senior Steering Group incorporated modern software development principles in policy and guidance. As of March 2023, there were 49 programs using the software acquisition pathway.	
Cloud computing Remove obstacles to DOD usage of cloud computing on commercial platforms, including Defense Information Systems Agency cloud access point limits, lack of authorization to operate (ATO)[b] reciprocity, and access to modern software development tools **Key stakeholders** DOD CIO	In February 2022, DOD published a memorandum on continuous authorization to operate (cATO) to provide guidance on the steps necessary to allow systems to operate under a cATO state.[c] DOD completed the transition to the new Generation 3 Boundary Cloud Access Points that addressed bandwidth limitations of earlier access point reciprocity.	DOD plans to continue to find and implement ways to increase the speed of security accreditation and to make software tools more accessible. For example, DOD reported that the Enterprise Software Initiative team is continuing to make agreements with software tools for DOD organizations to buy licenses with better terms and conditions. Additionally, DOD's Software Modernization Strategy outlines future actions related to securing data in the cloud to improve authorization to operate processes. For example, the strategy states that ATO implements security controls within DOD's risk tolerance.

Recommendation and key stakeholders	Examples of related actions reported by DOD	Examples of future related actions reported by DOD
Certify code/toolchain Shift from certification of executables for low- and medium-risk deployments to certification of code/architectures and certification of the development, integration, and deployment toolchain **Key stakeholders** DOD CIO	The Federal Information Security Modernization Act and National Institute of Standards and Technology Risk Management Framework assessments are performed on entire systems, including people, processes, and technology, as well as code and architecture.[d] In February 2022, DOD published a memorandum on cATO. Among other things, the memorandum encourages Development, Security, and Operations (DevSecOps) adoption and changes the approach for performing Risk Management Framework assessments.	DOD plans to publish additional guidance to implement the goals of the February 2022 cATO memorandum.
Hardware as a consumable Plan and fund computing hardware (of all appropriate types) as consumable resources, with continuous refresh and upgrades to current, secure operating systems and platform components **Key stakeholders** USD(A&S) CAPE	According to DOD officials, DOD has implemented consumption-based solutions for decades, and contracting officials have the tools needed to be successful in procuring consumption-based solutions without needing large changes to DOD's current acquisition framework. In November 2019, Defense Acquisition University (DAU) published the *DOD Cloud Acquisition Guidebook*. Among other things, the guidebook is designed to provide information to DOD staff, including program managers and contracting officials, on DOD cloud acquisition and deployments.	DOD plans to continue to evaluate new guidance on hardware as a consumable, if appropriate. For example, the Office of the USD(A&S) has continued to provide additional guidance related to the software acquisition pathway to guide the uses of services in software development.
Increase program management office experience Increase the knowledge, expertise, and flexibility in program offices related to modern software development practices to improve the ability of program offices to take advantage of software-centric approaches to acquisition **Key stakeholders** DAU	DAU has delivered training on modern software practices for Agile DevSecOps culture and implementation. DAU training includes courses related to Agile, cloud, and modern software development transformation and contracting.	DAU is developing a series of multi-course credentials on DevSecOps, among others. The credential content will combine commercial and DAU training.

Recommendation and key stakeholders	Examples of related actions reported by DOD	Examples of future related actions reported by DOD
Recruiting transient digital talent Restructure the approach to recruiting digital talent to assume that the average tenure of a talented engineer will be 2 to 4 years, and make better use of highly qualified experts, Intergovernmental Personnel Act employees, special hiring authorities, reservists, and enlisted personnel to provide organic software development capability, while at the same time incentivizing and rewarding internal talent **Key stakeholders** Under Secretary of Defense for Research and Engineering (USD(R&E)) USD(A&S)	A select number of DOD program offices and organizations have used special hiring authorities, such as those related to attracting highly qualified experts and those provided by the Intergovernmental Personnel Act, among others, to support the recruitment of digital talent.[e,f] Military departments are also implementing programs to train and use active duty personnel, including both officers and enlisted personnel, for software development.	DOD plans to continue to emphasize and investigate ways to increase the use of available hiring authorities, such as leveraging authorities available to different workforces, by working across DOD organizations and the military departments. DOD is also working to expand the DOD Cyber Workforce Framework to include software engineering, artificial intelligence, and machine learning work roles. DOD officials noted that these expansion efforts will help hiring managers conduct an analysis of DOD's workforce composition.
Continuous metrics Create and use automatically generated, continuously available metrics that emphasize speed, cycle time, security, user value, and code quality to assess, manage, and terminate software programs (and software components of hardware programs) **Key stakeholders** USD(A&S)	According to DOD, software acquisition pathway programs and Agile software pilot programs are developing software using modern Agile software practices and leveraging tools that automatically generate near-real time metrics.	DOD plans to continue to refine data collection and encourage decision authorities to leverage more real-time metrics to oversee and manage software programs.
Iterative development Shift the approach for acquisition and development of software (and software-intensive components of larger programs) to an iterative approach: start small, be iterative, and build on success or be terminated quickly **Key stakeholders** USD(A&S)	DOD established the software acquisition pathway and has provided guidance, briefings, and one-on-one support, among other resources, to projects planning to adopt the software acquisition pathway. The Office of the USD(A&S) engages with other DOD stakeholders to update policies and practices to address iterative approaches in testing and evaluation, cost estimation, and requirements development.	DOD plans to iteratively update guidance supporting the software acquisition pathway to incorporate lessons learned.

