United States Government Accountability Office

Report to Congressional Committees

June 2021

SOFTWARE DEVELOPMENT

DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices

GAO-21-351

GAO@100

Highlights

Highlights of GAO-21-351, a report to congressional committees

June 2021

SOFTWARE DEVELOPMENT

DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices

Why GAO Did This Study

For fiscal year 2021, DOD requested approximately $37.7 billion for IT investments. These investments included major business IT programs, which are intended to help the department carry out key business functions, such as financial management and health care.

The *National Defense Authorization Act for Fiscal Year 2019* included a provision for GAO to assess selected IT programs annually through March 2023. GAO's objectives for this review were to (1) summarize DOD's reported performance of its portfolio of IT acquisition programs and the reasons for this performance; (2) evaluate DOD's assessments of program risks; (3) summarize DOD's approaches to software development and cybersecurity and identify associated challenges; and (4) evaluate how selected organizational and policy changes could affect IT acquisitions.

To address these objectives, GAO selected 29 major business IT programs that DOD reported to the federal IT Dashboard (a public website that includes information on the performance of major IT investments) as of September 2020. GAO reviewed planned expenditures for these programs, from fiscal years 2019 through 2022, as reported in the department's FY 2021 budget request. It also aggregated program office responses to a GAO questionnaire that requested information about cost and schedule changes that occurred since January 2019 and the early impacts of COVID-19.

View GAO-21-351. For more information, contact Kevin Walsh at 202-512-6151 or walshk@gao.gov.

What GAO Found

According to the Department of Defense's (DOD) fiscal year (FY) 2021 budget request, DOD spent $2.8 billion on the 29 selected major business information technology (IT) programs in FY 2019. The department also reported that it planned to invest over $9.7 billion on these programs between FY 2020 and FY 2022. In addition, 20 of the 29 programs reported experiencing cost or schedule changes since January 2019. Program officials attributed cost and schedule changes to a variety of reasons, including modernization changes and requirements changes or delays. Seventeen of the 29 programs also reported experiencing challenges associated with the early impacts of the COVID-19 pandemic, including the slowdown of contractors' software development efforts.

DOD and GAO's assessments of program risk identified a range of program risk levels and indicated that some programs could be underreporting risks. Specifically, of the 22 programs that were actively using a register to manage program risks, DOD rated nine programs as low risk, 12 as medium risk, and one as high risk. In contrast, GAO rated seven as low risk, 12 as medium risk, and three as high risk. In total, GAO found 10 programs for which its numerical assessments of program risk reflected greater risk than reported by DOD, while DOD had three programs with greater reported risk than GAO. DOD officials noted that differences in risk levels might be associated with a variety of factors, including different risk assessment approaches. However, the differences in risk level GAO identified highlight the need for DOD to ensure that it is accurately reporting program risks. Until the department does so, oversight of some programs could be limited by overly optimistic risk perspectives.

As of December 2020, program officials for the 22 major DOD business IT programs that were actively developing software reported using approaches that may help to limit cost and schedule risks. (See table.)

Selected Software Development and Cybersecurity Approaches That May Limit Risks and Number of Major DOD Business IT Programs That Reported Using the Approach

Software development and cybersecurity approaches that may limit risk	Number of programs that reported using the approach
Using off-the-shelf software	19 of 22
Implementing continuous iterative software development	18 of 22
Delivering software at least every 6 months[a]	16 of 22
Developing or planning to develop a cybersecurity strategy	21 of 22
Conducting developmental cybersecurity testing	16 of 22
Conducting operational cybersecurity testing	15 of 22

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

[a]The Defense Innovation Board encourages more frequent delivery of working software to users for Agile and DevOps practices.

GAO also analyzed the risks of the 22 programs that were actively using central repositories known as risk registers to manage program risks. GAO used these registers to create program risk ratings, and then compared its ratings to those of the DOD chief information officer (CIO).

In addition, GAO aggregated DOD program office responses to the questionnaire that requested information about the software and cybersecurity practices used by 22 of the 29 IT programs that were actively developing software. GAO compared the responses to relevant guidance and leading practices.

GAO reviewed selected IT-related organizational and policy changes and reviewed reports and documentation related to the effects of these changes on IT acquisitions. GAO also aggregated program office responses to the questionnaire that requested information about DOD's implementation of these changes. This included information on DOD's implementation of best practices as part of its efforts to implement Agile software development. GAO met with relevant DOD officials to discuss each of the topics addressed in this report.

What GAO Recommends

GAO is making two recommendations to DOD related to revisiting the department's CIO risk ratings and improving data strategies and automated data collection efforts for the business system and software acquisition pathways necessary for stakeholders to monitor acquisitions and critical to the department's ability to assess acquisition performance.

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

Program officials also reported facing a variety of software development challenges while implementing these approaches. These included difficulties finding and hiring staff, transitioning from waterfall to Agile software development, and managing technical environments. DOD's continued efforts to address these challenges will be critical to the department's implementation of modern software development approaches.

DOD has also made organizational and policy changes intended to improve the management of its IT acquisitions, such as taking steps to implement Agile software development and improve data transparency. In addition, to address statutory requirements, DOD has taken steps to remove the department's chief management officer (CMO) position. However, the department had not yet sufficiently implemented these changes. Officials from many of the 18 programs GAO assessed that reported using Agile development reported that DOD had implemented activities associated with Agile transition best practices to only some or little to no extent, indicating that the department had not sufficiently implemented best practices. For example, 12 of the 18 programs reported that DOD's life-cycle activities only supported Agile methods to some or little to no extent. Program officials also reported challenges associated with implementing Agile software development. The department has a variety of efforts underway to help with its implementation of Agile software development. DOD officials stated that the department's transition to Agile will take years and will require sustained engagement throughout DOD.

In addition, DOD has taken steps aimed at improving the sharing and transparency of data it uses to monitor its acquisitions. According to a November 2020 proposal from the Office of the Under Secretary for Acquisition and Sustainment, DOD officials are to develop data strategies and metrics to assess performance for the department's acquisition pathways. However, as of February 2021, DOD did not have data strategies and had not finalized metrics for the two pathways associated with the programs discussed in this report. Officials said they were working with DOD programs and components to finalize initial pathway metrics. They stated that they plan to implement them in fiscal year 2021 and continue to refine and adjust them over the coming years. Without important data from acquistion pathways and systems, DOD risks not having timely quantitative insight into program performance, including its acquisition reform efforts.

Finally, DOD's CMO position was eliminated by a statute enacted in January 2021. This position was responsible for key efforts associated with the department's business systems modernization, which has been on GAO's High Risk List since 1995. DOD plans to take steps to address the uncertainty associated with the recent elimination of the position.

Contents

Figures

Abbreviations

AAF	adaptive acquisition framework
ATP	authority to proceed
CIO	chief information officer
CMO	chief management officer
COTS	commercial off-the-shelf
COVID-19	Coronavirus Disease 2019
DAU	Defense Acquisition University
DevOps	development and operations
DevSecOps	development, security, and operations
DHMSM	Department of Defense Healthcare Management System Modernization
DME	Development, Modernization, and Enhancement
DOD	Department of Defense
FY	fiscal year
IT	information technology
MAIS	major automated information system
Navy ERP	Navy Enterprise Resource Planning
NDAA	National Defense Authorization Act
O&M	Operations and Maintenance
OCIO	Office of the Chief Information Officer
OCMO	Office of the Chief Management Officer
OMB	Office of Management and Budget
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment

441 G St. N.W.
Washington, DC 20548

June 23, 2021

Congressional Committees

The Department of Defense (DOD) is one of the largest and most complex organizations in the world. To meet its mission to protect the security of our nation and deter war, DOD relies heavily on the use of information technology (IT). For fiscal year (FY) 2021, the department requested approximately $37.7 billion for its unclassified IT investments.[1]

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

The *John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019* included a provision for GAO to conduct annual assessments of selected DOD IT programs through March 2023.[2] This report presents the results of our second annual assessment. Our specific objectives for this assessment were to: (1) summarize DOD's reported performance of its portfolio of IT acquisition programs and the reasons for this performance; (2) evaluate DOD's assessments of program risks; (3) summarize DOD's approaches to software development and

[1]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year 2021 Budget Estimates* (February 2020). This figure is not a complete accounting of DOD's IT systems. For example, classified systems are not included. In addition, not all DOD IT expenditures are reported separately from their respective programs if those programs are developing more than software and hardware to support the software. For example, our annual assessments of DOD's weapons programs include programs that do not report software expenditures separately. See GAO, *Weapon Systems Annual Assessment: Updated Program Oversight Approach Needed*, GAO-21-222 (Washington, D.C., June 8, 2021).

[2]Pub. L. No 115-232,§ 833, 132 Stat. 1636, 1858 (Aug. 13, 2018). Under this provision, we are to report on these assessments no later than March 30 of each year from 2020 through 2023. Our assessment of the performance of DOD's weapon programs is included in a separate report, which we also prepared in response to section 833 of the NDAA for FY 2019. See GAO-21-222.

cybersecurity and identify associated challenges; and (4) evaluate how selected organizational and policy changes may affect IT acquisitions.

To address the first objective, we initially considered the 31 major business IT programs that DOD had reported to the federal IT Dashboard[3] as of September 2020. We then excluded two of these programs: one program that the department did not consider to be a business IT program and one program that it planned to retire in FY 2021. We selected the remaining 29 programs for our review. These included programs that support key areas such as personnel, financial management, health care, and logistics.

We examined how much money the department reported spending on the selected programs in fiscal year 2019 and planned to spend on these programs from fiscal years 2020 through 2022 by reviewing DOD's fiscal year 2021 budget request documentation.[4] Based on this documentation, we calculated the total actual and planned expenditures for the programs for the 4-year period. We included in the calculation the amounts associated with planned Development, Modernization, and Enhancement (DME) spending and Operations and Maintenance (O&M) spending for each program and for the portfolio of IT acquisition programs as a whole.

We also collected and analyzed key documents, reports, and artifacts pertaining to each program's life-cycle cost and schedule estimates. In addition, we aggregated program office responses to a GAO questionnaire that we developed and administered to all 29 programs in October 2020. Programs provided their responses between October 2020 and December 2020. The questionnaire sought information about program costs and schedule changes that had occurred since January 2019 and about the early impacts of the Coronavirus Disease 2019 (COVID-19) pandemic.

To assess the reliability of the budget data that DOD reported in the department's IT budget request database for the 29 selected programs, we compared the data to planned cost information provided by the

[3]The federal IT Dashboard is a public website managed by the Office of Management and Budget that includes information on the performance of major IT investments.

[4]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year 2021 President's Budget Request* (February 2020).

programs to identify any obvious inconsistencies.[5] In addition, we prepared and sent draft program summaries to the 15 (of the 29) programs with the largest planned expenditures and asked program staff to review the summaries and confirm their accuracy. We also corroborated program office responses to our questionnaire with relevant program documentation and interviews with program office officials. We determined that the data were sufficiently reliable for our reporting purposes.

To help ensure the reliability of the data collected via our questionnaire, including questions associated with subsequent objectives, we took steps to reduce measurement error and non-response error. Specifically, we conducted four pretests of the questionnaire with three programs to ensure that the questions were clear, unbiased, and consistently interpreted.[6] The pretests allowed us to obtain initial program feedback and helped ensure that officials within each program understood each question. The questionnaire allowed respondents to submit their answers electronically. We determined that the data were reliable for the purposes of this report.

For the second objective, we obtained program risk management plans and risk registers from 22 of the 29 selected programs.[7] We also collected from the federal IT Dashboard, information about DOD chief information officer (CIO) risk ratings for the 29 programs, as of December 2020.[8] We then analyzed the program risk registers to develop risk

[5]The Select and Native Programming-IT system is a database application used to collect and assemble information required in support of the IT budget request submitted to Congress. For example, it is used to generate DOD's IT-1 Report. DOD also uses the system to report its IT budget data on the IT Dashboard.

[6]We conducted two pretests with the same program.

[7]The remaining seven programs lacked a risk register, were not tracking active risks, or did not provide likelihood and consequence scores with reported risk items. This is in accord with DOD's risk-management guidance, which does not require programs to maintain a risk register.

[8]As of December 2020, DOD CIO risk ratings were last updated on the federal IT Dashboard in April 2020. As of February 2021, programs had not reported updated risk ratings to the Dashboard. An official from the DOD OCIO stated that the office completed updated ratings in November 2020, but those had not yet been made public on the federal IT Dashboard. This official stated that the delay is due to the budget submission process being underway and the change in presidential administrations.

ratings for the acquisitions and compared those ratings to the DOD CIO risk ratings.

Specifically, using information contained in the risk registers that we obtained from the 22 programs between October and December 2020, we combined the probability and impact of every active risk, as identified in the risk registers of each of the selected programs, to calculate what is known as the exposure of each risk.[9]

Exposure scores, which were based on industry and government leading practices, as well as DOD's own guidance for managing risks, ranged from "very low" to "very high."[10] Specifically, for each of the risk exposure scores, we assigned a 1 (very high risk) to 5 (very low risk) rating. We then averaged the numerical risk ratings to obtain an overall risk rating (or assessment) for the acquisition as a whole, which ranged from 1 (very high risk) to 5 (very low risk). This 1-5 rating scale is consistent with the scale that federal CIOs use for reporting program risk to the federal IT Dashboard.

Table 1 shows how our overall program risk ratings corresponded to risk exposure ratings. Appendix I includes additional information about how we calculated the program risk ratings.

Table 1: Numerical Risk Ratings and Corresponding Risk Exposure Ratings

Numerical risk rating	Risk exposure rating
1	Very high
2	High
3	Medium
4	Low
5	Very low

Source: GAO analysis. | GAO 21-351

[9]According to the Software Engineering Institute, risk can be calculated as a combination of probability (or likelihood) and impact (or consequences). The institute gives credit for the formula to Barry W. Boehm. We used that formula to calculate risk exposure scores: risk exposure = likelihood of occurrence (probability) * loss due to undesirable outcome (impact).

[10]Exposure scores were based on SEI's risk calculations and OMB guidance, as well as DOD's risk management guidance.

We then averaged the combined risk exposure scores for each program and rounded the result to the nearest whole number to obtain an overall risk rating for the acquisition as a whole. We compared our risk rating for each of the 22 programs to the CIO risk ratings that had been reported on the IT Dashboard to determine differences in the ratings.

We discussed our findings with officials in the offices of the USD(A&S) and the CIO. We also discussed the ratings with officials from the four programs where our ratings of program risk differed by 2 or more levels from the DOD CIO's ratings. Our calculations were only intended to provide a standardized view of risk across all the programs we reviewed; this methodology was not intended to serve as a prescriptive approach to the programs' evaluations of risk.

For the third objective, we sought information on the software and cybersecurity practices used by the 29 selected IT programs via our questionnaire. Our identification of risks or challenges that might impact acquisition outcomes were based on questionnaire responses from the 22 programs that were in active acquisition.[11] We aggregated the program offices' questionnaire responses and compared this information to relevant guidance and leading practices to identify where there were gaps and inconsistencies.[12] In doing so, we identified possible risks and challenges associated with not following guidance and leading practices that may impact acquisition outcomes relative to cost, schedule, and technical performance.

We did not validate the questionnaire responses provided by the program offices, although we followed up with programs when responses were

[11]For the purposes of this assessment, programs are considered to be developing software if they did not report only being in the sustainment phase of acquisition. The 22 programs discussed in this section reported being in the development and production, deployment, and sustainment phases. Some programs also reported being in other phases or a combination of multiple phases.

[12]GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C., Sept. 28, 2020); Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Cybersecurity Test and Evaluation Guidebook* Version 2.0, Change 1, (Washington, D.C., February 10, 2020); Department of Defense, *Operation of the Defense Acquisition System*, Instruction 5000.02 (Washington, D.C., Jan. 23, 2020); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 (Washington, D.C., Jan. 24, 2020).

unclear or inconsistent. Where we discovered discrepancies, we clarified the responses accordingly.

To address the fourth objective, we reviewed selected IT-related organizational, policy, and statutory changes, as well as 3rd party reports and DOD reports and documentation related to the effects of these changes on IT acquisitions.[13] We also reviewed IT-related statutory changes that had been made since December 2017 and related organizational and policy changes made since December 2019.[14] Specifically, we evaluated changes associated with DOD's efforts to transition to greater use of Agile software development, improve software oversight, and implement the statutory repeal of its chief management officer (CMO) position.[15]

We selected the three noted areas of change based on their importance to the 29 programs covered within the scope of this review. We also coordinated with the GAO team conducting a companion assessment examining Major Defense Acquisition Programs in response to this same provision of the NDAA for FY 2019.[16] This report focuses on programs in the defense business systems and software acquisition pathways, while the companion assessment focuses on programs in the major capability acquisition and middle tier of acquisition pathways.

To determine the potential implications of these changes, we reviewed policies, plans, and guidance provided by DOD; reports that the department submitted to Congress; and internal program documentation. In addition, we interviewed officials within DOD's OCIO, Office of the

[13]For example, Department of Defense, *Report to Congress on Implementation of Defense Science Board Report Recommendations, "Design and Acquisition of Software for Defense Systems" Section 868 of the National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232)* (Washington, D.C., April 16, 2020); Department of Defense, *Proposal for Reports on Acquisition Programs and Activities* (Washington, D.C., November 5, 2020); and Department of Defense, *Agile Software Acquisition Guidebook: Best Practices & Lessons Learned from the FY18 NDAA Section 873/874 Agile Pilot Program* (Washington, D.C., February 27, 2020).

[14]The information we reported in our 2020 report under this same mandate was as of December 2019. See GAO, *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, GAO-21-182 (Washington, D.C.: December 23, 2021).

[15]*William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Pub. L. No. 116-283, § 901, 134 Stat. 3388, 3794 (Jan. 1, 2021).

[16]GAO-21-222.

Undersecretary for Acquisition and Sustainment (USD(A&S)), and Office of the CMO (OCMO). We also aggregated program office responses to the questionnaire that pertained to DOD's implementation of Agile best practices and associated challenges, and met with staff within the DOD OCIO and the Office of the USD(A&S) to discuss program responses. Appendix I provides a more detailed discussion of our objectives, scope, and methodology.

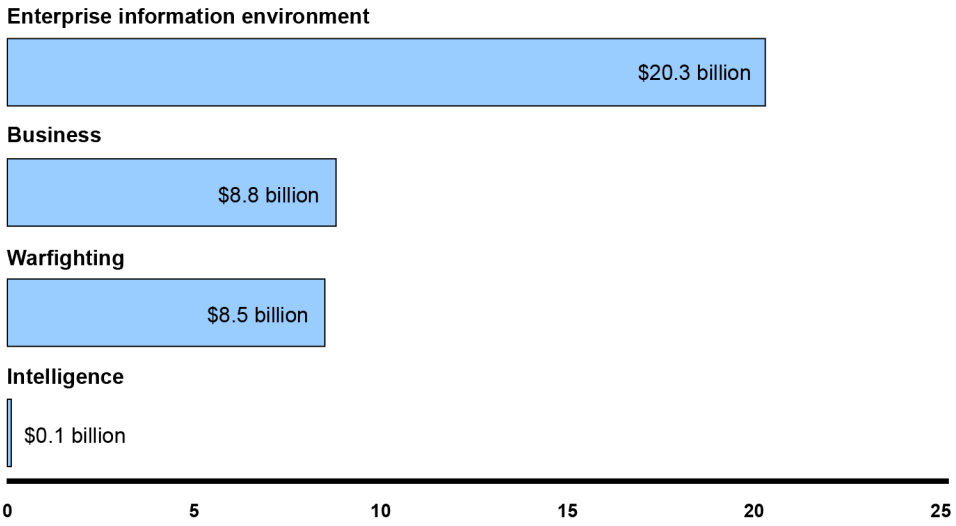
We conducted this performance audit from July 2020 to June 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In support of its military operations, DOD manages many IT investments, including investments in business, communications, and command and control systems. DOD's IT budget organizes investments in four categories, called mission areas—enterprise information environment, business, warfighting, and intelligence. Figure 1 shows the amount of DOD's total unclassified requested fiscal year 2021 IT budget (of $37.7 billion) that the department plans to spend on each of its mission areas, including the approximately $8.8 billion it plans to spend on developing, modernizing, operating, and maintaining its business system programs.[17]

[17]This figure does not include DOD's classified budget request. In addition, not all DOD IT expenditures are reported separately from their respective programs if those programs develop more than software and hardware to support the software. For example, our reports on DOD's weapon programs include programs that do not report software expenditures separately. See GAO-21-222.