Recommendation and key stakeholders	Examples of related actions reported by DOD	Examples of future related actions reported by DOD
Software research portfolio Maintain an active research portfolio into next-generation software methodologies and tools, including the integration of machine learning and artificial intelligence into software development, cost estimation, security vulnerabilities, and related areas **Key stakeholders** USD(R&E) DOD CIO	The Software Engineering Institute—a DOD Federally Funded Research and Development Center dedicated to software—maintains an active research portfolio into engineering for artificial intelligence systems and machine learning for software engineering.[g] In addition, the institute recently stood up a new artificial intelligence-focused division and led a software engineering community study into trends and future actions. In November 2021, the Offices of the USD(R&E), USD(A&S) and DOD CIO, in partnership with the military departments, published the Software Science and Technology Strategy. The strategy outlines DOD's future plans for next generation software technology to build up artificial intelligence, machine learning, software and technology digital capabilities, and the software workforce.	The Software Modernization Senior Steering Group, which oversees the implementation of the Software Modernization Strategy, will monitor the long-term research initiatives related to these areas and other efforts for years to come.
Transition emerging tools and methods Invest in transition of emerging tools and methods from academia and industry for creating, analyzing, verifying, and testing of software into DOD practice (via pilots, field tests, and other mechanisms) **Key stakeholders** USD(R&E) Director, Operational Test and Evaluation (DOT&E) DOD CIO	DOD has invested in software factories over the last several years to provide a mechanism for creating, analyzing, verifying, and testing software. DOT&E's Software Science and Technology Strategic Plan, which is currently being implemented, and DOD's Software Science and Technology Strategy are expected to increase work in areas related to investments in emerging tools and other technologies, and better tie the work to strategic priorities at the department.	
Collect data Automatically collect all data from DOD national security systems, networks, and sensor systems, and make the data available for machine learning (via federated, secured enclaves, not a centralized repository) **Key stakeholders** Chief Digital and Artificial Intelligence Office (CDAO) Joint Staff	DOD's September 2020 Data Strategy states that the department is adopting new technologies as part of its Digital Modernization program, including automation, artificial intelligence. DOD established CDAO to lead implementation of activities related to data analytics, artificial intelligence, and machine learning across the department. CDAO integrated the Joint Artificial Intelligence Center, Defense Digital Services, the Chief Data Officer, and Advana, DOD's enterprise data platform.	

Source: GAO analysis of DIB report and DOD information. | GAO-23-105611

Note: As part of the National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, § 1004(a) (g) (2021), Congress established the Commission on Planning, Programming, Budgeting, and Execution Reform to study the Planning, Programming, Budgeting, and Execution process, and to report and make recommendations for improving the process in 2023.

[a] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 8131(a). Subsequent appropriations acts included substantively similar language, but new initiatives under The Software and Digital Technology Pilot program were not included. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, § 8119(b) (2022) and Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 8107(b) (2022).

[b] The National Institute of Standards and Technology defines ATO as the official management decision given by a senior official or officials to authorize operation of an information system and to explicitly accept the risk to operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.

[c] Continuous authorization, otherwise known as cATO, encompasses validating the quality and security of the software development platform, process, and platform team. It couples ATO with automation to produce real-time and continuous evidence, verifying the defensive posture of the platform and resulting software in real-time.

[d] Pub. L. 113-283, § 3553(b)(6) (2014).

[e] 5 U.S.C. § 9903(a).

[f] 5 U.S.C. §§ 3371-3375.

[g] The Software Engineering Institute is a DOD Federally Funded Research and Development Center that focuses on software engineering, cybersecurity, and artificial intelligence.

Appendix V: Selected Practices Associated with Successful Reforms

Our prior work—including reports on leading practices on organizational mergers and transformations, collaboration, government streamlining and efficiency—shows that following certain change management practices helps to improve the likelihood of successful reforms.[1] Table 8 summarizes selected practices highlighted by our past work and selected key questions associated with each practice.

Table 8: Selected Change Management Practices from Past GAO Work Associated with Successful Agency Reforms

Selected change management practice	Selected key questions associated with the practice
Category for key questions: Goals and outcomes	
Establishing goals and outcomes	• To what extent has the agency established clear outcome-oriented goals and performance measures for the proposed reforms? • To what extent has the agency shown that the proposed reforms align with the agency's mission and strategic plan?
Category for key questions: Process for developing reforms	
Involving employees and key stakeholders	• How and to what extent has the agency consulted with Congress and other key stakeholders to develop its proposed reforms? • How and to what extent has the agency engaged employees and employee unions in developing the reforms (e.g., through surveys, focus groups) to gain their ownership for the proposed changes? • How and to what extent has the agency involved other stakeholders, as well as its customers and other agencies serving similar customers or supporting similar goals, in the development of the proposed reforms to ensure the reflection of their views? • Is there a two-way continuing communications strategy that listens and responds to concerns of employees regarding the effects of potential reforms?
Category for key questions: Implementing the reforms	
Leadership focus and attention	• Has the agency established a dedicated implementation team that has the capacity, including staffing, resources, and change management, to manage the reform process? • Has the agency designated a leader or leaders to be responsible for the implementation of the proposed reforms? • How will the agency hold the leader or leaders accountable for successful implementation of the reforms?
Managing and monitoring	• Has the agency developed an implementation plan with key milestones and deliverables to track implementation progress? • Has the agency put processes in place to collect the needed data and evidence that will effectively measure the reforms' outcome-oriented goals?
Category for key questions: Strategically managing the federal workforce	
Employee engagement	• How does the agency plan to sustain and strengthen employee engagement during and after the reforms?

[1] GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018). A list of related GAO work is included in appendix I of GAO-18-427.

Selected change management practice	Selected key questions associated with the practice
Strategic workforce planning	• To what extent has the agency conducted strategic workforce planning to determine whether it will have the needed resources and capacity, including the skills and competencies, in place for the proposed reforms or reorganization? • What employment- and mission-related data has the agency identified to monitor progress of reform efforts and to ensure no adverse effect on agency mission, and how is it using that data? • To what extent have the reforms included important practices for effective recruitment and hiring such as customized strategies to recruit highly specialized and hard-to-fill positions?

Source: GAO-18-427. | GAO-23-105611

Note: GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018).

Appendix VI: Key Attributes of Successful Performance Measures

Measuring performance allows organizations to track the progress they are making toward their goals. All attributes are not equal, and failure to have a particular attribute does not necessarily indicate that there is a weakness in that area or that the measure is not useful; rather, it may indicate an opportunity for further refinement. Table 9 summarizes nine key attributes of successful performance measures we have previously identified and the adverse consequences that may occur if they are missing.[1]

Table 9: Nine Key Attributes of Successful Performance Measures

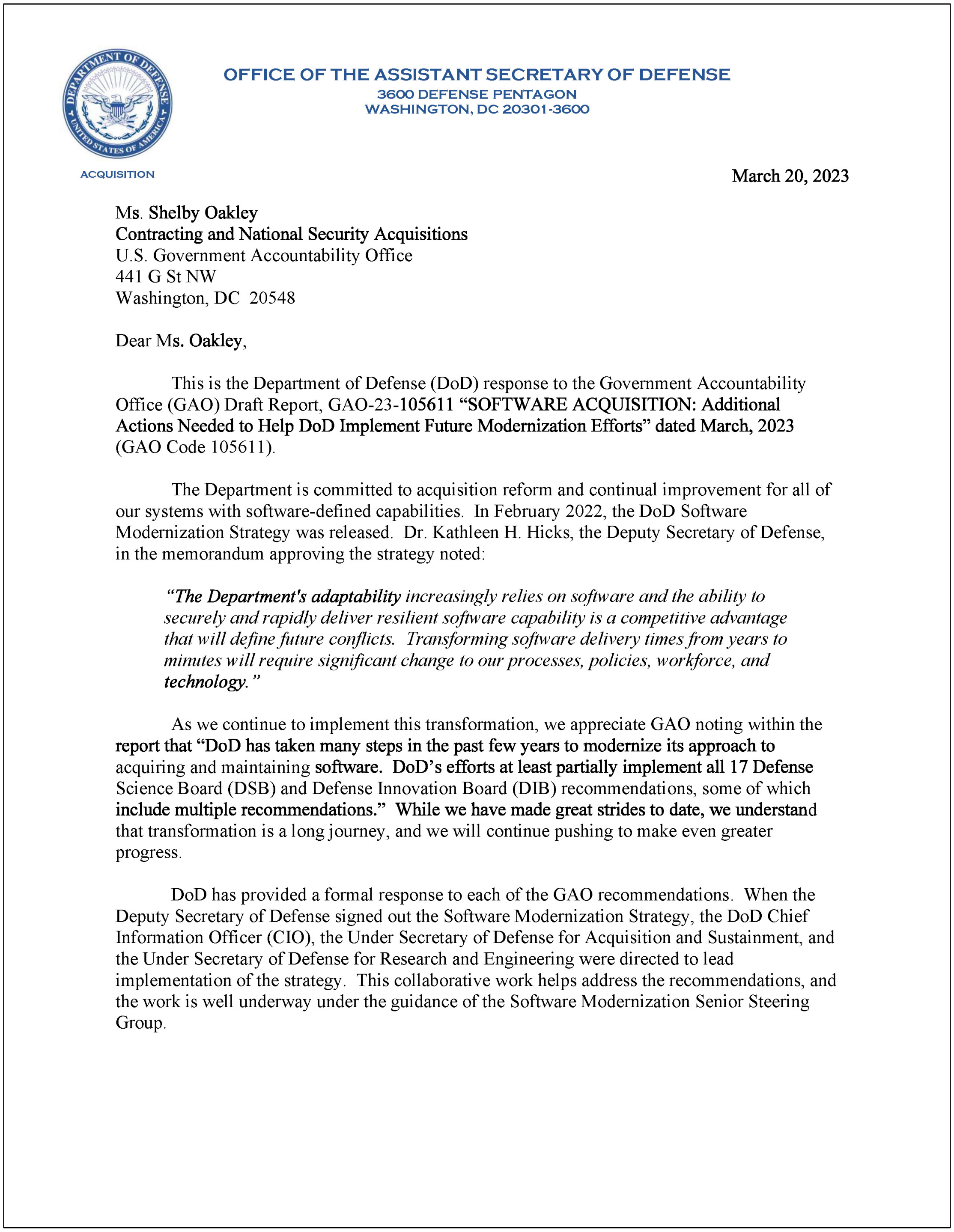
Attribute	Definition	Potentially adverse consequences of not meeting attribute
Linkage	Measure is aligned with division and agency-wide goals and mission and clearly communicated throughout the organization	Behaviors and incentives created by measures do not support achieving division or agency-wide goals or mission
Clarity	Measure is clearly stated and the name and definition are consistent with the methodology used to calculate it	Data could be confusing and misleading to others
Measurable target	Measure has a numerical goal	Cannot tell whether the performance is meeting expectations
Objectivity	Measure is reasonably free from significant bias or manipulation	Performance assessments may be systematically over- or understated
Reliability	Measure produces the same result under similar conditions	Reported performance data is inconsistent and adds uncertainty
Core program activities	Measures cover the activities that an entity is expected to perform to support the intent of the program	Not enough information available in core program areas to managers and stakeholders
Limited overlap	Measure should provide new information beyond that provided by other measures	Managers may have to sort through redundant, costly information that does not add value
Balance	Balance exists when a suite of measures ensures that an organization's various priorities are covered	Lack of balance could create skewed incentives when measures over-emphasize some goals
Government-wide priorities	Each measure should cover a priority such as quality, timeliness, and cost of service	A program's overall success is at risk if all priorities are not addressed