Figure 1: Department of Defense (DOD) Fiscal Year 2021 Unclassified Information Technology Budget by Mission Area (projected)



Source: GAO analysis of DOD information technology budget information. | GAO-21-351

DOD's Acquisition Policy and Framework for Managing Major IT Acquisitions

In January 2020, DOD updated its acquisition policy to create an acquisition framework to enable flexible and responsive acquisitions. DOD Instruction 5000.02 established the new adaptive acquisition framework (AAF) as well as high-level policy for the AAF, and assigned roles and responsibilities to acquisition officials.[18] The instruction described a transition from the department's previous acquisition approach, and the department subsequently issued new policies to continue replacing the old approach, currently in DOD Instruction 5000.02T.[19]

Under the AAF, program managers are to tailor their acquisition strategy to one or more AAF pathways. Additionally, the AAF calls for program managers to continuously address cybersecurity throughout the program life cycle and establish a risk-management program.

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

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

DOD Instruction 5000.02 establishes six acquisition pathways in the AAF: (1) urgent capability acquisition, (2) middle tier of acquisition, (3) major capability acquisition, (4) defense business systems acquisition, (5) software acquisition, and (6) defense acquisition of services. While Instructions 5000.02 and 5000.02T establish overarching policy for acquisition programs, the roles, responsibilities, and procedures for each pathway are specified in separate instructions.

Business System Acquisitions Pathway

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

In January 2020, DOD updated the instruction for the defense business system acquisition pathway to align defense business system acquisitions with the AAF.[20] While maintaining the general structure of the defense business system pathway, the 2020 update removed certain oversight requirements and encouraged a tailored approach to each program. The 2020 update also enabled and encouraged acquisition officials to delegate decision-making down to the "lowest practical level."

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

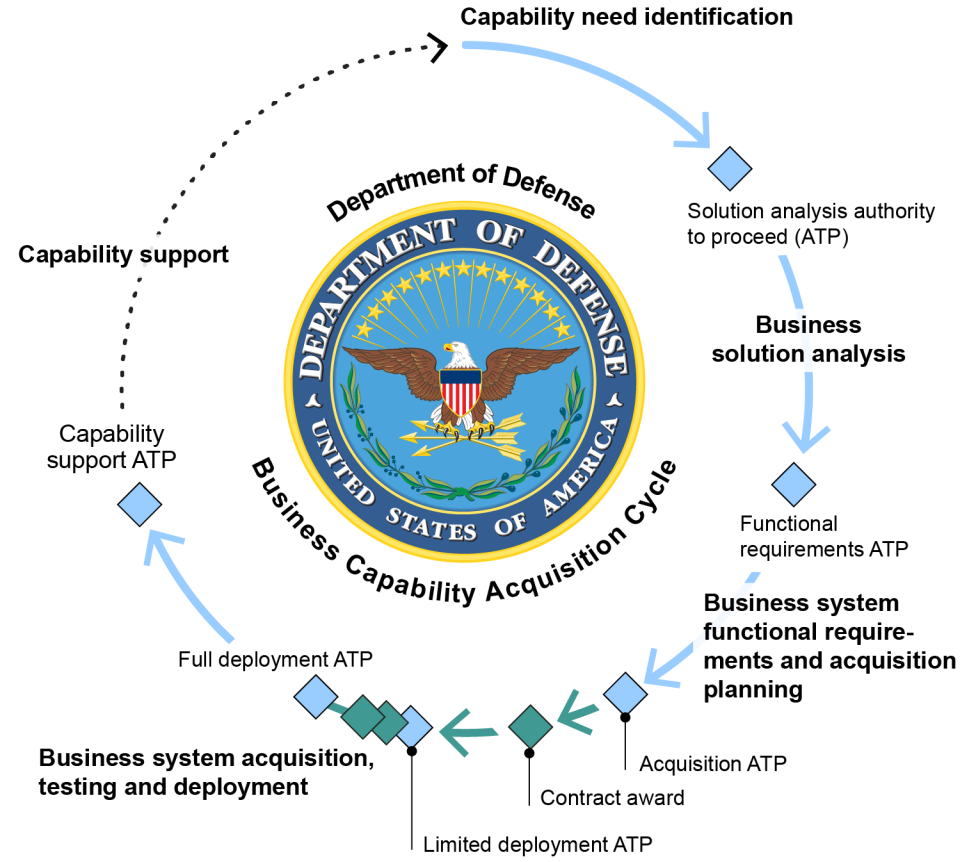
- align the program with commercial best practices;
- minimize the need for customization of commercial products to the maximum extent possible;
- conduct thorough industry analysis and market research of both process and IT solutions using commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software;
- tailor and delegate authority to proceed decision points, as necessary, to contribute to the successful delivery of business capabilities;
- automate testing; and

[20]Instruction 5000.75 establishes policy for the use of the five-phase business capability acquisition cycle for business system requirements and acquisitions. Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 [incorporating change 2 (Jan. 2020)] (Washington, D.C., Feb. 2, 2017).

- use Agile or incremental software development processes to the greatest extent practical.

Figure 2 shows the DOD business capability acquisition cycle.

Figure 2: DOD's Business Capability Acquisition Cycle



Source: Department of Defense Instruction 5000.75 (January 2020). | GAO-21-351

Software Acquisition Pathway

Section 800 of the NDAA for FY 2020 mandated that DOD develop the software acquisition pathway.[21] In October 2020, the department issued guidance titled Operation of the Software Acquisition Pathway, Instruction 5000.87.[22] According to this instruction, the purpose of this new pathway is to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software.

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

According to DOD Instruction 5000.02, the software acquisition pathway is intended to integrate modern software development practices such as Agile; development, security, and operations (DevSecOps); and lean practices.[23] Under this pathway, small cross-functional teams that include users, testers, software developers, and cybersecurity experts use enterprise services to deliver software rapidly and iteratively to meet user needs.

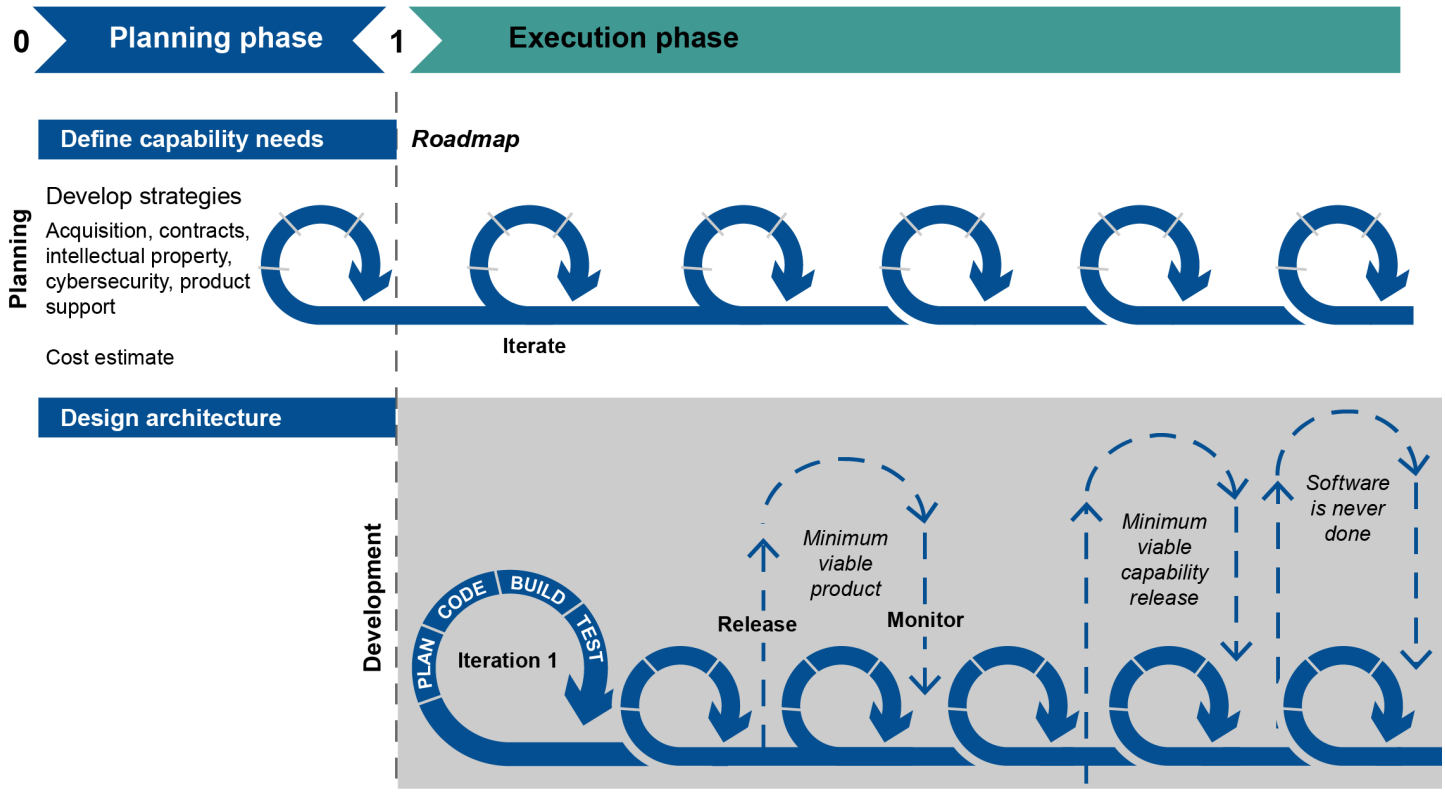
Under DOD Instruction 5000.87, the software acquisition pathway contains a planning phase and an execution phase. Figure 3 shows the two phases under this pathway.

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

[22]Department of Defense, *Operation of the Software Acquisition Pathway*, Instruction 5000.87 (Washington, D.C., October 2, 2020). Prior to the publication of Instruction 5000.87, the Department had an interim policy in effect. Department of Defense, *Software Acquisition Pathway Interim Policy and Procedures* (Washington, D.C., January 3, 2020).

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

Figure 3: DOD's Software Acquisition Pathway



Source: Department of Defense Instruction 5000.87 (October 2020). | GAO-21-351

DOD's Initial Implementation of Agile Software Development

Consistent with studies recommending DOD's transition toward Agile software development[24] and statutory mandates to help enable its transition toward Agile,[25] the department has begun implementing Agile as part of its software modernization initiative.

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

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

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

DOD has also created training,[26] issued guidance,[27] provided technical tools and resources,[28] and conducted outreach[29] to transition the department toward Agile. In addition, department leadership has taken steps to transition DOD through policy,[30] outreach efforts,[31] and the creation of a Software Modernization Senior Steering Group.

Further, DOD has established communities of practice and working groups to share information and address specific aspects of the

[26]See, for example, Department of Defense, *Self-learning*, accessed February 18, 2021, https://software.af.mil/training/. In addition, the Defense Acquisition University has established Agile and DevSecOps courses, see Defense Acquisition University, *DAU Agile and DevSecOps Training*¸ accessed February 8, 2021, https://www.dau.edu/training/career-development/logistics/blog/DAU-Agile-Software-and-DevSecOps-Training.

[27]This guidance includes: Department of Defense, *Agile Software Acquisition Guidebook: Best practices & lessons learned from the FY18 NDAA Section 873/874 Agile Pilot Program* (Washington, D.C., February 27, 2020); Department of Defense, *Agile Metrics Guide: Strategy Considerations and Sample Metrics for Agile Development Solutions*, Version 1.1 (Washington, D.C., September 23, 2019); and Department of Defense, *DoD Enterprise DevSecOps Reference Design*, Version 1.0 (Washington, D.C., August 12, 2019).

[28]These resources focus on providing programs with software development infrastructure. For example, see Department of Defense, *Platform One: DoD Enterprise DevSecOps Services*, accessed February 18, 2021, https://software.af.mil/dsop/services/; and Department of Defense, *Black Pearl*, accessed February 18, 2021, https://blackpearl.us/#!#portfolio.

[29]For example, DOD updates information on multiple publically available websites, hosts webinars, and holds town halls to further their software modernization efforts.

[30]For example, Department of Defense, *Software Development, Security, and Operations for Software Agility* (Washington, D.C., October 24, 2019); and Department of Defense, *Preferred Agile Framework* (Washington, D.C., December 28, 2019).

[31]For example, DOD leaders have published news articles and held regular information sessions on DOD's software modernization efforts.

department's Agile transition. For example, the Defense Acquisition University (DAU)[32] Agile Community of Practice has guidance and templates for programs transitioning to Agile practices;[33] DOD's Software Workforce Working Group aims to help DOD better recruit, hire, and retain software talent; and the Defense Security/Cybersecurity Authorization Working Group aims to promote software security policies that enable Agile development.

In addition, sections 873 and 874 of the NDAA for FY 2018 mandated that DOD implement two pilot programs to enable selected acquisition programs to embrace Agile practices.[34] DOD provided participating programs with training and tailored Agile guidance. The section 874 pilot lasted 1 year and DOD has shared lessons learned from the pilot related to the implementation of Agile practices. The section 873 pilot targeted large acquisition programs and is to continue through FY 2023.

DOD's Initial Steps to Modify How It Collects and Reports Acquisition Program Data

DOD is also taking steps to change how it collects data and metrics on acquisition programs as part of its broader acquisition reform and data management efforts. For example:

- In June 2020, the DOD USD(A&S) issued a memo calling for a data and analytics strategy to assess the progress of the department's policy transformation, promote transparent monitoring of the defense acquisition system throughout DOD, and inform program and portfolio decisions.[35]
- In August 2020, the Office of the USD(A&S) developed a data reporting plan intended to provide overarching guidance for all pathways within the AAF.[36] According to this plan, each owner of the acquisition pathway, in consultation with components and milestone

[32]Defense Acquisition University provides in-person and online classes to help develop qualified acquisition, requirements, and deployed defense personnel.

[33]Defense Acquisition University, IT Community of Practice: *Agile Acquisition (Software Engineering)*, accessed February 18, 2021, https://www.dau.edu/cop/it/Pages/Topics/SW-Engineering.aspx.

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

[35]Department of Defense, *Data Transparency to Enable Acquisition Pathways* (Washington, D.C., June 15, 2020).

[36]Department of Defense, *Secretary of Defense's Plan to Assess the Effects of Recent Acquisition Reforms and Who Will be Responsible for the Assessment as Well as What Data Will be Needed* (Washington, D.C., August 4, 2020).

decision authorities, must determine their own specific data strategy and reporting metrics to extract cost, schedule, and performance data.

- In September 2020, the Deputy Secretary of Defense issued a directive for managing all acquisition programs which stated that acquisition data should be transparently shared to the greatest extent possible across the military services and the Office of the Secretary of Defense.[37]
- In September 2020, the Deputy Secretary of Defense also issued a DOD data strategy. Among other goals, the strategy called for data to be visible, so consumers can locate the needed data, and accessible, so consumers can retrieve the data.[38]
- In November 2020, in response to a provision in the NDAA for FY 2020,[39] the USD(A&S) issued a report to congressional defense committees that described a proposal for reporting on acquisition programs.[40] According to the November 2020 report, the department proposed expanding its multipurpose data analytics system, called Advanced Analytics (ADVANA), to provide automated acquisition reporting for all programs, portfolios, and pathways within its AAF.
- In December 2020, the Office of the USD(A&S) released an Acquisition and Sustainment Data and Analytics Implementation Plan.[41] Among other objectives, the plan aims to make acquisition data available from authoritative sources in modern ways and to measure the effectiveness of policies, processes, and inputs on the defense acquisition system.

[37]Department of Defense, *The Defense Acquisition System*, DOD Directive 5000.01 (Washington, D.C., September 9, 2020).

[38]Department of Defense, *DOD Data Strategy* (Washington, D.C., September 30, 2020).

[39]Pub. L. No 116-92,§ 830, 133 Stat. 1198, 1492 (December 20, 2019).

[40]Department of Defense, *Proposal for Reports on Acquisition Programs and Activities* (Washington, D.C., November 5, 2020).

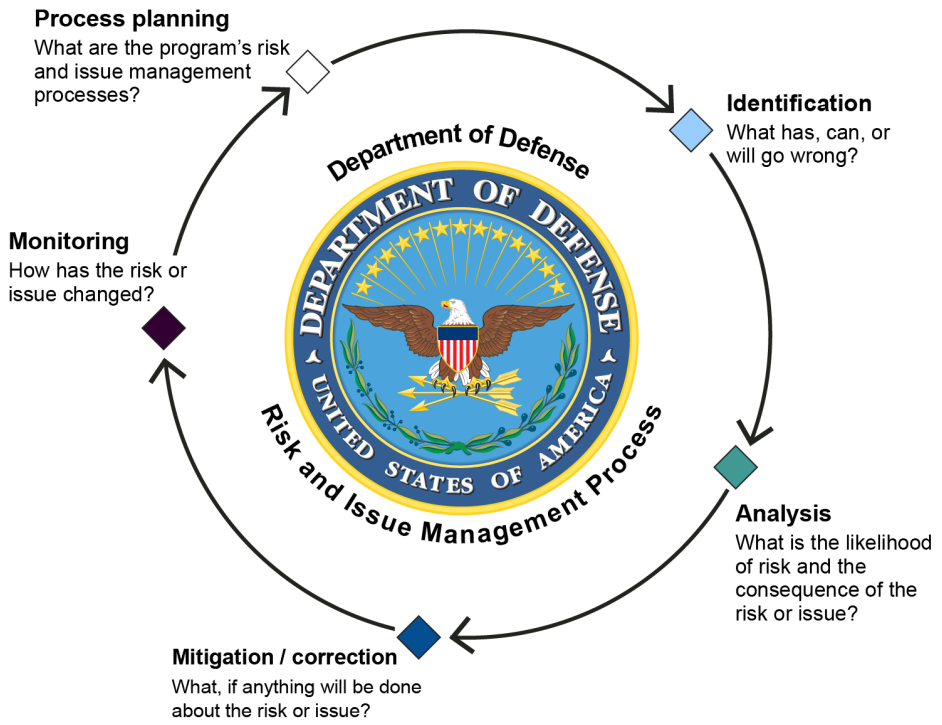
[41]Department of Defense, *Acquisition and Sustainment Data and Analytics Strategic Implementation Plan* (Washington, D.C., December, 2020).

In June 2021, we reported on the department's AAF data collection efforts and associated challenges with a focus on programs using the major capability acquisition and middle tier of acquisition pathways.[42]

DOD's Risk Management Guidance

According to DOD's January 2017 risk-management guide, risk management is an integral part of program management and systems engineering.[43] The guide describes the importance of managing program risks throughout a program's life cycle. The guide describes a five-step risk and issue management process that includes planning, identification, analysis, mitigation/correction, and monitoring. Figure 4 provides a high-level overview of this process.

Figure 4: DOD's Risk and Issue Management Process



Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (January 2017). | GAO-21-351

[42]GAO-21-222.

[43]DOD, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, January 2017.

The guide also states that programs commonly use risk registers as central repositories to describe and track risks. However, it does not explicitly require programs to establish and use risk registers. If using a risk register, the guide explains that programs should develop a risk register as early as possible in the programs' life cycle and include information for each risk, such as risk category, risk statement, likelihood, consequence, planned mitigation measures, and the person designated as responsible for the risk. Further, the guide explains that risk registers should also include linkages to a work breakdown structure or integrated master schedule and, where applicable, expected closure dates and documentation of changes.

DOD's Chief Management Officer Position Repealed by Statute

In 2007, the DOD designated the Deputy Secretary of Defense as the department's CMO. In addition, in 2008, the NDAA for FY 2008 established the position of deputy CMO. In 2016, the NDAA for FY 2017 established a standalone CMO position, effective February 1, 2018, that would be distinct from the Deputy Secretary of Defense and assigned a number of key responsibilities to the CMO.[44] In December 2017, the NDAA for FY 2018 amended Title 10[45] and later added additional responsibilities and functions for the CMO in the NDAA for FY 2019.[46]

The CMO's responsibilities were codified in section 132a of title 10, United States Code.[47] These responsibilities included managing DOD's enterprise business operations and exercising authority, direction, and control over the department's shared business services. The CMO was also responsible for overseeing efforts associated with the business system acquisition pathway.

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

[44]Pub. L. 114-328, § 901, 130 Stat. 2000, 2341 (December 23, 2016), codified at 10 U.S.C. § 132a.

[45]Pub. L. 115-91, § 910(b), 131 Stat. 1283, 1517 (December 12, 2017), codified at 10 U.S.C. § 132a.

[46]Pub. L. 115-232, § 921, 132 Stat. 1636, 1926 (August 13, 2018).

[47]10 U.S.C. § 132a.

response to our recommendations that called for such a position to be established.[48]

However, in June 2020, the Defense Business Board reported that the CMO position neither delivered the level of department-wide business transformation envisioned in the legislation, nor met the expectations of multiple Secretaries of Defense, Deputy Secretaries of Defense, other senior officials, or the congressional defense leadership.[49] The report also recommended that the CMO be "disestablished" and replaced with one of several alternatives.

In January 2021, section 901 of the *William M. (Mac) Thornberry NDAA for FY 2021* repealed the position of CMO within DOD. The NDAA also mandated that the department transfer the responsibilities, personnel, functions, and assets of the CMO to other officials, organizations, and elements and provide a report to Congress on associated recommendations for legislative action by January 2022.[50]

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

DOD's business systems modernization efforts have been on our High Risk List since 1995.[51] GAO's high-risk program focuses attention on government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement, or that are in need of transformation to address economy, efficiency, or effectiveness challenges. As we reported in March 2021, among other things, DOD has only partially met the leadership commitment criterion of our High Risk List.[52]

For example, we reported that department officials stated that, in March 2020, the department had established a Defense Business Systems and Enterprise Business Optimization Directorate within the OCMO. This new office was intended to assist the OCMO with implementation of statutory requirements for, among other things, managing defense business

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

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

[50]Pub. Law 116-283 § 901, 134 Stat. 3388, 3794 (January 1, 2021).

[51]See, for example, GAO, *High-Risk Series*, GAO-HR-95-1 (Washington, D.C., February 1, 1995). For additional work, see GAO-19-199 and GAO-19-157SP and our latest update to the High Risk List, GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2, 2021).

[52]GAO-21-119SP.

systems. We also reported that, in October 2020, the department developed a draft management playbook intended to assist the former OCMO with effectively delivering its mission. The draft playbook included information such as performance measures associated with streamlining the defense business systems environment.

GAO's Agile Assessment Guide Provides Best Practices for Implementing Agile Software Development

GAO developed the *Agile Assessment Guide* to help teams, programs, and organizations transition to Agile.[53] The guide includes Agile adoption best practices that address key risks associated with Agile transitions. These best practices are categorized in three functional categories: (1) organization environment, (2) program operations, and (3) team activities and dynamics. The guide also discusses the importance of establishing internal controls (e.g., policy and guidance) to support the practices discussed in the guide. The best practices and associated activities are shown in table 2.

Table 2: Categories of Agile Adoption, Best Practices, and Activities Associated with Each Category

Functional category	Best practice	Best practice activity description
Organization Environment	Organization activities support Agile methods	The organization should establish appropriate life-cycle activities and ensure that goals and objectives are clearly aligned.
	Organization culture supports Agile methods	The organization's sponsorship for Agile development should cascade throughout the organization and sponsors should understand Agile development. The Organization should also establish an environment supportive of Agile development. Incentives and rewards should be aligned to Agile development methods.
	Organization acquisition policies and procedures support Agile methods	Organization guidance should be appropriate for Agile acquisition strategies.
Program Operations	Staff are appropriately trained in Agile methods	Organization policy or guidance should ensure that all program staff are trained in Agile methods and call for Agile teams to have the appropriate technical expertise needed to perform their roles.
	Technical environments enables Agile development	Organization policy or guidance should call for technical and project tools being available to support Agile development. In addition, policy or guidance should call for system design that will support iterative delivery.
	Program controls are compatible with Agile	Organization policy or guidance should call for teams to maintain a sustainable development pace and track and monitor that development pace. In addition, policy or guidance should call for non-functional requirements and critical features to be defined and incorporated in development.

[53]GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C., September 28, 2020). GAO released the *Agile Assessment Guide* as an exposure draft for public comments on September 28, 2020.

Functional category	Best practice	Best practice activity description
Team Activities and Dynamics	Team composition supports Agile methods	Organization policy or guidance should call for self-organizing Agile teams and define the role of a product owner to support Agile methods.
	Work is prioritized to maximize value for the customer	Organization policy or guidance should call for Agile teams to use user stories to define work, requirements to be prioritized in a backlog based on value, including tracking and monitoring the value of work accomplished, and for Agile teams to estimate the relative complexity of user stories.
	Repeatable processes are in place	Organization policy or guidance should call for Agile teams to meet daily to review progress and discuss impediments, and observe end-iteration demonstrations and end-iteration retrospectives. In addition, organization policy or guidance should call for Agile projects to employ continuous integration and confirm mechanisms are in place to ensure the quality of code being developed. This includes setting expectations for automated testing and code quality and tracking and monitoring against these expectations.

Source: GAO Agile Assessment Guide. | GAO-21-351

The Federal IT Dashboard

The *Federal Information Technology Acquisition Reform Act* (FITARA) requires that covered agencies make detailed information on federal IT investments publicly available, in accordance with OMB guidance.[54] OMB displays these reports on the federal IT Dashboard, a public website that includes information on the performance of major IT investments. While OMB provides a general definition of a major IT investment, it gives each covered agency the flexibility to establish exact criteria.

The DOD CIO's FY 2021 guidance states that major IT investments include: (1) major defense acquisition programs[55] determined to be IT; (2) IT programs with a budget greater than $43 million for FY 2021 or greater

[54]Pub. L. No. 113-291, § 832, 128 Stat. 3292, 3440 (December 19, 2014); 40 U.S.C. § 11302.

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

than $558 million greater across the future years defense plan;[56] and (3) IT investments designated as major by department leadership.[57]

Currently, the federal IT Dashboard displays information on the cost, schedule, and performance of over 700 major IT investments at 26 federal agencies. In addition, OMB requires each agency's CIO to submit ratings to the Dashboard, which, according to OMB's instructions, should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals.

The public display of these data is intended to allow OMB, other oversight bodies, and the general public to hold agencies accountable for mission-related outcomes. We have issued a series of reports that have noted both the significant steps OMB has taken to enhance the oversight, transparency, and accountability of federal IT investments by creating the federal IT Dashboard, as well as issues with the accuracy and reliability of the data it contains.[58] Accordingly, we made recommendations to OMB to address these issues, which it has addressed.

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

[57]Department of Defense, *FY 2021 Information Technology/Cyberspace Activities Budget Guidance*, (Washington, D.C., August 8, 2019). The guidance also includes major automated information systems (MAIS) as major IT investments. However, the category has been otherwise removed from DOD policy and is no longer used by DOD officials when determining major IT investments. Regardless, the cost thresholds defined in the guidance are consistent with the cost thresholds formerly associated with MAIS.

[58]GAO, *IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments*, GAO-16-494 (Washington, D.C.: June 2, 2016); *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to Be More Accurate and Available*, GAO-14-64 (Washington, D.C.: Dec. 12, 2013); *IT Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies*, GAO-13-98 (Washington, D.C.: Oct. 16, 2012); *IT Dashboard: Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Making*, GAO-12-210 (Washington, D.C.: Nov. 7, 2011); *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy*, GAO-11-262 (Washington, D.C.: Mar. 15, 2011); and *Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Improvements Needed*, GAO-10-701 (Washington, D.C.: July 16, 2010).

DOD's Major Business IT Programs Reported Performance Changes and Challenges Due to Various Reasons, including COVID-19

According to DOD's FY 2021 budget request, the department spent $2.8 billion on the 29 selected major IT business programs in fiscal year 2019.[59] DOD also reported that it planned to invest over $9.7 billion on these programs between FY 2020 and FY 2022. Of the total amount that DOD reported spending and planning to spend between FY 2019 and 2022, the department categorized $9.1 billion (72 percent) as being used to operate and maintain the systems and the remaining $3.5 billion (28 percent) as being used to develop, modernize, and enhance the systems.

DOD CIO officials expressed concerns about how the traditional defense appropriations categories might limit the programs' abilities to take advantage of more modern approaches to software development. The officials also described an effort underway to pilot an alternative to the department's current approach for allocating funds to its IT programs.

Twenty of the 29 major business IT programs also reported experiencing a variety of cost or schedule changes since January 2019. Of these programs, four reported the extent to which program costs and schedules had changed, noting cost increases that ranged from $10 million to $11 million, and schedule delays that ranged from 3 months to 2 years.

Program officials attributed the changes to various factors, including cloud migration or modernization changes, requirements changes, and technical complexities.

Additionally, 17 of the 29 programs reported experiencing challenges associated with the COVID-19 pandemic. Twenty-eight reported taking actions to help the program address COVID-19 impacts. These actions included approving expanded telework arrangements and designating contractors as essential critical infrastructure workers.

DOD Plans to Spend Over $12 Billion on Its Major Business IT Programs, FY 2019 through FY 2022

Based on our analysis of DOD's FY 2021 IT budget request, DOD spent $2.8 billion on its 29 major IT business programs in fiscal year 2019. DOD also reported that it planned to invest over $9.7 billion on these programs between FY 2020 and FY 2022. As of February 2020, of the total $12.6 billion[60] DOD spent and planned to spend, the department categorized $9.1 billion (72 percent) for operations and maintenance (O&M) and the

[59]As of March 2021, DOD had not released its fiscal year 2022 budget request.

[60]Numbers do not add due to rounding.

remaining $3.5 billion (28 percent) for development, modernization, and enhancements (DME).

Table 3 shows the total actual and planned expenditures for the portfolio of 29 major business IT programs for FY 2019 through FY 2022, by program and fiscal year, as of February 2020.

Table 3: DOD Planned Expenditures for 29 Selected Major Business IT Programs from Fiscal Years (FY) 2019 through 2022, as of February 2020

Dollars in millions

Program	FY19 (actuals)	FY20 (projected)	FY21 (requested)	FY22 (planned)	4-year total
Department of Defense Healthcare Management System Modernization	600	578	807	981	**2,965**
Navy Enterprise Resource Planning	179	346	382	376	**1,282**
Global Combat Support System – Army	355	276	297	325	**1,254**
General Fund Enterprise Business System	161	158	174	168	**661**
Navy Standard Integrated Personnel System	96	65	134	252	**548**
Enterprise Business System	152	150	123	118	**543**
Defense Enterprise Accounting and Management System – Increment 1	105	129	128	142	**504**
Navy Maritime Maintenance Enterprise Solution	117	117	128	118	**480**
Defense Enrollment Eligibility Reporting System	96	98	105	109	**408**
Defense Agencies Initiative	74	104	90	100	**368**
Real-Time Automated Personnel Identification System and Common Access Card	73	77	84	87	**321**
Armed Forces Health Longitudinal Technology Application	118	83	67	45	**313**
Global Combat Support System Marine Corps / Logistics Chain Management	61	60	76	72	**269**
Defense Medical Logistics–Enterprise Solution	52	54	77	82	**265**
Distribution Standard System	47	49	77	71	**244**
Mepcom Integrated Resource System	57	59	51	52	**219**
Defense Medical Information Exchange	47	48	54	55	**203**
Naval Tactical Command Support System	47	52	51	49	**199**
Navy Electronic Procurement System	26	58	56	54	**194**
Distributed Learning System	39	51	48	48	**186**
Composite Health Care System	44	50	51	39	**184**
Army Contract Writing System	48	26	42	41	**157**
Air Force Integrated Personnel and Pay System	49	47	37	22	**156**
Defense Travel System	44	42	35	29	**151**
Standard Procurement System	32	36	35	32	**135**

Program	FY19 (actuals)	FY20 (projected)	FY21 (requested)	FY22 (planned)	4-year total
Navair Aviation Logistics Environment	33	22	36	31	**122**
Maintenance Repair and Overhaul Initiative	56	16	25	22	**120**
Defense Civilian Personnel Data System	29	40	35	9	**114**
Military Health System Virtual Health Program	3	13	3	3	**22**
Totals:	**2,842**	**2,902**	**3,308**	**3,534**	**12,586**

Source: GAO analysis of Department of Defense budget request data. | GAO-21-351

Notes: Numbers do not always add due to rounding. In addition, officials from three programs stated that these estimates include budgeted funds for emerging systems and modernization efforts that DOD officials will redirect to new programs that will be reflected in future budget requests. Moreover, since the budget request was published in February 2020, some programs have subsequently experienced cost estimate changes that will be reflected in future budget requests.

Several programs accounted for a large portion of DOD's actual and planned expenditures. Specifically, of the $12.6 billion in actual and planned spending from FY 2019 through FY 2022, three programs accounted for $5.5 billion (44 percent): the DOD Healthcare Management System Modernization (DHMSM) planned to spend almost $3 billion; and the Navy Enterprise Resource Planning (Navy ERP) and Global Combat Support System–Army (GCSS-A) each planned to spend almost $1.3 billion.

As of November 2020, program officials for DHMSM and GCSS-A reported that these programs were both operating in a mixed acquisition phase, as they were both developing new capabilities and sustaining existing capabilities. Navy ERP officials reported that the program was fully engaged in the production, deployment, and sustainment acquisition phase. According to DOD's FY 2021 budget request, DHMSM planned to spend 44 percent of its budgeted funds ($1.3 billion) on O&M, GCSS-A planned to spend 73 percent of its budgeted funds ($915.5 million) on O&M, and Navy ERP planned to spend 100 percent of its budgeted funds (almost $1.3 billion) on O&M from FY 2019 through 2022.

Table 4 provides additional information about the 29 major business IT programs' actual and planned expenditures from FY 2019 through 2022 and the percentage of those expenditures associated with O&M spending.

Table 4: DOD Programs' Total Actual and Planned Expenditures and Percentage of Total Actual and Planned Expenditures Associated with Operations and Maintenance (O&M) Spending, Fiscal Years (FY) 2019 through 2022

Program	Actual and planned expenditures, FY19 - FY22 (millions of dollars)	Amount of total actual and planned expenditures associated with O&M spending (percentage)
Navy Enterprise Resource Planning	1,282	100
Defense Enrollment Eligibility Reporting System	408	100
Armed Forces Health Longitudinal Technology Application	313	100
Global Combat Support System Marine Corps / Logistics Chain Management	269	100
Distribution Standard System	244	100
Defense Medical Information Exchange	203	100
Naval Tactical Command Support System	199	100
Distributed Learning System	186	100
Composite Health Care System	184	100
Standard Procurement System	135	100
Defense Travel System	151	98
Defense Civilian Personnel Data System	114	98
Defense Medical Logistics–Enterprise Solution	265	96
Enterprise Business System	543	92
Real-Time Automated Personnel Identification System and Common Access Card	321	89
Navy Maritime Maintenance Enterprise Solution	480	88
General Fund Enterprise Business System	661	85
Military Health System Virtual Health Program	22	82
Defense Agencies Initiative	368	76
Global Combat Support System – Army	1,254	73
Mepcom Integrated Resource System	219	67
Navy Standard Integrated Personnel System	548	58
Defense Enterprise Accounting and Management System – Increment 1	504	53
Department of Defense Healthcare Management System Modernization	2,965	44
Navair Aviation Logistics Environment	122	36
Army Contract Writing System	157	21
Air Force Integrated Personnel and Pay System	156	13
Navy Electronic Procurement System	194	2
Maintenance Repair and Overhaul Initiative	120	0

Source: GAO analysis of Department of Defense budget request data. | GAO-21-351

Note: These data include actual expenditures reported by DOD for fiscal year 2019 and planned expenditures for fiscal years 2020 through 2022. Officials from three programs (Navy Standard

Integrated Personnel System, General Fund Enterprise Business System, and Navair Aviation Logistics Environment) stated that these estimates include budgeted funds for emerging systems and modernization efforts that DOD officials will redirect to new programs reflected in future budget requests. In addition, since the budget request was published in February 2020, some programs have experienced cost estimate changes that will be reflected in future budget requests.

We have previously reported on DOD's spending on operating and maintaining systems, particularly legacy systems, in lieu of spending on developing new systems.[61] As we have noted, a small number of aging systems can drive portfolio cost growth, putting the department at higher risk of wasteful spending. Such systems can also create cybersecurity weaknesses, increasing vulnerability to threat actors.

In addition, recent studies have highlighted concerns with how funds are appropriated for DOD's IT programs. For example, the Defense Innovation Board[62] reported in May 2019 that traditional breakdowns of development versus sustainment are not suited for modern software development, where development is cyclical, not linear.[63] According to the Defense Innovation Board, programs face difficulties determining which activities are "development" and which are "maintenance" for software. As a result, the Defense Innovation Board recommended that Congress fund software acquisition programs through a single appropriation that covers the entire software development life cycle and supports iterative software development activities.

DOD OCIO's Software Modernization Lead also described concerns associated with the use of the traditional DME and O&M breakdowns in budgeting for IT systems. For example, traditionally, once a program proceeds into production and deployment, programs transition from a focus on research and development to a focus on maintaining the program. This can result in scenarios where programs stop investing in new code and begin focusing on maintaining a running system. However, without consistent updates, the system can become outdated or might not receive necessary updates to address critical system aspects, such as cybersecurity. DOD OCIO officials also described scenarios where

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

[62]The Defense Innovation Board is an independent federal advisory committee advising the Secretary of Defense on topics such as, people and culture; technology and capabilities; and practices and operations.

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

systems may have been in existence for so long that developers are no longer available; source code is no longer available; or developers no longer know how to compile code for the system. They contrasted this with more modern approaches of continuous ongoing advancement and development of a system.[64]

Officials from the DOD OCIO also described steps Congress and DOD have taken to address these concerns. For example, in September 2020, DOD initiated a pilot program to fund nine programs through a new budget activity. This activity, initially funded through components' Research, Development, Test and Evaluation[65] budgets, is to allow programs to report expenses under a single budget activity. Congress authorized funding for the pilot in the NDAA for FY 2021.

Twenty of the 29 Programs Reported Experiencing Cost or Schedule Changes since January 1, 2019

As of December 2020,[66] 20 of the 29 major business IT programs reported in response to our questionnaire that they had experienced either cost or schedule changes since January 1, 2019. Specifically, 17 programs reported experiencing changes to planned costs and 14 programs reported experiencing changes to planned schedules.

Four of the programs reported on the extent to which program costs and schedules changed. Specifically, two of the four programs provided dollar values of cost changes: increases of $10 million and $11.4 million. Similarly, three of the four programs reported specific schedule changes: delays ranging from 3 months to 2 years.

Of the 20 programs that reported they had experienced either cost or schedule changes since January 1, 2019, officials reported a variety of reasons for the cost and schedule changes, including:

- **Cloud Migration and Modernization Changes.** Five programs reported changes in cost or schedule due to changes to cloud migration and modernization efforts. This included migrating from

[64]These more modern approaches include incremental and Agile software development, discussed in this report.

[65]Research, Development, Test & Evaluation funds are used to pay for conducting research, development, and test and evaluation efforts.

[66]GAO received the majority of program questionnaire responses from DOD in October 2020; however, the dates in which we received responses ranges from October to December 2020.

Defense Information Systems Agency-hosted infrastructure to a private industry cloud infrastructure and the acceleration of planned cloud migrations in fiscal year 2020, as well as migrating from legacy systems to new systems.

- **Requirements Changes or Delays.** Five programs reported changes in cost or schedule due to new or unplanned requirements. This included mandatory changes to financial feeder systems, new Working Capital Fund[67] financial requirements, the addition of U.S. Space Force requirements, and delayed requirements from a vendor.
- **Unanticipated Technical Complexities.** Two programs reported changes in cost or schedule due to unanticipated technical complexities related to program efforts. This included the complexity of system replacements and greater than anticipated technical complexity for development activities.
- **Contracting Developments.** Two programs reported changes in cost or schedule due to contracting developments. This included new contractor support for a technical refresh and a bid protest.

Seventeen of the 29 Programs Reported Challenges as a Result of the COVID-19 Pandemic

The COVID-19 pandemic has had a massive impact across the world. As we have previously reported, agencies from across the federal government, including DOD, continued their operations while shifting many staff to telework, requiring an unprecedented level of dedication and agility among the federal workforce.[68] As of December 2020, 17 of the 29 DOD major business IT programs that we reviewed each reported experiencing one or more challenges as a result of the early impacts from COVID-19. These included a variety of challenges, such as slower software development, travel restrictions, and telework.[69]

Fifteen of the 17 programs reported program office challenges as a result of COVID-19. Of these 15, three reported that program office software development efforts were temporarily slowed due to COVID-19. However,

[67]Working capital funds operate as a self-supporting entity that conducts a regular cycle of businesslike activities. They are intended to create incentives for customers and managers to control costs.