Source: GAO. | GAO-23-105611

Note: The information in this table was drawn from GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, GAO-03-143 (Washington, D.C.: Nov. 22, 2002).

[1] For more information on these attributes, see GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures,* GAO-03-143 (Washington, D.C.: Nov. 22, 2002).

Appendix VII: Comments from the Department of Defense



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

ACQUISITION

March 20, 2023

Ms. Shelby Oakley
Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G St NW
Washington, DC 20548

Dear Ms. Oakley,

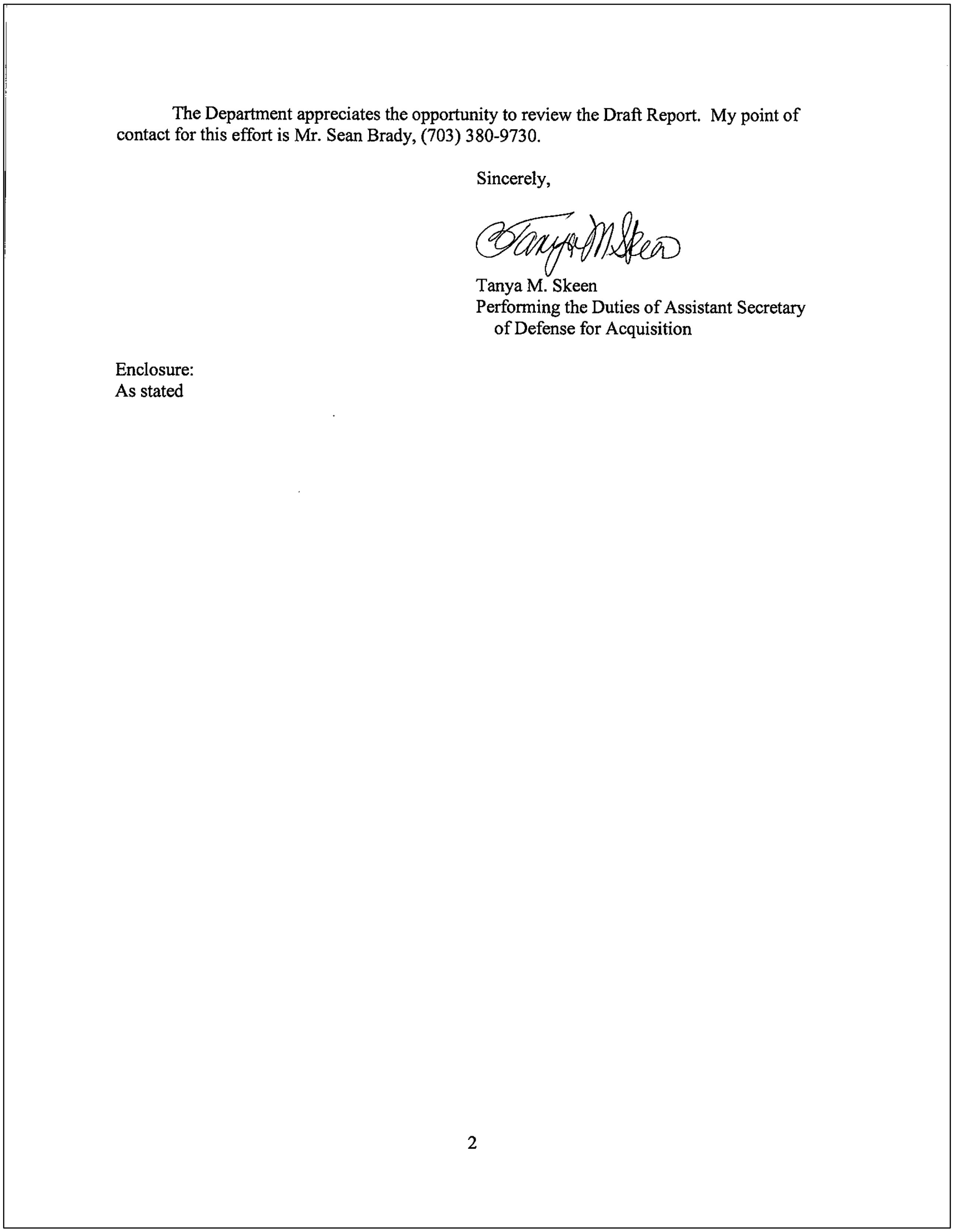
This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-23-105611 "SOFTWARE ACQUISITION: Additional Actions Needed to Help DoD Implement Future Modernization Efforts" dated March, 2023 (GAO Code 105611).