[68]We regularly issue government-wide reports on the federal response to COVID-19. For the latest report, see GAO, *COVID-19: Sustained Federal Action Is Crucial as Pandemic Enters Its Second Year*, GAO-21-387 (Washington, D.C.: Mar. 31, 2021). Our next government-wide report will be issued in July 2021 and will be available on GAO's website at https://www.gao.gov/coronavirus.

[69]Given the timing of our questionnaire, these responses reflect early impacts of COVID-19.

none of the programs reported cuts in staff hours or a halt to software development.

The 15 program offices also identified other challenges, including remote work and training, a change in demand for services, travel restrictions impacting operational testing and deployment abilities, and the re-prioritization of critical tasks to directly support the COVID-19 Task Force mission. Table 5 summarizes program offices' reported impacts related to COVID-19.

Table 5: Major DOD Business IT Programs Reported Program Office Challenges Related to COVID-19

Challenge related to COVID-19	Number of programs
Other[a]	15 of 29
Software development was temporarily slowed	3 of 29
Staff worked fewer hours or were temporarily furloughed	0 of 29
Software development was temporarily shut down	0 of 29

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

[a]Programs that reported "other" for program office challenges provided examples that included challenges related to travel restrictions, telework, and the redistribution of workloads due to personnel downtime.

According to the programs, the contractors for eleven programs also reported challenges related to COVID-19. Four programs reported that contractors' software development efforts were temporarily slowed due to COVID-19. Nine of the eleven programs also reported other challenges including slowdowns in productivity due to teleworking, a reprioritization of requirements to focus on the COVID-19 response, workloads redistributed due to personnel with COVID-19 symptoms/downtime, and contractors being directed to leave facilities and follow state requirements to quarantine before returning. None of the programs reported that contractor staff had worked fewer hours or were temporarily furloughed, software development was temporarily shut down, or that contractors went out of business. Table 6 summarizes challenges related to COVID-19 that contractors reported to programs.

Table 6: Major DOD Business IT Programs Reported Contractor Reported Challenges Related to COVID-19

Challenge Related to COVID-19	Number of programs
Other[a]	9 of 29
Software development was temporarily slowed	4 of 29
Staff worked fewer hours or were temporarily furloughed	0 of 29
Software development was temporarily shut down	0 of 29
Contractor(s) went out of business	0 of 29

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

[a]Programs that reported "other" for contractor reported challenges provided examples that included challenges related to contractor support being directed to leave facilities, planned work being reprioritized, and collaborative work being more difficult.

In addition, 11 programs reported that they experienced or expected to experience a variety of cost and schedule changes associated with the early impacts of the COVID-19 pandemic.

- Two of the 11 programs reported that cost and schedule changes associated with the early impacts of COVID-19 had already occurred.
- Four of the 11 programs reported that a cost impact had either occurred or was expected to occur.
- Four of the 11 programs reported that the cost impact had yet to be determined.
- Fifteen programs reported no cost impact as a result of COVID-19.[70]

Of the programs reporting that a cost impact occurred or would occur, the program that reported the highest cost impact estimated a cost increase of $2 million to $3 million.

Further, programs reported experiencing or anticipated experiencing schedule delays ranging from 4 to 32 weeks due to COVID-19. Six programs reported that the schedule impact had yet to be determined. Eleven programs reported that the COVID-19 pandemic did not have a schedule impact.

Program officials reported taking a variety of actions to address the early impacts of COVID-19. For example, 28 of the 29 major business IT programs reported approving expanded telework arrangements and 12 of

[70]Not all programs responded to these questions, and some selected multiple options.

the 29 programs reported designating contractors as essential workers. Table 7 summarizes actions programs reported taking to address the early impacts of COVID-19.

Table 7: Major DOD Business IT Programs Reported Taking Actions to Help Programs Address COVID-19 Early Impacts

Action	Number of programs
Approved expanded telework arrangements	28 of 29
Designated contractors essential critical infrastructure workers	12 of 29
Expedited new contract awards	4 of 29
Modified contract delivery dates	4 of 29
Other	4 of 29
Expedited release of withheld funding to prime contractor	0 of 29
Increased progress payment percentages for completed work and future production	0 of 29
Removed penalties for missing performance targets	0 of 29

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

While these responses reflect early impacts of COVID-19, these programs may face continued cost and schedule pressures for some time. These challenges further emphasize the importance of effective oversight in order to ensure that DOD mitigates these disruptions to its major business IT programs to the greatest extent possible to avoid delays in delivery of critical capabilities. We will continue to monitor DOD's efforts to mitigate COVID-19-related effects through our other ongoing work, such as on DOD's implementation of section 3610 of the *Coronavirus Aid, Relief, and Economic Security Act of 2020*. The act allows DOD and other federal agencies to reimburse contractors for the cost of paid leave during the COVID-19 pandemic.[71]

[71]GAO, *COVID-19 Contracting: Observations on Contractor Paid Leave Reimbursement Guidance and Use*, GAO-20-662 (Washington, D.C., Sept. 3, 2020).

DOD CIO Assessments Identified a Range of Program Risk Levels but Some Program Risks Could be Understated

OMB requires that each federal agency CIO rate the risk of its major IT investments on a scale of 1 to 5, with 1 reflecting more risk and 5 reflecting less risk.[72] These ratings subsequently are to be reported on OMB's federal IT Dashboard, which also displays cost, schedule, and performance data for major IT investments at 26 federal agencies.

DOD CIO's assessments of program risk identified a range of program risk levels and indicated that some programs could be underreporting risks. Specifically, of the 22 programs that were actively using a risk register to manage program risks, DOD rated nine as low risk, 12 as medium risk, and one as high risk.[73] In contrast, of these 22 programs, GAO rated seven as low risk, 12 as medium risk, and three as high risk. In total, we found 10 programs for which our numerical assessments of program risk reflected greater risk than reported by DOD. Our assessments matched DOD CIO's rating for nine programs and showed less risk than reported by the DOD CIO for three programs.

Notably, four programs had CIO risk ratings that differed by two or more points from our assessments. For three of these programs, our assessments indicated greater risk than the CIO risk rating. For one of these programs, our assessment indicated less risk than the CIO risk rating. Table 8 provides a summary of programs' reported risks, our associated risk ratings, and the DOD CIO's risk ratings.

[72]OMB, *FY 2021 IT Budget–Capital Planning Guidance* (Washington, D.C., June 28, 2019).

[73]The remaining seven programs lacked a risk register, did not track active risks, or did not track the types of data needed for our calculations. DOD's risk management guidance does not require programs to maintain a risk register.

Table 8: Comparison of GAO Risk Ratings and DOD's Chief Information Officer (CIO) Risk Ratings for Selected Major IT Programs

Program	Number of reported risks			GAO risk ratings[a]	DOD CIO risk ratings[b]
	High risks	Medium risks	Low risks		
Defense Travel System	1	0	0	1	3
Defense Agencies Initiative	4	3	0	2	3
Defense Enterprise Accounting and Management System – Increment 1	1	0	0	2	3
Department of Defense Healthcare Management System Modernization	5	9	5	3	3
Real-Time Automated Personnel Identification System and Common Access Card	2	1	2	3	3
Maintenance Repair and Overhaul Initiative	1	1	1	3	3
Navy Electronic Procurement System	1	1	1	3	3
Defense Civilian Personnel Data System	1	2	0	3	3
Air Force Integrated Personnel and Pay System	0	9	3	3	3
Navair Aviation Logistics Environment	0	4	0	3	3
Standard Procurement System	0	2	0	3	3
Global Combat Support System Marine Corps / Logistics Chain Management	3	5	3	3	4
Navy Enterprise Resource Planning	1	4	1	3	4
Armed Forces Health Longitudinal Technology Application	6	15	5	3	5
Global Combat Support System – Army	4	17	11	3	5
Defense Enrollment Eligibility Reporting System	1	1	2	4	3
Naval Tactical Command Support System	3	0	4	4	5
Defense Medical Logistics–Enterprise Solution	1	6	18	4	5
General Fund Enterprise Business System	1	5	6	4	5
Army Contract Writing System	0	0	5	5	2
Enterprise Business System	0	0	2	5	4
Composite Health Care System	0	0	2	5	5

Legend: Red = High risk rating, Yellow = Medium risk rating, Green = Low risk rating

Source: GAO analysis of IT Dashboard and agencies' data. | GAO-21-351

[a]We developed the GAO rating by calculating the risk rating of each individual risk contained in a program's risk register, averaging the risk rating of all individual risks, and rounding that average to the nearest whole number. Programs provided risk registers to us between October and December 2020. See appendix I for a detailed description of our risk calculations.

[b]DOD reports CIO evaluation ratings to the federal IT Dashboard based on the Chief Information Officer's evaluation of program risk. DOD CIO risk ratings were those last reported on the federal IT Dashboard in April 2020.

CIO officials stated that different approaches for assessing program risks was likely a factor in the difference between the DOD CIO's and our risk ratings. According to the officials, the CIO ratings are intended to reflect

the CIO's assessment of risk and may be based on additional programmatic information not included in our assessment methodology, which focused primarily on program risk registers. As such, the inherently judgmental nature of the CIOs' assessments may reflect broader considerations that, in their organization's view, better represent the overall risk of an investment.[74]

Officials from the DOD OCIO also noted that they receive proposed program risk ratings from DOD component organizations' CIOs and review information provided to them along with those risk ratings. These officials stated that they usually use the rating submitted by the component when reporting to the federal IT Dashboard, but they might work with a component to change a proposed risk rating if they identify a discrepancy between the rating and what they know about the program. However, such an approach may introduce additional judgment into the process of developing a CIO risk rating.

In addition, our analysis shows that program risks may have evolved over time as programs actively monitored and mitigated their risks and as programs changed over time. In particular, as of December 2020, DOD CIO risk ratings had been last reported on the federal IT Dashboard in April 2020.[75] In contrast, we used risk registers provided by programs that reflected more recent assessments of risk. Specifically, we analyzed risk registers that programs provided to us between October and December 2020. The acquisition manager from one of the three programs we identified as high risk also noted that our evaluation was reflective of a single point in time.

Further, DOD's guidance on risk management emphasizes the importance of adopting a culture of risk management to manage uncertainty and increase predictable outcomes. Consistent with this approach, programs that track a larger number of higher risks might be managing risks more carefully and proactively than programs that track a

[74]Officials from the DOD OCIO stated that the risk ratings are initially reported to the DOD CIO by DOD component organizations (e.g., military departments). The DOD Office of the CIO reviews the reported ratings and supporting information and looks for discrepancies before submitting the ratings to the federal IT Dashboard. If DOD CIO officials identify discrepancies, they work with component officials to resolve the discrepancies, potentially changing the DOD CIO's risk rating.

[75]Officials from the DOD OCIO stated that they provided more recent submissions to OMB. However, as of February 2021, those submissions had not yet been made available to the public. According to those officials, this was due to the timing of the annual budget process and the change in presidential administrations.

smaller number of higher risks. However, such an approach would also result in a higher risk rating using our approach.

Program officials responsible for the four programs where our risk ratings differed by two or more points (i.e., the largest differences) cited reasons for these differences that were consistent with the above-stated reasons. For example, a program official from the Army Program Executive Office (PEO) responsible for GCSS-A stated that the difference might be attributed to the program being in a different stage of development at the time DOD reported the CIO risk ratings to the federal IT Dashboard than when we collected its risk register. In addition, a program official from the Defense Human Resources Activity Program Executive Office, the component office responsible for the Defense Travel System program, stated that the difference was likely related to organizational changes that also improved how risks were being managed at the program level between the time that the CIO rating was developed and the time we reviewed the program's risk register.

Finally, the CIO of the Defense Health Agency, the lead component for the Armed Forces Health Longitudinal Technology Application, stated that the program had been in the operations and maintenance phase for many years, was stable, and was supported by an experienced staff. As a result, the DOD CIO rating for the program was low risk. However, the official added that program office staff track risks thoroughly, which is likely the reason that the risk register includes a risk profile that resulted in a medium risk rating by GAO. For example, one risk identified on the risk register is associated with the risk of delays in ongoing development of the programs' successor system. Program officials noted that this risk is outside of the program's control and does not impact the ability of the program to continue functioning as designed. Nevertheless, our assessment of risk relied solely on data from program risk registers.

Regarding the one program where the DOD CIO risk rating showed greater risk than our risk rating by two or more points, a program official from the Program Executive Office responsible for the Army Contract Writing System stated that the program was still in development at the time DOD reported the CIO risk rating to the federal IT Dashboard, but was more mature later in the year. In particular, this official stated that the program was initially fielded to a pilot site by the end of 2020.

Nevertheless, our assessments show that some programs could be underreporting program risks. In those cases, public and congressional interest in and oversight of those programs could be limited by overly

optimistic risk perspectives, resulting in a less clear picture of the risks facing those programs.

DOD IT Programs Reported Using Software Development and Cybersecurity Approaches That May Limit Risk; DOD is Taking Steps to Address Reported Challenges

As of December 2020, DOD program officials reported using approaches that may help to limit risks to cost and schedule outcomes for 22 major business IT programs we assessed that were developing software.[76] For example, 18 of the 22 programs reported using continuous iterative software development, as recommended by the Defense Science Board.[77] According to the Defense Science Board, continuous iterative software development allows program staff to catch errors quickly and continuously, integrate new code with ease, and obtain user feedback throughout the application development process.

In addition, 21 of 22 programs reported developing or planning to develop an approved cybersecurity strategy, as called for by DOD guidance.[78] These strategies are intended to help ensure that program staff are planning for and documenting cybersecurity risk management efforts, which begin early in the programs' life cycle. Table 9 details the nine approaches that we identified that may help to limit risks, as well as the number of programs that reported implementing them.

[76]For the purposes of this assessment, programs are considered to be developing software if they did not report being in the sustainment phase of acquisition, or if they reported being in sustainment but also reported being in another phase of acquisition. The 22 programs discussed in this section reported being in the development and production, deployment, and sustainment phases. Officials from some programs also reported being in other phases or a combination of multiple phases. Program officials from the 7 programs not included in this section only reported that their programs were in sustainment.

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

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

Table 9: Major DOD Business IT Program Officials Reported Software Development and Cybersecurity Approaches That May Limit Risks

Software development and cybersecurity approaches that may limit risk	Number of programs that reported using the approach
Using off-the-shelf software	19 of 22
Using at least one recommended development process[a]	19 of 22
Delivering a minimum deployable product[b]	18 of 22
Implementing continuous iterative software development	18 of 22
Delivering software at least every 6 months[c]	16 of 22
Developing or planning to develop a cybersecurity strategy	21 of 22
Conducting cybersecurity assessment(s)	15 of 16[d]
Conducting developmental cybersecurity testing	16 of 22
Conducting operational cybersecurity testing	15 of 22

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

[a]Program officials were asked if they used any of the following software development processes recommended by the Defense Science Board: software factory, delivery of minimum viable product followed by successive next viable products, continuous iterative development, iterative development training for program managers and staff, software documentation provided to DOD at each production milestone, and independent verification and validation for machine learning.

[b]These products are also commonly called minimum viable products.

[c]The Defense Innovation Board encourages the delivery of working software to users more frequently for Agile and DevOps practices.

[d]We only asked the 16 programs that had created a cybersecurity strategy (of the 21 that had created or planned to create a cybersecurity strategy) to answer the associated question about whether they had conducted cybersecurity assessments.

Program officials also reported a variety of software development challenges associated with these approaches. These included difficulties finding and hiring staff, transitioning from waterfall to Agile software development, and managing technical environments.

Major DOD Business IT Programs Reported Using Software Development and Cybersecurity Approaches That May Limit Negative Outcomes

Programs Reported Using a Variety of Software Types

According to DOD Instruction 5000.75, *Business Systems Requirements and Acquisition*, DOD business system acquisitions should minimize the need for customization of commercial products to the maximum extent possible.[79] Specifically, program staff should use COTS and GOTS solutions, to the extent practicable. However, program staff should be careful to limit the degree to which they customize the off-the-shelf software. The *Defense Acquisition Guidebook* notes that modifying COTS software places programs at risk of losing the ability to use product upgrades and of finding it difficult to acquire a suitable replacement for the product from other commercial sources.[80]

According to DOD, the use of COTS software is intended to reduce software development time, allow for faster delivery, and lower life-cycle costs due to increased product availability and use of modern technologies. By leveraging commercial software, business program staff can position themselves to limit some of the risks inherent in other approaches and leverage the benefits of using commercial software.

Consistent with DOD guidance, officials from 19 programs that were developing software reported using COTS or GOTS software.[81] In total,

[79]DOD, *Business System Requirements and Acquisition*, Instruction 5000.75 (Washington D.C.: January 2020).

[80]Department of Defense, *Defense Acquisition Guidebook* (Washington, D.C: September 2020).

[81]We did not collect documentation to validate program responses to the software portion of our questionnaire.

officials from the 22 major business IT programs reported using a variety of software types. As reported by the officials,

- 15 programs were using COTS with DOD specific customizations.
- 1 programs were using COTS software with no DOD-specific modifications.
- 6 programs were using GOTS software with DOD-specific customizations.
- 1 program was using GOTS software with no DOD-specific modifications.
- 4 programs were using custom software with commercial hardware.
- 0 programs were using custom software running on custom hardware.
- 2 programs were using another kind of software.[82]

Programs Reported Using a Variety of Iterative Software Processes

Programs reported using a variety of iterative software processes that could result in cost or schedule benefits. In February 2018, the Defense Science Board[83] recommended that DOD implement certain iterative software development processes for its IT programs. According to the Defense Science Board report, some software development practices, like the use of a "software factory"[84] and continuous iterative development, could yield cost and schedule benefits for software-intensive DOD acquisition programs. Table 10 describes these iterative software development practices and shows the iterative software

[82]We asked program officials to select from the following list of software types: COTS software with DOD-specific customization needed, including reports, interfaces, conversions, extensions, and configurations; COTS software with no DOD-specific modifications or maintenance over the life cycle of the product; GOTS software with DOD-specific customization needed, including reports, interfaces, conversions, extensions, and configurations; GOTS software with no DOD-specific modifications or maintenance over the life cycle of the product; custom software running on commercial hardware and standard operating systems; custom software running on custom hardware; and other. We did not ask program officials the extent to which they intended to customize software.

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

[84]A software factory is a low-cost, cloud-based computing approach used to assemble a set of software tools enabling developers, users, and management to work together on a daily tempo.

development processes that officials from the 22 major business IT programs reported using.

Table 10: Officials from Major DOD IT Programs That Were Developing Software Reported Using Iterative Processes

Iterative development process	Description	Number of programs that reported using each process
Software factory	Low-cost, cloud-based computing used to assemble a set of software tools enabling developers, users, and management to work together on a daily tempo.	8 of 22
Delivery of minimum viable product, followed by successive next viable product	Development technique in which a new product or website is developed with sufficient features to satisfy early adopters.	13 of 22
Continuous iterative development	Way of developing software in smaller blocks that can be incrementally evaluated by a user community. This incremental approach allows updates and improvements to be rapidly incorporated into the software.	16 of 22
Iterative development training for program managers and staff	Service acquisition career managers develop a training curriculum to create and train a cadre of software-informed program managers, sustainers and software acquisition specialists.	12 of 22
Software documentation	Written text or illustration that accompanies computer software or is embedded in the source code.	18 of 22
Independent verification and validation for machine learning	Using machine learning in software systems coupled with independent testing to help monitor the systems.	5 of 22
None of the above		4 of 22

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

Eighteen Programs Reported Identifying a Minimum Deployable Product

In February 2018, the Defense Science Board recommended that all DOD software acquisition programs deliver a minimum deployable product.[85] Such a product follows a continuous iterative software development process that delivers a version with the minimum capabilities necessary to provide usable functionality to customers. One goal of developing a minimum deployable product is to enable users to evaluate the product's performance during use in order to create the basis of the next software iteration. According to the Defense Science Board, this allows developers to be better informed about users' evaluations and feedback on product performance.

[85]Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018). The Defense Science Board recommended that programs develop a minimum viable product. This term is equivalent to a minimum deployable product. Our questionnaire used the term minimum deployable product.

According to the Defense Science Board, managers and staff for programs that are not delivering a minimum deployable product are potentially at risk of being less informed about the extent to which their software is meeting user needs at early stages of the software development cycle. By not developing a minimum deployable product, programs could be at an increased risk of lengthy program failure due to product issues being found late in the development cycle as well as increased length of time to deliver value to users.

Consistent with the Defense Science Board's recommendation, officials from 18 of the 22 programs that were developing software reported that they had identified a minimum deployable, minimum releasable, or minimum viable product; officials from the remaining four programs reported that they were not. Eleven of the 18 programs reported that they had delivered this product.[86]

Eighteen Programs Reported Using an Iterative Software Development Approach

In February 2018, the Defense Science Board recommended that DOD acquisition program staff implement continuous iterative software development approaches, such as Agile, development and operations (DevOps), and DevSecOps and incremental.[87] The Defense Science Board describes iterative approaches as a way of breaking down the software development of a large application into smaller chunks. As discussed, DOD is working to transition to greater use of iterative software development, particularly using an Agile approach, based on legislative direction and internal policy changes.

According to the Defense Science Board, continuous iterative software development allows program staff to catch errors quickly and continuously, integrate new code with ease, and obtain user feedback throughout the application development process. This is in contrast to the more traditional software development approach, called waterfall. A

[86]The questions associated with this section and the preceding section's discussion of minimum viable products were different, which may result in programs providing different responses. Specifically, the question associated with these responses asked if programs had identified a minimum deployable, minimum releasable, or minimum viable product; and a follow-up asked if they had delivered this product. The question in the preceding section asked if programs were using the "Delivery of minimum viable product, followed by successive next viable product." Note that the terms minimum deployable, minimum releasable, or minimum viable product are often used interchangeably. See appendix II for the questionnaire that we provided to programs as part of this assessment.

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

waterfall approach uses linear and sequential phases of development that may be implemented over a longer period before resulting in a single delivery of software capability. Although a waterfall approach may be appropriate in some circumstances, in May 2019, the Defense Innovation Board concluded that iterative software development may reduce cost growth compared to a waterfall approach.[88]

Officials from 18 of the 22 programs that were developing software reported using at least one of the software development approaches that supports continuous, iterative development.[89] Conversely, officials from 11 programs reported that they were using a waterfall approach. In particular, three of the 11 reported that they were only using a waterfall approach and the remaining eight reportedly used waterfall in combination with an iterative approach, including Agile. Table 11 defines the software development approaches and shows the approaches that officials from the major business IT programs that were developing software reported using.

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

[89]The software development approaches are not mutually exclusive, and some program officials reported using multiple software development approaches.

Table 11: Officials from Major Business IT Programs That Were Developing Software Reported Using a Variety of Development Approaches

Approach	Description	Number of programs that reported using each approach[a]
Approaches that support continuous, iterative development		18 of 22
Agile	Software is delivered in increments throughout the project, but built iteratively by refining or discarding portions as required based on user feedback.	14 of 22
DevOps	This approach combines “development” and operations”, emphasizing communication, collaboration, and continuous integration between both software developers and users.	6 of 22
DevSecOps	This model combines “development,” “security,” and “operations,” and emphasizes communication, collaboration, and continuous integration between software developers and users.	5 of 22
Incremental	This model sets high-level requirements early in the effort and functionality is delivered in stages. Multiple increments each deliver part of the overall required program capability. Several builds and deployments are typically necessary to satisfy approved requirements.	11 of 22
Approaches that may or may not support continuous, iterative development		8 of 22[a]
Mixed	This approach is a combination of two or more different approaches.	8 of 22
Other	Other software development approach.	1 of 20[b]
Approach that likely does not support continuous, iterative development		11 of 22[a]
Waterfall	This approach uses linear and sequential phases of development that may be implemented over a longer period of time before resulting in a single delivery of software capability.	11 of 22

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

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

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

Sixteen Programs Reported Delivering Software At Least Every 6 Months

OMB guidance calls for certain agency CIOs and chief acquisition officers to ensure and certify that acquisition strategies and plans apply adequate incremental development, which OMB defines as planned and actual delivery of new or modified technical functionality to users at least every 6 months.[90] Additionally, the Defense Innovation Board calls for program staff using Agile and DevSecOps practices to deliver working software to users on a continuing basis—as frequently as every 2 weeks.[91] According to the Defense Innovation Board, if program officials do not allow for more

[90]At DOD, the USD(A&S) is the chief acquisition officer. OMB, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

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

frequent software delivery, they may lose opportunities to obtain information from users and face challenges when adjusting requirements to meet and adjust to customer needs.

Of the 22 programs that were actively developing software, officials from 16 programs reported delivering software functionality every 6 months or less, as called for in OMB's guidance. Officials from four programs reported that the average length of time between software releases was greater than 6 months.[92] Officials from the 22 major business IT programs reported that their programs delivered software as follows (the average length of time between releases): [93] As reported by the officials,

- 4 programs were delivering software functionality in less than 1 month.
- 8 programs were delivering software functionality between 1 and 3 months.
- 7 programs were delivering software functionality between 4 and 6 months.
- 1 program was delivering software functionality between 7 and 9 months.
- 3 programs were delivering software functionality between 10 and 12 months.
- 1 program was delivering software functionality in more than 13 months.
- 3 programs reported "N/A or don't know."[94]

Twenty-one Programs Reported Using an Approved Cybersecurity Strategy

DOD Instruction 8500.01, *Cybersecurity*, requires that DOD major IT program officials use approved cybersecurity strategies.[95] The approved strategies are to include information such as cybersecurity and resilience

[92]Officials from one program reported multiple average lengths of time between releases, including both less than and greater than every six months.

[93]Some programs reported multiple average lengths of time between software releases.

[94]"N/A or don't know" was a single option provided to program officials. Officials from one program that selected this option reported that it is changing the frequency of its releases, and officials from another reported that its users may not have access to capabilities for a long time after developers release new software. Officials from the third program reported that they were only planning one software release.

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

requirements and key system documentation for cybersecurity testing and evaluation analysis and planning. These strategies are intended to help ensure that program staff are planning for and documenting cybersecurity risk management efforts, which begin early in the programs' life cycle.

According to DOD Instruction 8500.01, if cybersecurity risk management is not undertaken early in the system development, programs are at risk of increased costs, schedule delays, and a negative impact on the performance of the system. Additionally, incorporating cybersecurity practices early in the development cycle makes it easier and less costly for a program to effectively manage cybersecurity risks.

Officials from 16 of 22 programs developing software reported having an approved cybersecurity strategy, and officials from five programs reported that they plan to have one.[96] The remaining program reported not using or planning to have an approved cybersecurity strategy.[97]

Programs Reported Conducting a Variety of Cybersecurity Assessments

DOD Instructions 5000.02T and 5000.75 require that business IT program staff conduct a cybersecurity vulnerability assessment.[98] Assessments for potential cybersecurity vulnerabilities should be included in programs' cybersecurity testing and assessment processes. These assessments include cooperative vulnerability identification and a cooperative vulnerability and penetration assessment, but program staff may also conduct other types of assessments.[99]

According to DOD's test and evaluation guidebook, cybersecurity testing and evaluation is intended to identify and mitigate exploitable system

[96]We did not collect documentation to validate program responses to the cybersecurity portion of our questionnaire.

[97]Officials from this program reported that they do not use an approved cybersecurity strategy because the program is a collection of previously independent applications, systems, and networks and was thus not required to develop a cybersecurity strategy. However, DOD 5000.82 requires that all acquisitions of systems containing IT have a cybersecurity strategy.

[98]DOD, *Business System Requirements and Acquisition*, Instruction 5000.75 (Washington D.C.: January 2020).

[99]DOD, *Operation of the Defense Acquisition System*, Instruction 5000.02T Change 9 (Washington D.C.: November 2020).

vulnerabilities.[100] The guidebook notes that early discovery of system vulnerabilities can facilitate remediation and reduce impact on program cost, schedule, and performance.

Officials from 15 of the 16 programs that were developing software and reported having cybersecurity strategies also reported that they conducted a cybersecurity vulnerability assessment.[101] These included assessments such as table top exercises, where staff talk through how they would respond to simulated scenarios, and full system assessments, where tests are conducted on complete systems. Table 12 summarizes the cybersecurity assessments that officials from major business IT programs that were developing software reported using.

Table 12: Officials from Major DOD IT Programs Reported Conducting Various Cybersecurity Assessments

Assessment type	Assessment description	Number of programs that conducted each type of assessment (out of 16 total)
Table top assessment	An assessment that brings people together to talk through how they would respond to simulated scenarios and often involve small collaborative teams that prepare briefings on notional threat scenarios. Based on those results, officials can create a path forward for addressing those scenarios, which could include administering additional testing, conducting follow-on analysis, or accepting the risk posed by the threat.	12 of 16
Full-system assessment	A test performed on a complete system to evaluate its compliance with specified requirements	11 of 16
Component assessment	A test of individual hardware and software components or groups of related components.	10 of 16
Cooperative assessment	Tests by assessors in which program office representatives, including developer support, are encouraged to participate to observe and characterize vulnerabilities, potential exploits, and follow-on fixes that may be needed. These assessments may involve any number of cybersecurity test events, such as system and network scans, vulnerability validation, penetration tests, access control checks, physical inspection, personal interviews, and reviews of system architecture and components	10 of 16
Assessment during operational testing	A vulnerability assessment conducted on production systems that supports the evaluation of system effectiveness, suitability, and survivability.	10 of 16
Assessment during developmental testing	A vulnerability assessment conducted early in the system lifecycle intended to identify cybersecurity issues and vulnerabilities, facilitate remediation, and reduce impact on cost, schedule, and performance.	8 of 16

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

[101]We only asked program officials to respond to this question if they reported having developed an approved cybersecurity strategy.

Assessment type	Assessment description	Number of programs that conducted each type of assessment (out of 16 total)
Adversarial assessment	A cybersecurity developmental test and evaluation activity that uses realistic threat exploitation techniques in representative operating environments to evaluate a system's cyber survivability and operational resilience in a mission context.	8 of 16
Penetration test	A penetration test, which may or may not be conducted as part of a cooperative assessment, is a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.	7 of 16
Other		4 of 16

Source: GAO analysis of Department of Defense IT program data; Department of Defense Cybersecurity Test and Evaluation Guidebook; National Institute of Standards and Technology Special Publication 800.53 | GAO-21-351

Note: Some program officials reported using more than one type of assessment; not all program officials responded to every question.

Programs Reported Conducting Required Developmental and Operational Cybersecurity Testing

DOD Instruction 5000.02T[102] required that DOD major business and non-business IT program staff complete both developmental and operational cybersecurity testing.[103] Developmental cybersecurity testing and evaluation is intended to identify cybersecurity vulnerabilities before program deployment, whereas cybersecurity operational testing evaluates operational programs. However, program staff can perform other developmental and operational cybersecurity assessments.

According to the DOD C*ybersecurity Test and Evaluation Guidebook*, not performing developmental testing increases risk of cost and schedule growth and poor program performance.[104] In addition, according to the

[102]DOD issued DOD Instruction 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers*, on December 31, 2020. This instruction incorporated and cancelled Enclosure 13 of DODI 5000.02T, which required developmental and operational cybersecurity testing for major IT programs. Programs in this assessment provided questionnaire responses before December 31, 2020. However, developmental and operational cybersecurity testing is still required under DODI 5000.89, *Test and Evaluation*.

[103]According to DOD's *Cybersecurity Testing and Evaluation Guidebook*, operational cybersecurity testing supports the evaluation of system effectiveness, suitability, and survivability. Developmental testing identifies cybersecurity issues and vulnerabilities early in the system lifecycle in order to facilitate the remediation and reduction of impact on cost schedule and performance. Department of Defense, *Cybersecurity Test and Evaluation Guidebook* Version 2.0, Change 1 (Washington, D.C., February 10, 2020).

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

guidebook, not performing operational testing increases the risk of program staff not resolving operational cybersecurity issues.

Officials from 20 of the 22 programs included in our assessment that were developing software reported conducting either developmental cybersecurity testing, operational cybersecurity testing, or both. In particular, 16 programs reported conducting developmental cybersecurity testing and 15 programs reported conducting operational cybersecurity testing. Eleven programs reported conducting both developmental and operational cybersecurity testing and 2 programs reported conducting neither developmental nor operational testing. These programs either had not reached the developmental or operational stages of cybersecurity testing or program officials did not report plans to conduct these tests. Table 13 identifies the extent to which program officials reported conducting cybersecurity developmental and operational testing.

Table 13: Officials from Major DOD IT Programs Reported Conducting Developmental and Operational Cybersecurity Testing

Testing phase and number of programs that reported conducting assessments associated with each phase	Assessment conducted	Assessment definition	Number of programs conducting assessments (out of 22 total)
Developmental testing 16 of 22	Cooperative vulnerability and identification	Cooperative vulnerability identification is a cybersecurity developmental test and evaluation activity that collects data needed to identify vulnerabilities and plan the means to mitigate or resolve them, including system scans, analysis, and architectural reviews.	8 of 22
	Adversarial assessment	An adversarial cybersecurity developmental test is a cybersecurity developmental test and evaluation activity that uses realistic threat exploitation techniques in representative operating environments.	4 of 22
	Other kind of assessment		9 of 22
	No assessments		5 of 22
Operational testing 15 of 22	Cooperative vulnerability and penetration assessment	A cooperative vulnerability and penetration assessment examines a system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities	8 of 22
	Adversarial assessment	An adversarial assessment assesses the ability of a system to support its mission while withstanding cyber threat activity representative of an actual adversary.	7 of 22
	Other kind of assessment		6 of 22
	No assessments		7 of 22
Neither developmental nor operational testing			2 of 22

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

Note: Some program officials reported using more than one type of assessment.

Appendix II is the questionnaire that we provided to program officials.

Major Business IT Programs in Active Development Reported Various Challenges with Software Development

In May 2019, the Defense Innovation Board reported that defense software programs are challenged in recruiting, retaining, managing, and developing a software development workforce.[105] Of the 22 programs that were developing software, officials from 18 reported that they faced software development workforce challenges, consistent with the Defense Innovation Board's reported challenges.[106] Table 14 summarizes the programs' reported challenges with government and contractor software development staff.

Table 14: DOD IT Program Officials Reported Challenges with Software Development Staffing

	Number of programs that reported experiencing challenges	
Challenge	**with government staff**	**with contractor staff**
Concurrency/overlap in staff	11 of 22	13 of 22
Difficult to find staff with required expertise	12 of 22	13 of 22
Difficult to hire enough staff to complete software development	9 of 22	13 of 22
Difficult to hire staff in time to perform planned work	10 of 22	14 of 22
Difficult to obtain necessary staff training	6 of 22	5 of 22
Software engineering staff plans were not realized as expected	10 of 22	13 of 22
Other	4 of 22	2 of 22

Source: GAO analysis of Department of Defense IT program data. | GAO-21-351

As of January 2021, DOD OCIO officials told us that they have efforts in place to address software development and cybersecurity workforce challenges. For example, the officials reported that they are tracking workforce metrics for software developers. In addition, the officials reported that the Cyber Excepted Service Targeted Local Market

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

[106]Program officials provided responses to a list of six challenges. Program officials were also given the opportunity to identify challenges that were not already listed.

Supplement[107] is planned to increase the basic pay of software developers to more closely match private-sector salaries. These officials added that Section 230 of the NDAA for FY 2020 requires DOD to measure and report on metrics related to the capability, capacity, utilization, and readiness of software development staff to develop and deliver operational capabilities and employ modern business practices.[108] They noted that how DOD will address this requirement is under discussion with the new administration.

Officials from the Office of the USD(A&S) added that most program staffing challenges are handled within the services and agencies. Nevertheless, they stated that USD(A&S) has worked with the Defense Digital Service, the Office of the Under Secretary of Defense for Research and Engineering, the DOD CIO, the Office of the Under Secretary of Defense for Personnel and Readiness, and the military departments to develop a plan to address challenges regarding recruiting, developing, and retaining DOD's software development workforce. They added that the Office of the USD(A&S) is also currently developing a strategy to identify and address gaps in software development training, and that the Defense Acquisition University (DAU) plays a key role in this effort.[109] A&S officials stated that DAU has trained over 1,400 personnel in Agile software practices and is working with DOD to create additional courses and webinars to train software development staff in modern software development practices.

In addition, officials from the 22 programs that were developing software reported experiencing significant non-staff challenges related to their software development efforts. For example:

- Four programs reported a number of challenges associated with managing both waterfall and Agile approaches. Notably, officials from

[107]According to DOD Instruction 1400.25, Volume 3006, *DOD Civilian Personnel Management System: Cyber Excepted Service (CES) Compensation Administration*, the Targeted Local Market Supplement is a type of local market supplement that may be implemented within the CES pay band and grade structure in appropriate circumstances. Local market supplements adjust pay band and grade rates and reflect the difference between the CES base rate structure and the competitive requirements for the labor market in the CES locality area.

[108]Pub. L. 116-92 § 230, 133 Stat. 1197, 1274 (December 20, 2019).

[109]Some of DOD's efforts to recruit, develop, train, and retain software staff are detailed in A&S's Software Development and Software Acquisition Training and Management Programs, a report required under Section 862 of the *NDAA for FY 2020*.

all four of these programs reported difficulty 1) committing to more timely and frequent user input, 2) adopting new Agile tools in a timely manner, and 3) establishing and maintaining technical environments that support Agile. Officials from three of the four programs also reported that Agile guidance was not clear. In addition, officials from one program reported that its software development teams had difficulty transitioning to self-directed work under Agile.

- Two programs reported that transitioning from waterfall to Agile software development was a challenge.
- One program reported that it relied on enterprise tools and environments that were not ready to support software development.
- One program reported that it had issues with the stability of its development and test environment.

Additional challenges reported by program officials included competing and concurrent requirements from separate customers or stakeholders; integrating the core application with third party applications; software obsolescence; and administrative restrictions associated with a change in fiscal years.

Regarding the challenges associated with transitioning to greater use of Agile software development, as discussed in this report, officials from the office of the DOD CIO and USD(A&S) stated that department is aware of the challenges associated with this transition. The officials also stated that many of DOD's implementation efforts, previously discussed in this report, have not been fully implemented or adopted across DOD. They noted that DOD is continuing work to address them and acknowledged that DOD's transition to Agile will take years and require sustained engagement throughout DOD.

DOD Has Taken Steps to Improve How It Manages Software Investments, but More Remains to Be Done

Since December 2019, DOD has made organizational and policy changes intended, in part, to improve how the department manages its software investments. These changes include taking steps to improve DOD's transition to Agile software development and improve oversight of its acquisition programs. DOD has made progress in each of these areas, but more remains to be done.

DOD Has Not Fully Implemented Best Practices in Its Transition to Agile Software Development, but Has Additional Work Underway

As discussed previously, DOD has implemented legislative[110] and policy changes to enable and encourage Agile software development.[111] While DOD has taken initial steps to implement Agile throughout the department, many of the 18 of 29 programs in our review that reported implementing this software development approach indicated that the department had not sufficiently implemented Agile transition best practices. These programs added that they had encountered challenges with Agile software development.

DOD's Agile Programs Reported That the Department Had Not Sufficiently Implemented Agile Best Practices

Many of the 18 major DOD IT programs that reported using Agile reported that the department had implemented activities associated with the best practices described in the September 2020 GAO *Agile Assessment Guide*[112] to only some or little to no extent—thus, indicating that DOD had not sufficiently implemented the Agile best practices.[113] Specifically, a majority of the programs reported that

- DOD had only implemented the best-practice activities associated with helping to ensure the organizational environment supports Agile development to either some or little to no extent for six of the seven related best practices activities;
- DOD had only implemented the best-practice activities associated with helping program operations support Agile development only to some or little to no extent for five of the seven related best practices activities; and
- DOD had only implemented the best-practice activities associated with helping to ensure team activities and dynamics support Agile

[110]The earliest legislative changes we reviewed for this report were included in the NDAA for 2018, Pub. L. No 115-91, 131 Stat. 1283 (December 12, 2017). Our review focused on legislation associated with organizational and policy changes that have occurred since December 2019.

[111]While this report refers to Agile software methodologies, the department also has efforts strengthening DevSecOps methodologies. Since DevSecOps is another form of modern iterative development, we include resources the department released to help support DevSecOps as steps the department has taken to implement Agile.

[112]GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C., September 28, 2020). GAO released the *Agile Assessment Guide* as an exposure draft for public comments on September 28, 2020. Also see GAO-20-213.