The Department is committed to acquisition reform and continual improvement for all of our systems with software-defined capabilities. 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 GAO noting within the report that "DoD has taken many steps in the past few years to modernize its approach to acquiring and maintaining software. DoD's efforts at least partially implement all 17 Defense Science Board (DSB) and Defense Innovation Board (DIB) recommendations, some of which include multiple recommendations." While we have made great strides to date, we understand that transformation is a long journey, and we will continue pushing to make even greater progress.

DoD has provided a formal response to each of the GAO recommendations. When the Deputy Secretary of Defense signed out the Software Modernization Strategy, the DoD Chief Information Officer (CIO), the Under Secretary of Defense for Acquisition and Sustainment, and the Under Secretary of Defense for Research and Engineering were directed to lead implementation of the strategy. This collaborative work helps address the recommendations, and the work is well underway under the guidance of the Software Modernization Senior Steering Group.



The Department appreciates the opportunity to review the Draft Report. My point of contact for this effort is Mr. Sean Brady, (703) 380-9730.

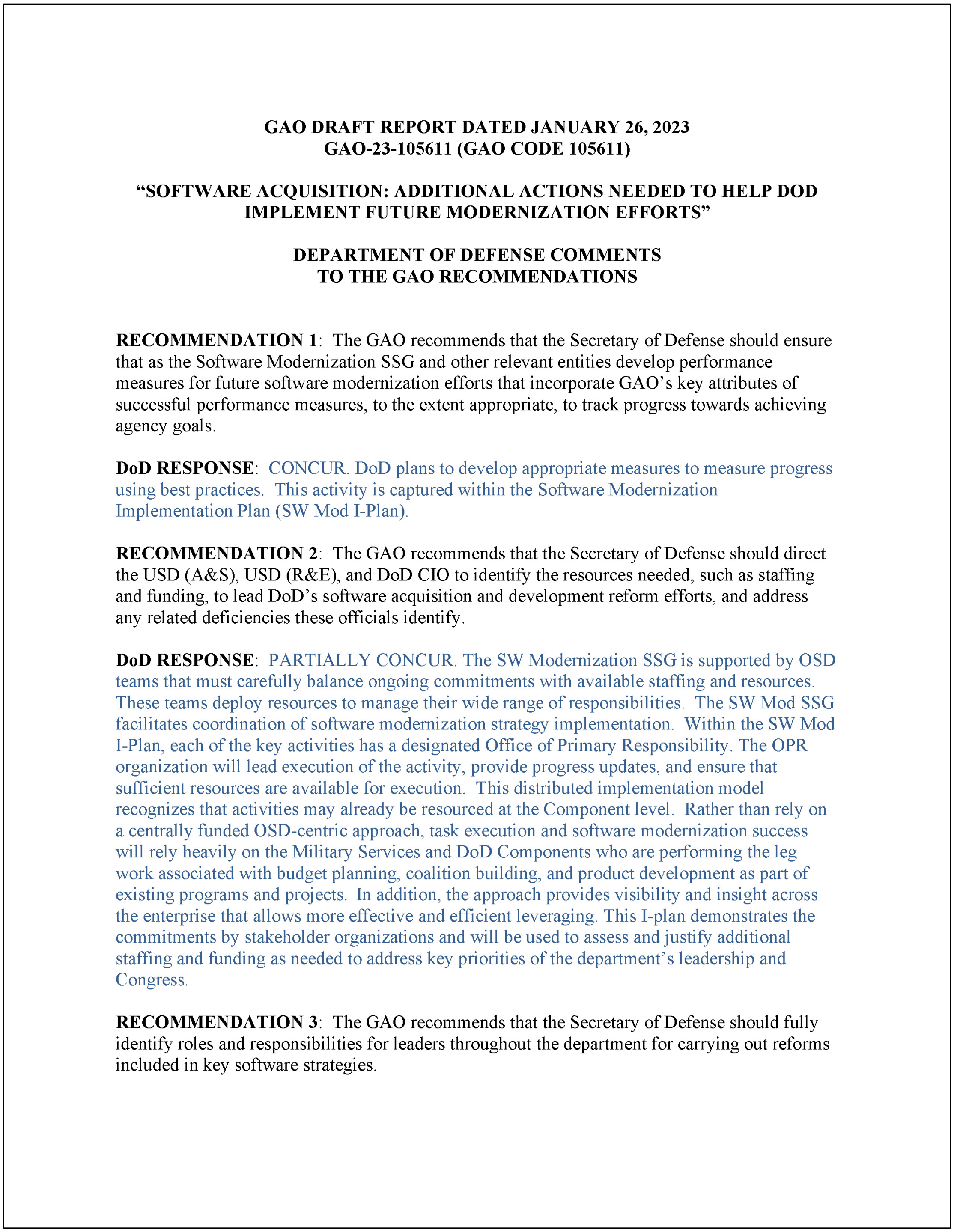
Sincerely,

Tanya M Skeen

Tanya M. Skeen
Performing the Duties of Assistant Secretary
of Defense for Acquisition

Enclosure:
As stated

2



GAO DRAFT REPORT DATED JANUARY 26, 2023
GAO-23-105611 (GAO CODE 105611)

"SOFTWARE ACQUISITION: ADDITIONAL ACTIONS NEEDED TO HELP DOD IMPLEMENT FUTURE MODERNIZATION EFFORTS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

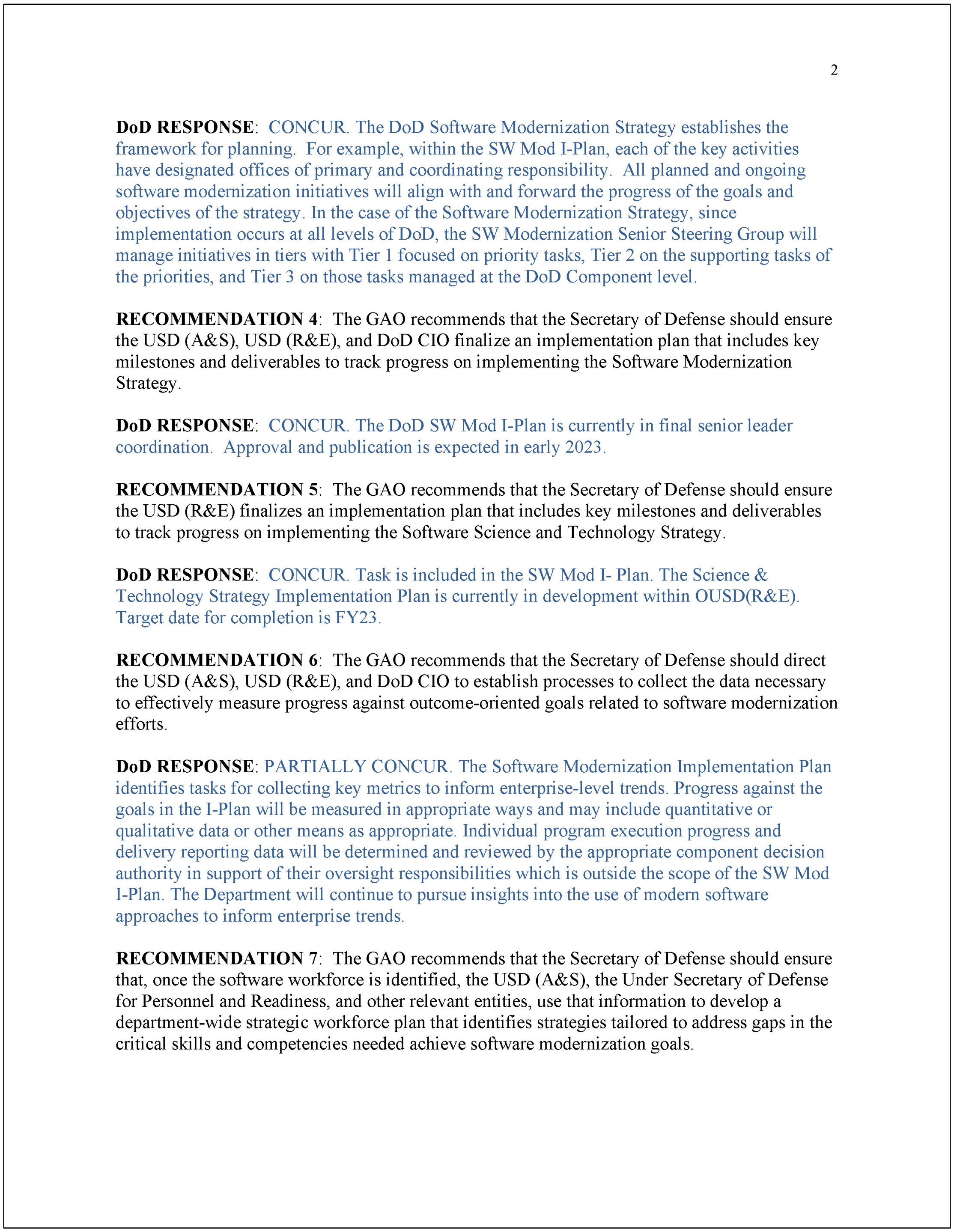
RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that as the Software Modernization SSG and other relevant entities develop performance measures for future software modernization efforts that incorporate GAO's key attributes of successful performance measures, to the extent appropriate, to track progress towards achieving agency goals.