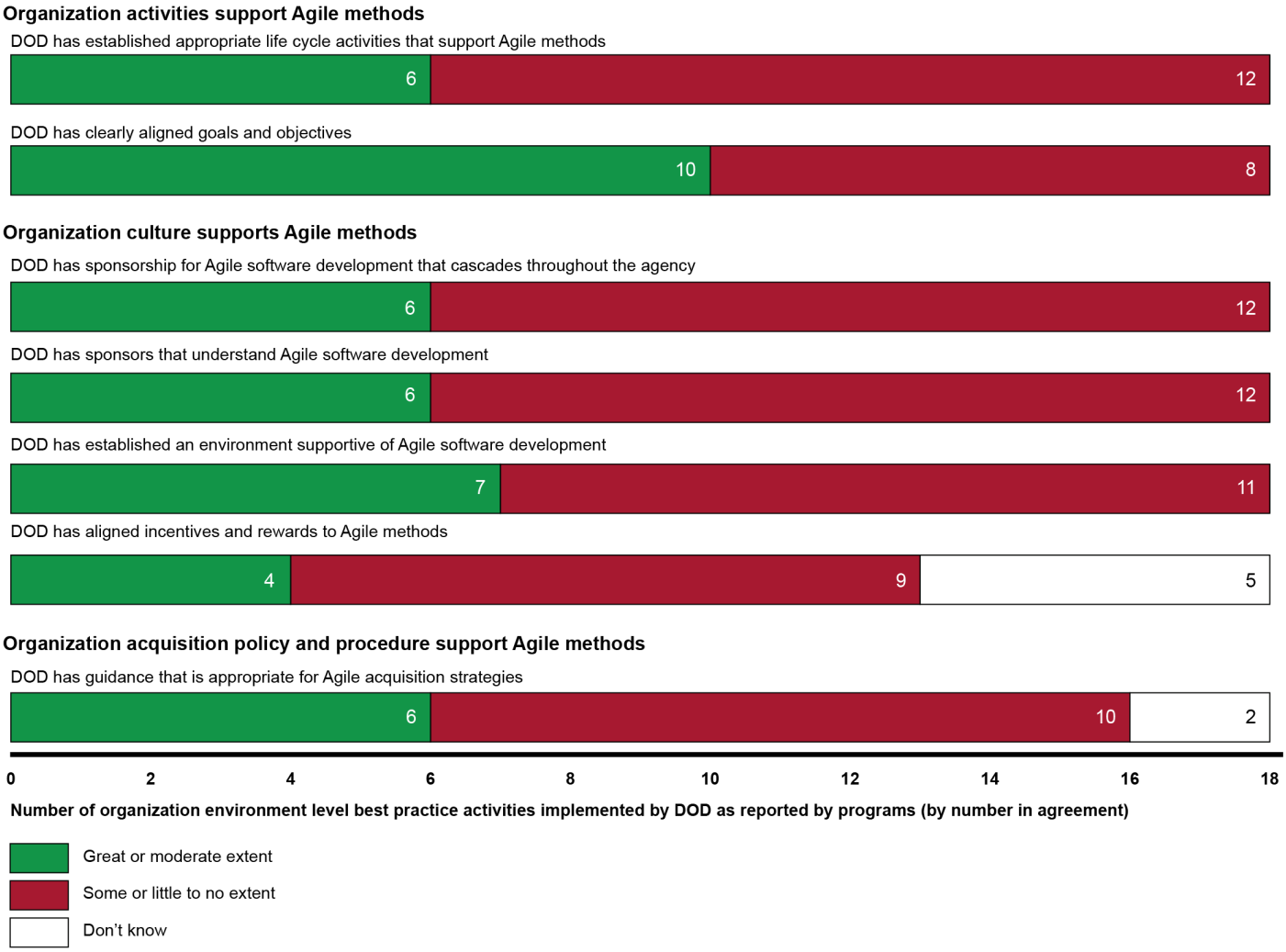
[113]We only included responses for programs that were currently using Agile. One program that is planning to transition to Agile, but has not yet done so, responded to the questions on DOD's implementation of Agile transition best practices, but we removed these responses from our assessment.

development only to some or little to no extent for seven of the ten related best practices activities.

Organization Environment

The 18 programs that reported using Agile generally indicated that DOD had not adequately implemented activities associated with the organization environment level best practices. In particular, the majority of these programs reported that DOD had implemented the best-practice activities to either some or little to no extent for six of the seven related activities. For example, 12 of the 18 programs reported that DOD's life-cycle activities supported Agile methods to some or little to no extent. Figure 5 summarizes the programs' responses regarding DOD's implementation of organization environment level best practice activities.

Figure 5: Extent to Which DOD Has Implemented Organization Environment Level Best Practice Activities, as Reported by Programs (by number in agreement)



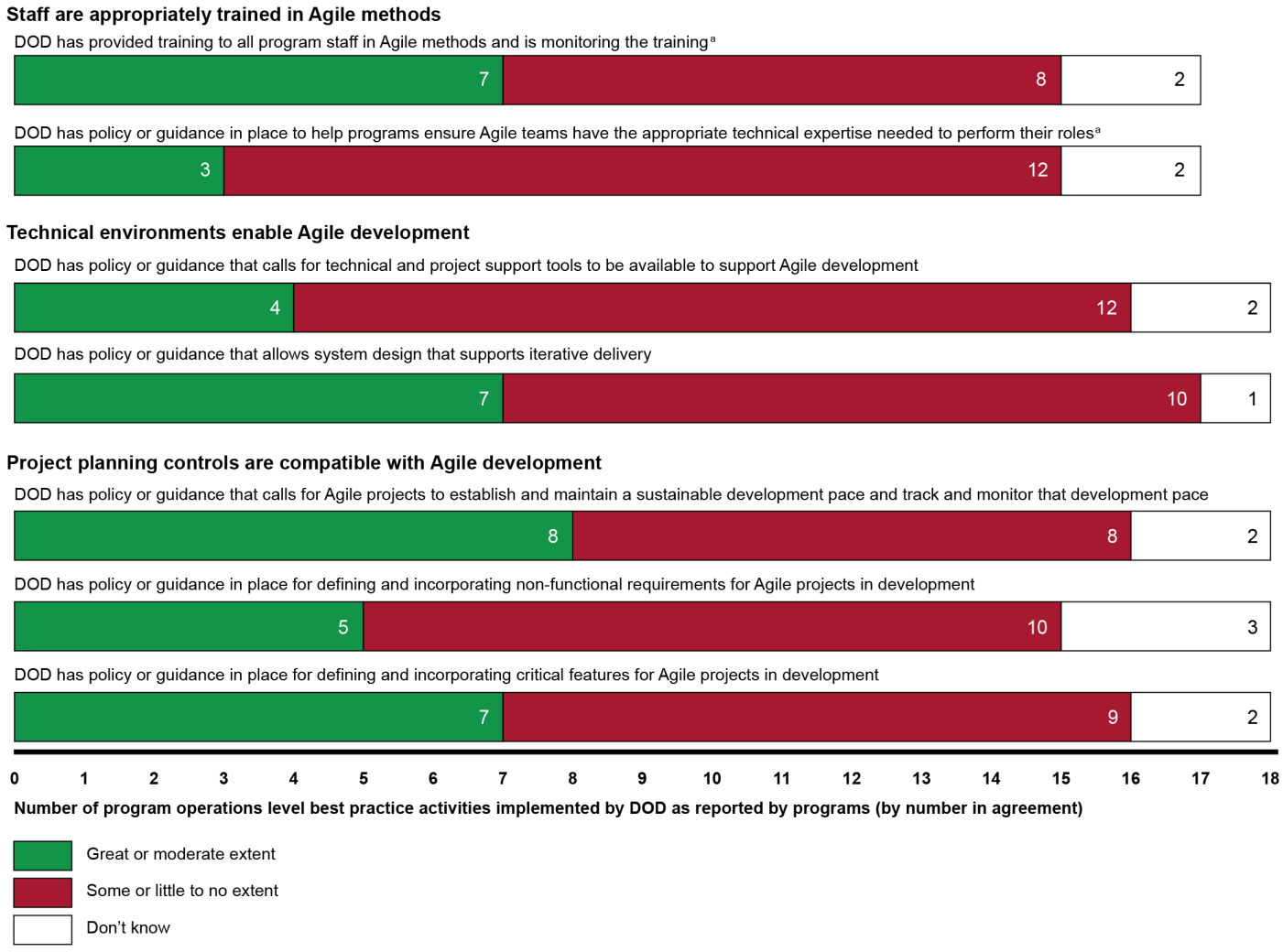
Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

Program Operations

Programs that reported using Agile indicated that DOD had not sufficiently implemented activities associated with the program operations level best practices. A majority of programs reported that DOD implemented five of the seven activities only to some or little to no extent. Between eight and 12 programs reported that DOD implemented best practices to some or little to no extent for all seven activities. For example, 12 of the 18 programs reported that DOD had some or little to

no policy or guidance in place to help programs ensure Agile teams have appropriate technical expertise. In addition, 12 programs reported that DOD had some or little to no policy or guidance that calls for technical and project support tools to be available to support Agile development. Figure 6 summarizes the programs' responses regarding DOD's implementation of program operations level best practice activities.

Figure 6: Extent to Which DOD Has Implemented Program Operations Level Best Practice Activities, as Reported by Programs (by number in agreement)



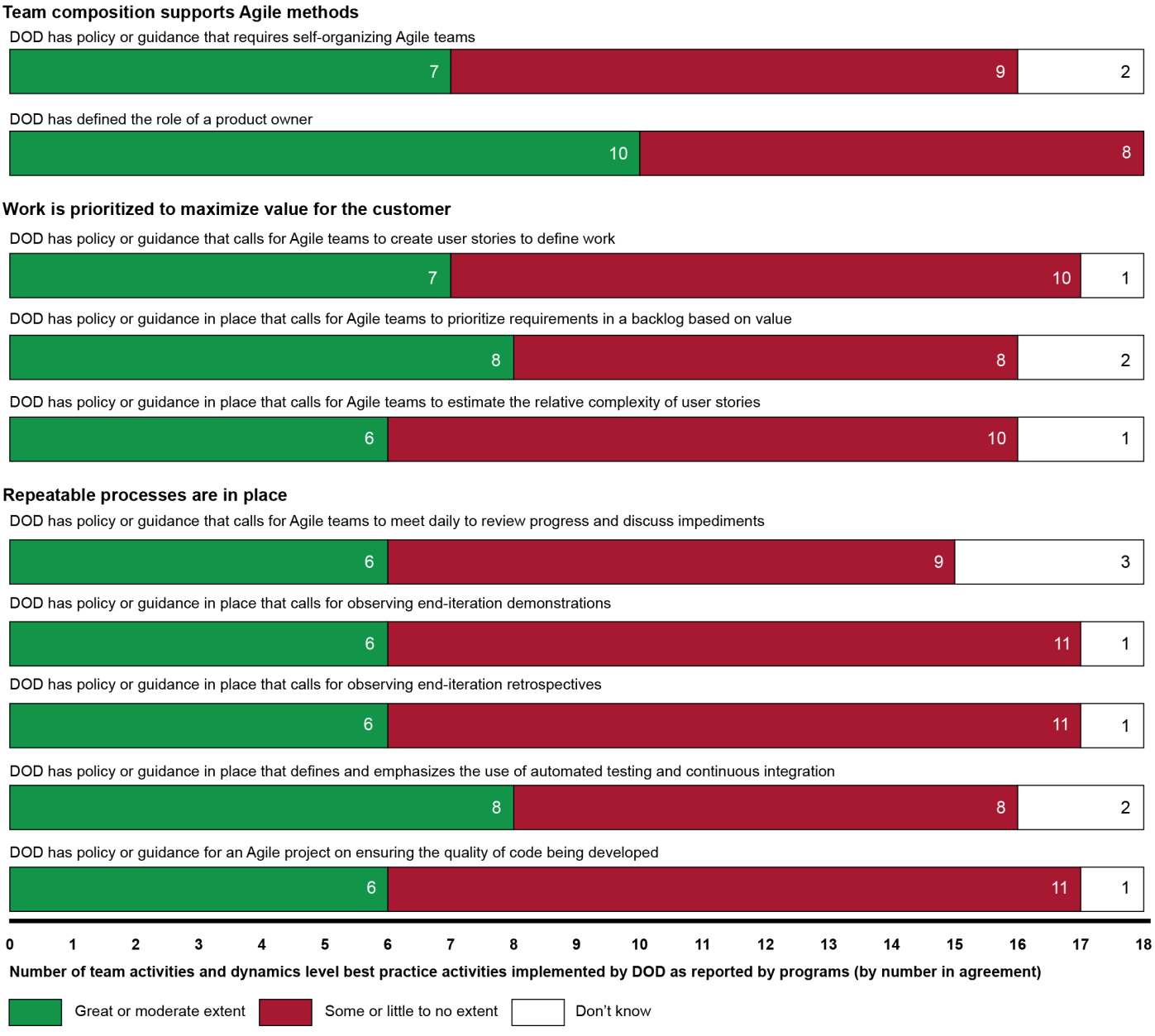
Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

[a]One program responded "not applicable" to two of these questions, and we removed these responses from our assessment. As a result, total responses for all questions do not add to 18.

Team Activities and Dynamics

Programs that reported using Agile indicated that DOD had not sufficiently implemented activities associated with the team activities and dynamics level best practices. For seven of 10 activities, a majority of programs reported that DOD had implemented the activity to only some or little to no extent. For example, 11 programs reported that DOD had policy or guidance in place that calls for observing end-iteration demonstrations to either some or little to no extent. In addition, 11 programs reported that DOD had some or little to no policy or guidance for an Agile project to ensure the quality of code being developed. Figure 7 summarizes the programs' responses regarding DOD's implementation of team activities and dynamics level best practice activities.

Figure 7: Extent to Which DOD Has Implemented Team Activities and Dynamics Level Best Practice Activities, as Reported by Programs (by number in agreement)



Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-351

DOD's Agile Programs Reported Challenges Associated with the Transition

As of December 2020, the 18 programs that reported they were currently using Agile and one program that previously used Agile reported experiencing challenges with Agile software development.[114] The most frequently cited challenge was that traditional artifact reviews did not align with Agile (13 programs). In addition, many of the programs reported challenges associated with procurement practices that may not support Agile projects (11 programs); traditional status tracking that did not align with Agile (11 programs); technical environments that were difficult to establish and maintain (11 programs); and difficulty with timely adoption of new tools (10 programs). Table 15 shows the number of programs that faced specific Agile software development challenges.

Table 15: Major Department of Defense IT Programs Reported Challenges in Implementing Agile Software Development

Challenge	Faced the challenge	Did not face the challenge	Don't know
	Number of programs reporting on Agile development challenges, out of 19 total		
Traditional artifact reviews do not align with Agile	13	5	1
Procurement practices may not support Agile projects	11	5	3
Traditional status tracking does not align with Agile	11	6	2
Technical environments were difficult to establish and maintain	11	7	1
Timely adoption of new tools was difficult[a]	10	6	2
Compliance reviews were difficult to execute within an iteration time frame	9	7	3
Staff had difficulty committing to more timely and frequent input	9	8	2
Federal reporting practices do not align with Agile	8	5	6
Organization had trouble committing staff	7	9	3
Teams had difficulty collaborating closely	7	10	2
Agile guidance was not clear	7	10	2
Teams had difficulty managing iterative requirements	6	11	2
Customers did not trust iterative solutions	5	11	3
Teams had difficulty transitioning to self-directed work	4	12	3

Source: GAO analysis of DOD questionnaire responses. | GAO 21-351

[a]One program responded "not applicable" to one of these questions, and we removed that response from our assessment. As a result, total responses for all questions do not add to 19.

[114]We previously reported on these challenges in *Software Development: Effective Practices and Federal Challenges in Applying Agile Methods*, GAO-12-681 (Washington, D.C.: Jul 27, 2012).

Program officials also reported other challenges with the Agile transition. For example, officials from two programs stated that the interim software pathway provided little structural or governance guidance over Agile project management.[115] Another program stated that component-level policy might not exist or might conflict with DOD policy. The program explained that DOD's guidance on inheritance and reuse of certification and accreditation documentation[116] is rarely followed by the component, making it difficult for the program to execute DOD policy as written.

In addition, senior management staff from two programs participating in DOD's Section 873 Agile pilot programs stated that efforts from the Office of the USD(A&S) were helpful in their respective Agile transitions. [117] However, officials from these programs also reported encountering challenges outside of resources USD(A&S) could provide. For example, as of December 2020, the deputy product manager from one program stated that the program was locked into a waterfall development contract. An official from another program stated that other offices in DOD still expected the level of planning and reporting typical of waterfall programs.

Officials from the offices of the DOD CIO and USD(A&S), including officials involved in DOD's Software Modernization Initiative, stated that DOD is aware of these challenges and is continuing work to address them. The officials added that, while they plan to build on the momentum of their efforts to modernize DOD's people, processes, tools, and policies, they acknowledge that DOD's transition to Agile will take years and

[115]DOD subsequently updated this guidance. We did not ask for program feedback on this updated guidance.

[116]The certification and accreditation process, now covered by DOD's Risk Management Framework, requires systems document their security authorization process. Inheritance and reuse of that documentation allows programs to use systems or technical solutions that have already been authorized by a different DOD component without having to re-authorize that solution. For example, the Air Force provides pre-certified containers for programs to use without having to certify the containers themselves.

[117]Section 873 of the 2018 NDAA established a pilot program to transition major software-intensive systems to Agile over a 5-year period. Two defense business systems that were among the 29 programs in our review participated in the pilot program. DOD reported on the pilot program in Department of Defense, *Report to Congress on Section 869 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232): Status of Pilot Program Required Under Section 873 of the NDAA for FY18 (P.L. 115-91)* (Washington, D.C., April 2019). One of these two programs reported that it had not yet transitioned to Agile, so we did not include that program's responses as part of our evaluation of DOD's implementation of Agile best practices. Specifically, that program reported "not applicable" for each practice.

require sustained engagement throughout DOD. The officials also stated that many of DOD's implementation efforts, previously discussed in this report, have not been fully implemented or adopted across DOD. They stated that they plan to continue the multi-year effort required to transition DOD.

DOD Has Not Yet Fully Defined Its Plans for Improving Software Oversight

As discussed previously, since June 2020, DOD has issued a series of policies, memos, and plans intended to improve the sharing and transparency of data it uses to monitor its acquisitions. In particular, according to the Office of the USD(A&S)'s November 2020 proposal for reporting on acquisition programs and activities, DOD's owners of the acquisition pathways are to develop 1) a data strategy and 2) metrics to assess performance.[118] The Defense Innovation Board has also recommended that DOD remove manual reporting processes and begin collecting automated metrics from programs as part of a broader shift toward Agile software development.[119] DOD subsequently reported that it aims to minimize additional reporting and maximize efficiency through the use of automation and existing metrics.[120]

However, DOD does not have data strategies for the software and business system acquisition pathways and lacks a defined approach for automated data collection. Officials from USD(A&S) stated that they are working with stakeholders to finalize strategies for the software and business system acquisition pathways, and plan to implement them using the Defense Acquisition Visibility Environment (DAVE) and ADVANA[121] in FY 2021.

[118]Department of Defense, *Proposal for Reports on Acquisition Programs and Activities* (Washington, D.C., November 5, 2020).

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

[120]Department of Defense, *Report to Congress on Implementation of Authority for Continuous Integration and Delivery of Software Applications and Upgrades to Embedded Systems* (Washington, D.C., January 19, 2021).

[121]As discussed, ADVANA is a system used to analyze data across the department. DOD has proposed to expand the use of the system to include acquisition data. DOD plans to use DAVE to automatically retrieve acquisition data and ADVANA to analyze the data stored in DAVE. DOD plans to use both systems to implement its data and analytics strategy and provide automated acquisition data for all reporting programs, portfolios, and pathways within its adaptive acquisition framework.

As for pathway metrics, DOD officials provided draft metrics for the software acquisition pathway; however, while USD(A&S) officials said they plan to implement defense business system metrics, as of March 2021, they had not yet defined draft metrics for the defense business system pathway. DOD has also provided guidance to its programs that use Agile, encouraging them to use Agile-centric metrics.[122] While the draft metrics and related guidance are positive steps, they are not yet sufficient to assess the performance of DOD's acquisition pathways. In February 2021, officials said they are continuing to work with the programs and components to determine the right balance of reporting and measures that provide sufficient feedback at the enterprise-level and that they will continue to refine and adjust the metrics after implementing them in fiscal year 2021. They added that DOD plans to integrate these metrics (which DOD calls reporting elements) into DAVE and military service reporting systems and analyze them using ADVANA.

Regarding automation, DOD's planned efforts to assess its acquisition pathways using DAVE and ADVANA may help DOD automate its collection of metrics. According to the USD(A&S)'s data and analytics strategic implementation plan and USD(A&S) officials, USD(A&S) plans to automatically retrieve acquisition program data from component databases, as appropriate. However, as of February 2021, USD(A&S) had not yet defined what data will be automatically retrieved or how often it will be retrieved.