DoD RESPONSE: CONCUR. DoD plans to develop appropriate measures to measure progress using best practices. This activity is captured within the Software Modernization Implementation Plan (SW Mod I-Plan).

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should direct the USD (A&S), USD (R&E), and DoD CIO to identify the resources needed, such as staffing and funding, to lead DoD's software acquisition and development reform efforts, and address any related deficiencies these officials identify.

DoD RESPONSE: PARTIALLY CONCUR. The SW Modernization SSG is supported by OSD teams that must carefully balance ongoing commitments with available staffing and resources. These teams deploy resources to manage their wide range of responsibilities. The SW Mod SSG facilitates coordination of software modernization strategy implementation. Within the SW Mod I-Plan, each of the key activities has a designated Office of Primary Responsibility. The OPR organization will lead execution of the activity, provide progress updates, and ensure that sufficient resources are available for execution. This distributed implementation model recognizes that activities may already be resourced at the Component level. Rather than rely on a centrally funded OSD-centric approach, task execution and software modernization success will rely heavily on the Military Services and DoD Components who are performing the leg work associated with budget planning, coalition building, and product development as part of existing programs and projects. In addition, the approach provides visibility and insight across the enterprise that allows more effective and efficient leveraging. This I-plan demonstrates the commitments by stakeholder organizations and will be used to assess and justify additional staffing and funding as needed to address key priorities of the department's leadership and Congress.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should fully identify roles and responsibilities for leaders throughout the department for carrying out reforms included in key software strategies.



DoD RESPONSE: CONCUR. The DoD Software Modernization Strategy establishes the framework for planning. For example, within the SW Mod I-Plan, each of the key activities have designated offices of primary and coordinating responsibility. All planned and ongoing software modernization initiatives will align with and forward the progress of the goals and objectives of the strategy. In the case of the Software Modernization Strategy, since implementation occurs at all levels of DoD, the SW Modernization Senior Steering Group will manage initiatives in tiers with Tier 1 focused on priority tasks, Tier 2 on the supporting tasks of the priorities, and Tier 3 on those tasks managed at the DoD Component level.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure the USD (A&S), USD (R&E), and DoD CIO finalize an implementation plan that includes key milestones and deliverables to track progress on implementing the Software Modernization Strategy.

DoD RESPONSE: CONCUR. The DoD SW Mod I-Plan is currently in final senior leader coordination. Approval and publication is expected in early 2023.