USD(A&S) officials stated in February 2021 that program management offices derive the most value from automated metrics and that metrics reported to programs' component oversight bodies and to USD(A&S) do not require the level of detail provided by automated metrics. In addition, they stated that different program contexts might cause automated metrics to lose meaning outside the program office unless supplemented with manual reporting. Officials also stated that they plan to iteratively improve the metrics and how they collect them, which may lead to potential improvements through automation. In the meantime, software performance metrics from automated feeds would be entered manually by programs for the foreseeable future. The officials stated that USD(A&S)

[122]Department of Defense, *Agile Metrics Guide: Strategy Considerations and Sample Metrics for Agile Development Solutions*, Version 1.1 (Washington, D.C., September 23, 2019). Practical Software & Systems Measurement, *PSM Continuous Iterative Development Measurement Framework*, Version 1.05 (Washington, D.C., June 15, 2020).

currently plans to get data from software pathway programs about every six months.

Until DOD defines and implements data strategies for the software and business system pathways, DOD risks not having timely quantitative insight into its acquisition reform efforts. As a result, its ability to measure and report on the full impacts of its efforts is currently limited. In addition, DOD will continue to be unable to take advantage of opportunities for continuously updated insight into programs to inform program and pathway oversight.

Moreover, if the data strategies for the business system and software pathways focus on automated data collection that meets the needs of programs, component decision authorities, OSD, and oversight bodies, DOD will be better positioned to meet its goals in a more efficient manner. With mature reporting based on automated data , DOD could reduce the reporting burden on programs, collect and share visible and accessible data, assess its efforts to implement Agile software development, and provide improved insight on programs to Congress.

DOD Plans to Take Steps to Address the Repeal of the Chief Management Officer Position

As discussed previously in this report, the NDAA for FY 2021 eliminated the DOD CMO position. The law also requires the Secretary of Defense to submit recommendations to Congress by January 2022 on appropriate legislative actions to carry out the repeal of the CMO position.

On January 11, 2021, the then-Deputy Secretary of Defense issued a memo outlining how some of the former CMO responsibilities are to be reorganized.[123] The memo called for several immediate changes, including:

- The DOD Comptroller is to establish an organization and capability responsible for, among other things, data analytics, ADVANA, and, in coordination with the CIO, business IT systems requirements;
- The Director of Cost Assessment and Program Evaluation, supported by DOD's Washington Headquarters Service, was to establish a working group by January 15, 2021, to develop a plan for each duty and responsibility that were previously assigned to the OCMO to be reassigned to a DOD official. The plan is to address the personnel,

[123]Department of Defense, *Disestablishment of the Chief Management Officer of the DOD and Realignment of Functions and Responsibilities* (Washington, D.C., January 11, 2021).

functions, and assets (including contact resources) of the OCMO, as appropriate.

- The Director of Cost Assessment and Program Evaluation, supported by DOD's Washington Headquarters Service, is to identify DOD issuances and other guidance that must be changed to implement the NDAA for FY 2021 provisions eliminating the OCMO.

In her February 2021 confirmation hearing, the new Deputy Secretary of Defense stated that she plans to review this transition of responsibilities and ensure that it occurs rapidly and smoothly.[124]

Conclusions

DOD relies heavily on the use of IT to protect the security of our nation. For FY 2021, the department requested approximately $37.7 billion for its unclassified IT investments. DOD plans to spend $12 billion on the 29 largest business IT systems between FY 2019 and FY 2022. However, since 1995, we have identified DOD's efforts to modernize its business systems as high risk, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments.

For its major business IT programs, DOD identified a range of program risk levels. However, our quantitative assessments reflected greater risk than reported by the department for almost half of the programs. Accordingly, programs could be understating risks, further increasing the chances of cost growth and schedule delays.

To DOD's credit, the selected major business IT programs are taking a variety of software development and cybersecurity actions that can mitigate risks to cost and schedule. These actions and other ongoing efforts have the potential to improve how DOD acquires and manages its IT systems. However, the department does not yet have a specific plan for how it will provide automated oversight of IT programs and portfolios. DOD's ability to oversee and manage these critical systems will be important to their success, as well as the department's future capabilities.

As DOD continues to implement its numerous reform efforts, it has multiple opportunities to improve the performance of its IT systems,

[124]United States Senate, *Hearing to Consider the Nomination of Honorable Kathleen H. Hicks to be Deputy Secretary of Defense* (Washington, D.C., February 2, 2021).

implement efficient and tailored oversight and management processes, and reduce risk across its systems.

Recommendations

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

The Secretary of Defense should direct the Chief Information Officer to revisit program risk ratings for its next submission to the federal IT Dashboard for the programs where the DOD CIO's program risk ratings indicated less risk than GAO's assessments of program risk. (Recommendation 1)

The Secretary of Defense should direct the Under Secretary of Defense for Acquisition and Sustainment, in consultation with appropriate internal and external stakeholders, to ensure the data strategies and data collection efforts for the business system and software acquisition pathways define, collect, automate, and share, with the appropriate level of visibility, the metrics necessary for stakeholders to monitor acquisitions and that are critical to the department's ability to assess acquisition performance. (Recommendation 2)

Agency Comments and Our Evaluation

DOD provided written comments on a draft of this report. In its comments, the department concurred with our recommendations. Specifically, the department stated that it planned to examine risk ratings for the programs where DOD's CIO risk ratings indicated less risk than GAO's assessment. In addition, the department stated that it had identified, and was in the process of finalizing, reporting information standards for each of its pathways, including the business and software acquisition pathways. Further, the department stated that USD(A&S) was collaborating with the services on short- and long-term plans for automating data implementation and collection for all Adaptive Acquisition Framework pathway core data standards. DOD's comments are reproduced in Appendix III.

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

If you or your staff members have any questions on matters discussed in this report, please contact me at (202) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Kevin Walsh
Director, Information Technology and Cybersecurity

List of Committees

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

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

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

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

Appendix I: Objectives, Scope, and Methodology

The *John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019* included a provision for GAO to conduct annual assessments of selected Department of Defense (DOD) information technology (IT) programs through March 2023.[1] Our specific objectives for this assessment were to: (1) summarize DOD's reported performance of its portfolio of IT acquisition programs and the reasons for this performance; (2) evaluate DOD's assessments of program risks; (3) summarize DOD's approaches to software development and cybersecurity and identify associated challenges; and (4) evaluate how selected organizational and policy changes may affect IT acquisitions.

To address the first objective, we initially considered the 31 major business IT programs that DOD had reported to the federal IT Dashboard as of September 9, 2020. We then excluded two of these programs: one program that DOD did not consider to be a business IT program and one program that DOD planned to retire in FY 2021. We selected the remaining 29 programs for our review. These included programs that support key areas such as personnel, financial management, health care, and logistics.

To determine how much money DOD spent in fiscal year 2019 and planned to spend between fiscal years 2020 and 2022, we reviewed DOD's fiscal year 2021 budget request documentation.[2] Based on information contained in that request, we calculated the total actual and planned expenditures for the programs during the 4 year period. We included in the calculation the amounts associated with planned Development, Modernization, and Enhancement (DME) and Operations and Maintenance (O&M) spending, for each program and for the portfolio of IT acquisition programs as a whole.

We also collected and analyzed key documents, reports, and artifacts pertaining to each program's lifetime cost and schedule estimates, including information such as acquisition program baseline reports, program schedules, and acquisition strategies and aggregated program office responses to a GAO questionnaire we developed and administered to all 29 programs in October 2020. Programs provided their responses

[1]Pub. L. No 115-232,§ 833, 132 Stat. 1636, 1858 (Aug. 13, 2018). This report is a companion to GAO-21-222, also issued under this mandate, which discusses major DOD IT systems and DOD weapon programs.

[2]Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year 2021 Budget Estimates* (February 2020).

between October 2020 and December 2020. The questionnaire included questions about program costs and schedule changes that had occurred since January 2019 and about the early impacts of the Coronavirus Disease 2019 (COVID-19) pandemic.

To assess the reliability of the budget data DOD reported in the department's IT budget request database[3] for the 29 selected programs, we compared it to planned cost information provided by the programs to identify any obvious inconsistencies. In addition, we sent program summaries to the 15 programs that had the highest planned expenditures over the four year period discussed in this report and asked program staff to review the summaries and confirm their accuracy. We also corroborated program office responses to our questionnaire with relevant program documentation and interviews with program office officials. We determined that the data were sufficiently reliable for our reporting purposes.

To help ensure the reliability of the data collected via our questionnaire, including questions associated with subsequent objectives, we took steps to reduce measurement error and non-response error. Specifically, we conducted four pretests of the questionnaire with three programs to ensure that the questions were clear, unbiased, and consistently interpreted.[4] The pretests allowed us to obtain initial program feedback and helped ensure that officials within each program understood each question. The questionnaire allowed respondents to submit their answers electronically. We determined that the data were reliable for the purposes of this report.

For the second objective, we obtained and analyzed program risk management plans and risk registers from 22 of the 29 programs to develop risk ratings for the acquisitions and compared our analysis to DOD CIO-reported program risk ratings.[5] We also collected from the

[3]The Select and Native Programming-IT system is a database application used to collect and assemble information required in support of the IT budget request submitted to Congress. For example, it is used to generate DOD's IT-1 Report. DOD also uses the system to report its IT budget data on the IT Dashboard.

[4]We conducted two pretests with the same program.

[5]The remaining seven programs lacked a risk register, were not tracking active risks, or did not provide likelihood and consequence scores with reported risk items. This is in accord with DOD's risk-management guidance, which does not require programs to maintain a risk register.

federal IT Dashboard information about DOD chief information officer (CIO) risk ratings for the 29 selected programs, as of December 2020.[6] We then analyzed the program risk registers to develop risk ratings for the acquisitions and compared those ratings to the DOD CIO risk ratings.

Specifically, to determine the extent to which the program risk ratings we calculated were consistent with associated CIO risk ratings reported on the federal IT Dashboard, we met with staff from the Office of the DOD Chief Information Officer (OCIO) to discuss their program risk rating process and collected relevant information, such as DOD and Office of Management and Budget (OMB) guidance for calculating risk ratings for the federal IT Dashboard. We also collected information about program risk ratings from the federal IT Dashboard and from the 29 programs included in our scope.

We reviewed CIO risk ratings that were reported on the Dashboard as of December 2020. Those risk ratings were as of April 2020 and, as of February 2021, programs had not reported updated risk ratings to the Dashboard. We also obtained risk management plans and risk registers that programs provided between October and December 2020.

According to OMB guidance for CIO evaluation reports, CIO's should consult with appropriate stakeholders and provide numeric evaluations that reflect the CIO's best judgment of the current level of risk for an investment in terms of its ability to accomplish its goals.[7] Further, OMB's guidance states that these evaluations should be informed by factors, including but not limited to: risk management, requirements management, contractor oversight, historical performance, human capital, and other factors that the CIO deems important to forecasting future success.

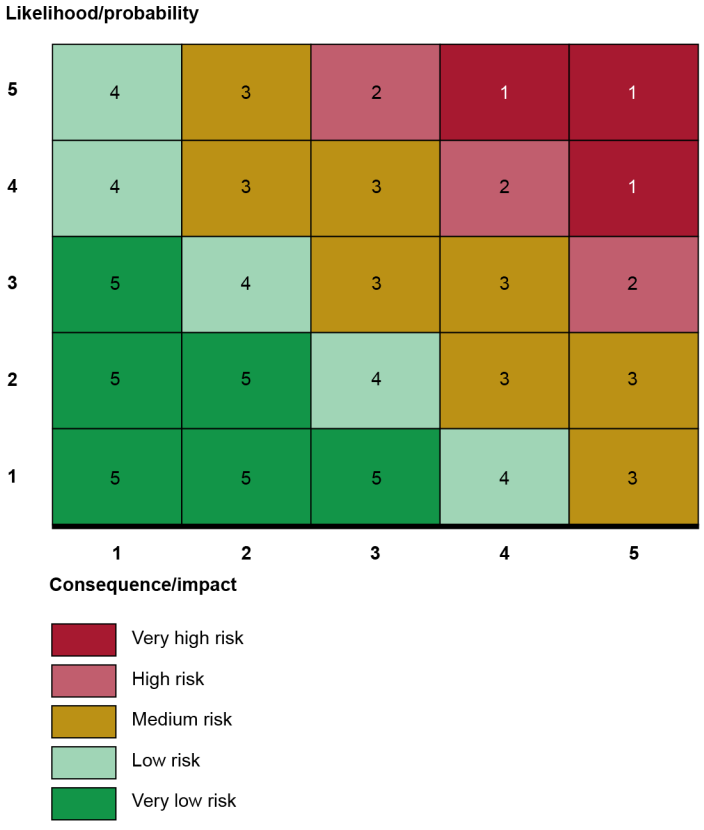
Regarding risk registers, DOD guidance states that consistent predefined likelihood and consequence criteria provide a structured means for

[6]As of December 2020, DOD CIO risk ratings were last updated on the federal IT Dashboard in April 2020. As of February 2021, programs had not reported updated risk ratings to the Dashboard. An official from the DOD OCIO stated that the office completed updated ratings in November 2020, but those had not yet been made public on the federal IT Dashboard. This official stated that the delay is due to the budget submission process being underway and the change in presidential administrations.

[7]Office of Management and Budget, *FY 2021 IT Budget–Capital Planning Guidance* (June 28, 2019).

evaluating risks.[8] According to DOD, once the analysis of likelihood and impact is complete, programs should use its risk matrix to convert the combination of likelihood and maximum cost, schedule, and performance impact scores to form a risk level (or risk exposure) score for each risk. Furthermore, DOD adds that while these values are used to define the risk level, additional factors should be considered such as the cost-effectiveness of perceived risk mitigation options, the frequency of occurrences, time frame, and interrelationship with other risks. Figure 8 shows DOD's matrix for using probability and impact values to determine risk exposure scores as well as the overall risk rating for a program.

Figure 8: Risk Exposure Scores Resulting from Department of Defense Probability and Impact Values



Source: DOD guidance and GAO analysis. | GAO-21-351

[8]Department of Defense, *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs* (Washington, D.C., January 9, 2017).

Note: Program risk registers used a 1-5 scale where 1 was the lowest value for likelihood and consequence, while the Office of Management and Budget used a scale where 1 was the highest value for risk and 5 was the lowest value.

To create our evaluations of risk, we used information contained in risk registers provided by 22 programs. The remaining seven programs lacked a risk register, were not tracking active risks, or did not provide likelihood and consequence scores with reported risk items.[9] Specifically, we combined the probability and impact of every active risk in the risk registers of each of the selected programs and used DOD's risk reporting matrix to determine what is known as the exposure of each risk.[10] Exposure scores, which were based on industry and government leading practices, as well as DOD's own guidance for managing risks, ranged "very low" to "very high."[11] Specifically, for each of the risk exposure scores, we assigned a 1 (very high risk) to 5 (very low risk) rating. We then averaged the numerical risk ratings to obtain an overall risk rating (or assessment) for the acquisition as a whole, which ranged from 1 (very high risk) to 5 (very low risk). This 1-5 rating scale is consistent with the scale that federal CIOs use for reporting program risk to the federal IT Dashboard. Table 16 shows how our overall program risk ratings corresponded to risk exposure ratings.

Table 16: Numerical Risk Ratings and Corresponding Risk Exposure Ratings

Numerical risk rating	Risk exposure rating
1	Very high
2	High
3	Medium
4	Low
5	Very low

Source: GAO analysis. | GAO 21-351

[9]This is in accord with DOD's risk management guidance, which does not require programs to maintain a risk register.

[10]According to the Software Engineering Institute, risk can be calculated as a combination of probability (or likelihood) and impact (or consequences). The institute gives credit for the formula to Barry W. Boehm. We used that formula to calculate risk exposure scores: risk exposure = likelihood of occurrence (probability) * loss due to undesirable outcome (impact).

[11]Exposure scores were based on SEI's risk calculations and OMB guidance, as well as DOD's risk management guidance.

We then averaged the combined risk exposure scores for each program, rounded the result to the nearest whole number to obtain an overall risk rating (or assessment) for the acquisition as a whole, and translated the result into green, yellow, and red grades as shown in table 17.

Table 17: Range of Risk Ratings and Corresponding Color

Risk rating range	Color
Greater than 3	Green
3	Yellow
Less than 3	Red

Legend: Red = high risk rating, Yellow = medium risk rating, Green = low risk rating

Source: GAO. | GAO 21-351

Table 18 shows how we would assess the following hypothetical program (Generic Investment) as having a risk rating that is medium risk (yellow).

Table 18: Example of Probability, Impact, Exposures, and Grading, based on the Evaluation of Risks for a Generic Investment

Individual risk	Probability	Impact	Risk exposure	Individual risk rating
Risk A	1	1	Very low	5
Risk B	2	2	Very low	5
Risk C	3	3	Medium	3
Risk D	4	4	High	2
Risk E	5	5	Very high	1
Risk F	5	4	Very high	1
Risk G	4	3	Medium	3
Risk H	3	2	Low	4
Risk I	2	1	Very low	5
Risk J	1	5	Medium	3
Average				3.2
Program risk rating				3 (medium risk)

Legend: Red = high risk rating, Yellow = medium risk rating, Green = low risk rating

Source: GAO. | GAO 21-351

We then compared our assessment to the CIO ratings on the Dashboard, and met with agency officials to discuss our findings and corroborate the Dashboard's data. Our calculations are only intended to provide a standardized view of risk across all the programs we reviewed. This

methodology is not intended to serve as a prescriptive approach to the agencies' evaluation of investment risk, rather a baseline metric for evaluating DOD's progress in mitigating these risk items moving forward.

For the third objective, we sought information on the software and cybersecurity practices used by the 29 selected IT programs via our questionnaire. Our identification of risks or challenges that might impact acquisition outcomes focused on the 22 programs' responses to the questionnaire that were actively developing software. For the purposes of this assessment, we considered programs to be developing software if they did not report being in the sustainment phase of acquisition, or if they reported being in sustainment but also reported being in another phase of acquisition.[12] We selected the topics of software development approaches and cybersecurity practices to help ensure consistency with companion work being conducted under this same provision in the NDAA for FY 2019 that focuses on the software development approaches and cybersecurity practices of DOD weapon programs.[13]

We aggregated program office responses and compared the aggregated information from our questionnaires to relevant guidance and leading practices[14] to identify where there were gaps. In doing so, we identified possible risks and challenges associated with not following guidance and leading practices that may affect acquisition outcomes relative to cost, schedule, and technical performance. We received responses to our program questionnaires from all of the programs we assessed between October and December 2020.

We did not validate the responses provided by the program offices, although we followed up with programs when responses were unclear or

[12]The 22 programs discussed in this section reported being in the development and production, deployment, and sustainment phases. Officials from some programs also reported being in other phases or a combination of multiple phases.

[13]GAO-21-222.

[14]GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C., Sept. 28, 2020); *Defense Science Board, Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019); Department of Defense, *Cybersecurity Test and Evaluation Guidebook* Version 2.0, Change 1, (Washington, D.C., February 10, 2020); Department of Defense, *Operation of the Defense Acquisition System*, Instruction 5000.02 (Washington, D.C., Jan. 23, 2020); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 (Washington, D.C., Jan. 24, 2020).

inconsistent. Where we discovered discrepancies, we clarified the responses accordingly. We also included the questionnaire that we provided to program officials in appendix II.

To develop the definitions for Agile software development and project management practices included this report, we first reviewed GAO's *Agile Assessment Guide*.[15] In developing this guide, GAO reviewed information related to Agile software development practices and compiled a draft of best practices commonly mentioned across different sources, and sent a draft set of Agile adoption best practices to a group of experts for review in advance of Agile expert working group meetings.

These meetings took place three times a year between August 2016 and August 2019, with approximately 400 experts participating. GAO received comments from some of these experts both during these meetings and by email after the meetings. We supplemented information from the GAO *Agile Assessment Guide* with information from the Project Management Institute's Agile Practice Guide.[16] *The Agile Practice Guide* was developed by experts from the Project Management Institute and the Agile Alliance. We also used information from Carnegie Mellon's Software Engineering Institute, National Institute of Standards and Technology reports, and prior GAO reports to develop definitions.[17]

To address the fourth objective, we reviewed selected IT-related organizational, policy, and statutory changes and reviewed 3rd party reports mandated by Congress, and DOD reports and documentation

[15]GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C., Sept. 28, 2020). GAO released the *Agile Assessment Guide* as an exposure draft for public comments on September 28, 2020.