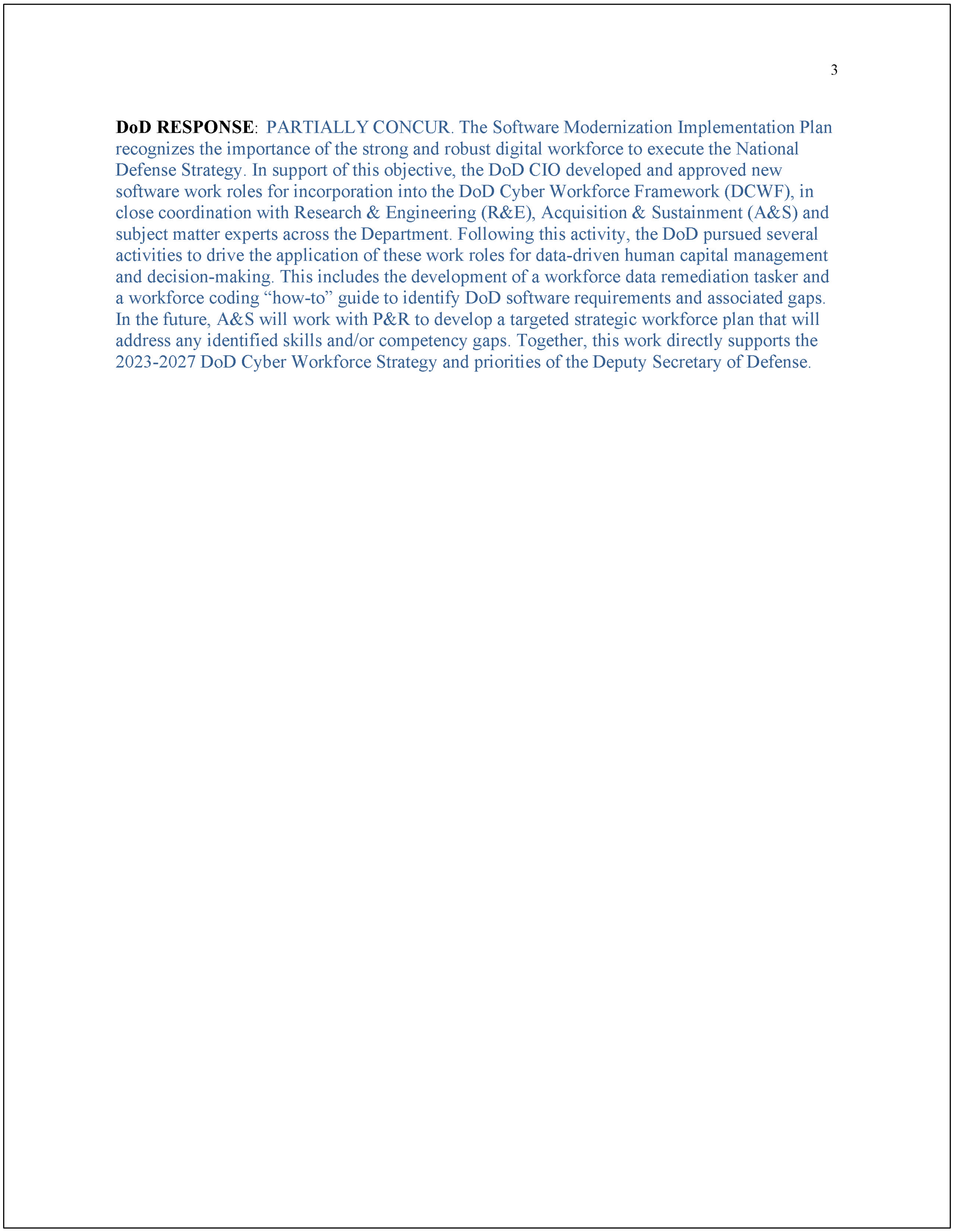
RECOMMENDATION 5: The GAO recommends that the Secretary of Defense should ensure the USD (R&E) finalizes an implementation plan that includes key milestones and deliverables to track progress on implementing the Software Science and Technology Strategy.

DoD RESPONSE: CONCUR. Task is included in the SW Mod I- Plan. The Science & Technology Strategy Implementation Plan is currently in development within OUSD(R&E). Target date for completion is FY23.

RECOMMENDATION 6: The GAO recommends that the Secretary of Defense should direct the USD (A&S), USD (R&E), and DoD CIO to establish processes to collect the data necessary to effectively measure progress against outcome-oriented goals related to software modernization efforts.

DoD RESPONSE: PARTIALLY CONCUR. The Software Modernization Implementation Plan identifies tasks for collecting key metrics to inform enterprise-level trends. Progress against the goals in the I-Plan will be measured in appropriate ways and may include quantitative or qualitative data or other means as appropriate. Individual program execution progress and delivery reporting data will be determined and reviewed by the appropriate component decision authority in support of their oversight responsibilities which is outside the scope of the SW Mod I-Plan. The Department will continue to pursue insights into the use of modern software approaches to inform enterprise trends.

RECOMMENDATION 7: The GAO recommends that the Secretary of Defense should ensure that, once the software workforce is identified, the USD (A&S), the Under Secretary of Defense for Personnel and Readiness, and other relevant entities, use that information to develop a department-wide strategic workforce plan that identifies strategies tailored to address gaps in the critical skills and competencies needed achieve software modernization goals.



DoD RESPONSE: PARTIALLY CONCUR. The Software Modernization Implementation Plan recognizes the importance of the strong and robust digital workforce to execute the National Defense Strategy. In support of this objective, the DoD CIO developed and approved new software work roles for incorporation into the DoD Cyber Workforce Framework (DCWF), in close coordination with Research & Engineering (R&E), Acquisition & Sustainment (A&S) and subject matter experts across the Department. Following this activity, the DoD pursued several activities to drive the application of these work roles for data-driven human capital management and decision-making. This includes the development of a workforce data remediation tasker and a workforce coding “how-to” guide to identify DoD software requirements and associated gaps. In the future, A&S will work with P&R to develop a targeted strategic workforce plan that will address any identified skills and/or competency gaps. Together, this work directly supports the 2023-2027 DoD Cyber Workforce Strategy and priorities of the Deputy Secretary of Defense.

Appendix VIII: GAO Contact and Staff Acknowledgments

GAO Contact

Shelby S. Oakley, (202) 512-4841 or oakleys@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff members made key contributions to this report: Anne McDonough (Assistant Director), Andrew Burton (Analyst-in-Charge), Tammy Beltran, Holland Freeman, Stephanie Gustafson, Cale Jones, Christine Pecora, and Adam Wolfe. Other contributions were made by Michael Holland, Gina Hoover, Sarah Veale, and Kevin Walsh.

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