[16]Project Management Institute, *Agile Practice Guide* (Washington, D.C.: September, 2017).

[17]GAO, *TSA Modernization: Use of Sound Program Management and Oversight Practices Is Needed to Avoid Repeating Past Problems*, GAO-18-46 (Washington, D.C.: Oct. 17, 2017); GAO, *Effective Practices and Federal Challenges in Applying Agile Methods*, GAO-12-681 (Washington, D.C.: Jul. 27, 2017); National Institute of Standards and Technology, *Vetting the Security of Mobile Applications*, NIST SP 800-163 (Gaithersburg, MD.: January 2015); Carnegie Mellon University, Software Engineering Institute, *The Importance of Software Architecture in Big Data Systems* (Pittsburgh, PA.: Jan. 13, 2014); Carnegie Mellon University, Software Engineering Institute, *Don't Play Developer Testing Roulette: How to Use Test Coverage* (Pittsburgh, PA.: Oct. 14, 2019); Carnegie Mellon University, Software Engineering Institute, *Design Research in the Context of Federal Law Enforcement* (Pittsburgh, PA,: Oct. 11, 2019); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (May 2019).

related to the effects of these changes on IT acquisitions. We selected the changes to review by identifying sections from the NDAAs for FYs 2018, 2019, 2020, and 2021 that pertained to IT acquisitions, acquisition reform efforts that impact IT acquisitions, or management of major business IT programs.[18] We then identified organizational and policy changes that have occurred since December 2019 that also affect IT acquisitions, acquisition reform efforts, or management of major business IT programs.[19]

Our efforts focused on organizational, legislative, and policy changes pertaining to DOD IT business systems and software systems. We also drew on our previous work with DOD's major IT systems to select additional key changes.[20] We selected the sections and policy changes to help ensure consistency with companion work conducted under this same provision of the NDAA for FY 2019. Specifically, we evaluated changes associated with DOD's efforts to transition to greater use of Agile software development, improve software oversight, and enact the statutory repeal of its CMO position. We selected these changes based on their importance to the programs covered within the scope of this assessment. We also coordinated with the GAO team conducting a companion assessment examining major defense acquisition programs that was conducted under this same provision of the NDAA for FY 2019.[21]

[18] Pub. L. No 115-91, 131 Stat. 1283 (December 12, 2017), Pub. L. No 115-232, 132 Stat. 1636 (August 13, 2018), Pub. L. No 116-92, 133 Stat. 1198 (December 20, 2019), Pub. L. No 116-283, 134 Stat. 3388 (January 1, 2021).

[19]Department of Defense, *Operation of the Adaptive Acquisition Framework*, Instruction 5000.02 (Washington, D.C., Jan. 23, 2020); Department of Defense, *Operation of the Defense Acquisition System*, Instruction 5000.02T [incorporating change 10 (Dec. 31 2020)] (Washington, D.C., Jan. 7, 2015); Department of Defense, *Business Systems Requirements and Acquisition*, Instruction 5000.75 [incorporating change 2 (Jan. 24, 2020)] (Washington, D.C., Feb. 2, 2017); and Department of Defense, *Operation of the Software Acquisition Pathway*, Instruction 5000.87 (Washington, D.C., October 2, 2020).

[20]GAO, *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, GAO-21-182 (Washington, D.C.: December 23, 2020); GAO, *Business Systems Modernization: DOD Has Made Progress in Addressing Recommendations to Improve IT Management, but More Action Is Needed*, GAO-20-253 (Washington, D.C.: March 5, 2020); GAO, *DOD Major Automated Information Systems: Adherence to Best Practices Is Needed to Better Manage and Oversee Business Programs*, GAO-18-326 (Washington, D.C.: May 24, 2018).

[21]GAO-21-222.

To understand and assess the potential implementation of these changes, we reviewed policies, plans, and guidance provided by DOD; reports that DOD submitted to Congress; and internal program documentation. We also interviewed officials within DOD's Office of the Chief Information Officer, Office of the Under Secretary for Acquisition and Sustainment, and Office of the Chief Management Officer. For this review, we assessed whether DOD had policies, plans, or guidance in place and whether they addressed topics required by legislation and/or department policy. We did not assess the effectiveness or quality of particular policies, plans, or guidance.

In addition, we aggregated program office responses to the questionnaire that pertained to DOD's implementation of Agile best practices to determine the extent to which DOD is taking steps to implement practices defined in GAO's *Agile Assessment Guide*.[22] Our questionnaire also asked these same programs, plus one program that reported previously using Agile, to identify which challenges they faced with Agile software development. We also met with staff within the DOD OCIO and the Office of the USD(A&S) to discuss program responses.

As discussed previously, we put our questionnaire through a quality assurance process. We also interviewed officials from two programs participating in the Section 873 Agile pilot to discuss the implications and challenges of their programs' transition to Agile.[23]

We used GAO's *Agile Assessment Guide* to highlight potential improvements or risks DOD may experience depending on a successful or incomplete transition, respectively. We used our interviews with department officials and understanding of DOD's implementation efforts to describe steps DOD is taking to successfully implement these changes.

We conducted this performance audit from July 2020 to June 2021 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

[22]GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C., September 28, 2020). GAO released the *Agile Assessment Guide* as an exposure draft for public comments on September 28, 2020.

[23]Section 873 of the 2018 NDAA established a pilot program to transition major software-intensive systems to Agile over a 5-year period.

findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Program Office Questionnaire

In October 2020, we distributed the following questionnaire to program officials associated with the 29 programs discussed in this report. Program officials provided responses to the questionnaire between October and December 2020.

2021 DOD IT Quick Look Assessment – 104440

United States Government Accountability Office
Software and Cybersecurity Questionnaire

The National Defense Authorization Act for Fiscal Year 2019 includes a provision for the Government Accountability Office (GAO) to conduct an assessment of selected Department of Defense (DOD) information technology (IT) programs annually through March 2023. As part of this review, GAO is disseminating this questionnaire to collect relevant information about software development and cybersecurity practices for your program.

Responses to the questionnaire will allow GAO to assess how major DOD IT programs are implementing various software development approaches and cybersecurity practices, to report on associated challenges and program risks, and to identify areas for inquiry in future Quick Look assessments. Responses to this questionnaire might be used to make recommendations to DOD; however, GAO does not intend to use program responses to make recommendations to individual programs. We ask program offices to answer the questions that follow as fully as possible.

We look forward to receiving your response to this questionnaire by **October 16, 2020.**

If you have questions or need clarification on any point related to the engagement, please contact your assigned analyst, engagement Analyst-in-Charge Tyler Mountjoy (MountjoyT@gao.gov), or Assistant Director Michael Holland (HollandM@gao.gov).

Thank you,
Tyler Mountjoy

1

Section I: Contact Information

1. **What is the name, title, and contact information of the person(s) with whom GAO should follow up on information provided in this questionnaire?**

Name(s):	Click or tap here to enter text.
Title(s):	Click or tap here to enter text.
E-mail Address(es):	Click or tap here to enter text.
Phone Number(s):	Click or tap here to enter text.

Section II: Program Profile

2. **What is the name of the program?** Click or tap here to enter text.

3. **Under which military department or Defense agency does the program fall?** Click or tap here to enter text.

4. **Where is the program's headquarters located?** Click or tap here to enter text.

5. **Who is the program manager?** *Please provide the program manager's name, organization, and title.* Click or tap here to enter text.

6. **Who is the milestone decision authority?** *Please provide the milestone decision authority's name, organization, and title.* Click or tap here to enter text.

7. **How would you describe the purpose of the program?** *Please describe the program briefly below and provide program documentation that supports this description e.g. APB, CDD or other document.*

   Click or tap here to enter text.

8. **Per DOD's Instruction 5000.02, which acquisition pathway(s) is the program using?** *Instruction 5000.02 establishes policies and procedures for managing DOD acquisition programs. Check all pathways that apply.*

Pathways	Yes	No	Don't Know
a. Urgent Capability Acquisition	☐	☐	☐
b. Middle Tier Acquisition	☐	☐	☐
c. Major Capability Acquisition	☐	☐	☐
d. Software Acquisition	☐	☐	☐
e. Defense Business Systems Acquisition	☐	☐	☐
f. Defense Acquisition of Service	☐	☐	☐
g. Other (*Please describe*): Click or tap here to enter text.	☐	☐	☐

2

9. Does the program involve software acquisition activities that are governed by, or were affected by, the following requirements? *(Select all that apply)*

Requirements	Yes	No	Don't Know
a. 10 U.S.C. § 2322a (Requirement for consideration of certain matters during the acquisition of noncommercial computer software)	☐	☐	☐
b. Section 800 of the National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116–92 (Continuous integration and delivery of software applications and upgrades to embedded systems)	☐	☐	☐
c. Section 873 of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115–91 (Pilot program to use agile or iterative development methods to tailor major software-intensive warfighting systems and defense business systems)	☐	☐	☐
d. Section 874 of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91 (Software development pilot program using agile best practices)	☐	☐	☐
e. Section 875 of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115–91 (Pilot program for open source software)	☐	☐	☐

Section III: Cost and Schedule

Please provide documentation to support responses to questions 10 through 21 below.

10. Which acquisition phase is the program in currently in?

☐ Development

☐ Production, Deployment, and Sustainment

☐ Mixed

☐ Other (*Please describe*): Click or tap here to enter text.

3

11. What is the most recent milestone the program has achieved? *If the program's most recent milestone applies to an acquisition pathway the program is no longer in, please select the name of this most recent milestone.*

- ☐ Need Identification (Material Development Decision)
- ☐ Solution Analysis ATP
- ☐ Risk Reduction Decision (Milestone A)
- ☐ Technology Maturation and Risk Reduction
- ☐ Functional Requirements ATP
- ☐ Requirements Decision Point (CDD Validation Decision)
- ☐ Development Request for Proposal (RFP) Release Decision
- ☐ Acquisition ATP
- ☐ Development Contract Award Decision or Development Decision (Milestone B)
- ☐ Limited Deployment ATP(s)
- ☐ Low-Rate Initial Production (LRIP) or Limited Deployment and Operational Test (Milestone C)
- ☐ Full Deployment ATP
- ☐ Full-Rate Production (Full Deployment Decision)
- ☐ Capability Support ATP
- ☐ Other (*Please describe*): Click or tap here to enter text.

12. When did the program achieve the milestone identified in question 11? *Please provide actual date.*
Click or tap here to enter text.

4

13. What is the next milestone the program plans to achieve?

- ☐ Need Identification (Material Development Decision)
- ☐ Solution Analysis ATP
- ☐ Risk Reduction Decision (Milestone A)
- ☐ Technology Maturation and Risk Reduction
- ☐ Functional Requirements ATP
- ☐ Requirements Decision Point (CDD Validation Decision)
- ☐ Development Request for Proposal (RFP) Release Decision
- ☐ Acquisition ATP
- ☐ Development Contract Award Decision or Development Decision (Milestone B)
- ☐ Limited Deployment ATP(s)
- ☐ Low-Rate Initial Production (LRIP) or Limited Deployment and Operational Test (Milestone C)
- ☐ Full Deployment ATP
- ☐ Full-Rate Production (Full Deployment Decision)
- ☐ Capability Support ATP
- ☐ Other (*Please describe*): Click or tap here to enter text.

14. When does the program plan to achieve the next milestone? *Please provide planned date.* Click or tap here to enter text.

15. If the program has not yet achieved full operating capability (FOC), full deployment Authority to Proceed (ATP), or an equivalent milestone, when does it plan to achieve it? Click or tap here to enter text.

16. What is the program's current expected fiscal year 2021 cost? Click or tap here to enter text.

17. What is the program's current planned total lifecycle cost, broken down by the following categories?

a. Research, Development, Testing and Evaluation:	Click or tap here to enter text.
b. Procurement:	Click or tap here to enter text.
c. Acquisition Operations and Maintenance:	Click or tap here to enter text.
d. Total Acquisition Cost:	Click or tap here to enter text.
e. Operations and Support:	Click or tap here to enter text.
f. Total Lifecycle Cost:	Click or tap here to enter text.

5

18. What is the date of the cost estimate associated with these costs? *Please provide date and a cost estimate that supports the above reported costs.* Click or tap here to enter text.

19. What is the base year for the cost numbers above? Click or tap here to enter text.

20. Has the program experienced changes to its planned cost since January 1, 2019?

☐ Yes (*Please describe the changes, the date(s) the changes occurred, and the reasons for the changes)*: Click or tap here to enter text.
☐ No

21. Has the program experienced changes to its planned schedule since January 1, 2019?

☐ Yes (*Please describe the changes, the date(s) the changes occurred, and the reasons for the changes)*: Click or tap here to enter text.
☐ No

Section IV: Software Development

For the purposes of this questionnaire, software development refers to developing, acquiring, configuring, sustaining, and/or managing any software product, including custom, GOTS, and COTS products. Question and answer applicability may vary based on acquisition phase and software type.

22. Which of the following best describes the type of software the program is developing? *(Select one)*

☐ Commercial off-the-shelf software with DOD-specific customization needed, including reports, interfaces, conversions, extensions, and configurations

☐ Commercial off-the-shelf software with no DOD-specific modifications or maintenance over the life cycle of the product

☐ Government off-the-shelf software with DOD-specific customization needed, including reports, interfaces, conversions, extensions, and configurations

☐ Government off-the-shelf software with no DOD-specific modifications or maintenance over the life cycle of the product

☐ Custom software running on commercial hardware and standard operating systems

☐ Custom software running on custom hardware

☐ Other (*Please describe*): Click or tap here to enter text.

23. Did the program incorporate a software factory as a key evaluation criterion in the source selection process?

☐ Yes
☐ No *(Please explain why not*): Click or tap here to enter text.

6

24. Does the program use the following development processes? *(Select all that apply)*
Note: The February 2018 Defense Science Board report on Design and Acquisition of Software for Defense Systems recommended these processes.

Development Processes	Yes	No	Not Applicable
a. Software Factory	☐	☐	☐
b. Delivery of minimum viable product, followed by successive next viable products	☐	☐	☐
c. Continuous Iterative Development	☐	☐	☐
d. Iterative Development training for Program Managers and staff	☐	☐	☐
e. Software documentation (e.g., test files, application programming interfaces, design documents, performance tests, tools) provided to DOD at each production milestone	☐	☐	☐
f. Independent Verification and Validation for Machine Learning	☐	☐	☐
g. None of the above *(Please explain below):* Click or tap here to enter text.	☐	☐	☐

25. Does the program employ the following types of software development approaches? *(Select all that apply) See Defense Acquisition University DAU and the Defense Innovation Board for definitions of software development approaches.*

a) Agile development — Employing? ☐ Yes ☐ No

b) Waterfall approach — Employing? ☐ Yes ☐ No

c) Incremental approach — Employing? ☐ Yes ➔ ☐ No — Length of increment: Click or tap here to enter text.

d) Mixed approach — Employing? ☐ Yes ➔ ☐ No — Please describe: Click or tap here to enter text.

e) DevOps — Employing? ☐ Yes ☐ No

f) DevSecOps — Employing? ☐ Yes ☐ No

g) Other approach — Employing? ☐ Yes ➔ ☐ No — Please describe: Click or tap here to enter text.

7

26. How many releases (i.e., a planned segment of requirements that deploys needed capabilities) has the program planned over the course of the total software development effort? Click or tap here to enter text.

27. How many releases has the program <u>delivered</u> so far? Click or tap here to enter text.

28. On average, how many months are there between each release?

☐ Less than one month
☐ 1 – 3
☐ 4 – 6
☐ 7 – 9
☐ 10-12
☐ 13+
☐ N/A or Don't Know *(Please explain)*: Click or tap here to enter text.

If you selected Agile in question 25 above, please answer questions 29 through 37 below. If Agile is not selected, please skip to question 38.

29. Does the program use the following Agile frameworks? *(Select all that apply)*

Agile Frameworks	Yes	No
a. Scrum	☐	☐
b. Scaled Agile Framework (SAFe)	☐	☐
c. Extreme Programming (XP)	☐	☐
d. Lean Software Development	☐	☐
e. Kanban	☐	☐
f. Other (*Please identify below*): Click or tap here to enter text.	☐	☐
g. To Be Determined	☐	☐

8

30. Does the program use the following Agile techniques? *(Select all that apply)*

Agile Techniques	Yes	No
a. User stories	☐	☐
b. Story mapping	☐	☐
c. Agile portfolio planning	☐	☐
d. Relative estimation/team estimation	☐	☐
e. Prioritized backlog	☐	☐
f. Dedicated customer/product owner	☐	☐
g. Co-located teams (common work area)	☐	☐
h. Integrated teams (integrated development and testing)	☐	☐
i. Short iterations	☐	☐
j. Frequent releases	☐	☐
k. Cross-functional teams	☐	☐
l. Daily stand-up meetings	☐	☐
m. Sprint/iteration planning	☐	☐
n. End-iteration reviews/demos	☐	☐
o. End-iteration retrospectives	☐	☐
p. Definition of done/definition of readiness	☐	☐
q. Minimum Viable Product	☐	☐
r. Other (*Please identify below*): Click or tap here to enter text.	☐	☐

31. Does the program use the following engineering practices? *(Select all that apply)*

Engineering Practices	Yes	No
a. Unit testing	☐	☐
b. Coding standards	☐	☐
c. Continuous integration	☐	☐
d. Refactoring	☐	☐
e. Continuous delivery	☐	☐
f. Continuous deployment	☐	☐
g. Pair programming	☐	☐
h. Test-driven development	☐	☐
i. Automated acceptance testing	☐	☐
j. Collective code ownership	☐	☐
k. Sustainable pace	☐	☐
l. Behavior-driven development	☐	☐
m. Emergent Design	☐	☐
n. Other *(Please identify below)*: Click or tap here to enter text.	☐	☐

9

32. Does the program use the following tools or metrics to track software development progress?
(Select all that apply)

Software Development Progress Tools and Metrics	Yes	No
a. Sprint Burndown: tracks the completion of work throughout the sprint	☐	☐
b. Epic and Release Burndown: tracks the progress of development over a larger body of work than a sprint	☐	☐
c. Velocity: the average amount of work a team completes during a sprint	☐	☐
d. Control Chart: shows the cycle time for a given process (e.g., product, version, or sprint)	☐	☐
e. Cumulative Flow Diagram: shows whether the flow of work across the team is consistent	☐	☐
f. Automated test coverage: the percent of certain elements of code that have been exercised by automated tests	☐	☐
g. Lead Time: time it takes from code commit to running in production successfully	☐	☐
h. Deployment Frequency: frequency of software deployment to production	☐	☐
i. Mean Time to Restore: how long it takes to restore an application or platform when an unplanned outage occurs	☐	☐
j. Change Fail Rate: percentage of changes made to applications or platform once pushed to production	☐	☐
k. Roadmap	☐	☐
l. Other *(Please identify below)*: Click or tap here to enter text.	☐	☐

10

33. Does the program measure success in its Agile development effort in the following ways? *(Select all that apply)*

Agile Development Success Measurements	Yes	No
a. Customer/user satisfaction	☐	☐
b. Operational value delivered	☐	☐
c. Velocity	☐	☐
d. Budget vs. actual cost	☐	☐
e. Planned vs. actual stories per iteration	☐	☐
f. Planned vs. actual stories per release dates	☐	☐
g. Iteration burndown	☐	☐
h. Burn-up chart	☐	☐
i. Cycle time	☐	☐
j. Release burndown	☐	☐
k. Work-in-progress	☐	☐
l. Defect resolution	☐	☐
m. Mean Time to Restore	☐	☐
n. Customer retention	☐	☐
o. Estimation accuracy	☐	☐
p. Earned value	☐	☐
q. Change failure rate	☐	☐
r. Revenue/sales impact	☐	☐
s. Cumulative flow chart	☐	☐
t. Product utilization	☐	☐
u. Individual hours per iteration/week	☐	☐
v. Scope change in a release	☐	☐
w. Deployment frequency	☐	☐
x. Other *(Please identify below)*: Click or tap here to enter text.	☐	☐

11

34. Does the program use the following types of project management tools? *(Select all that apply)*

Project Management Tools	Yes	No
a. Kanban board	☐	☐
b. Task board	☐	☐
c. Bug tracker	☐	☐
d. Spreadsheet	☐	☐
e. Agile project management tool	☐	☐
f. Wiki	☐	☐
g. Automated build tool	☐	☐
h. Unit test tool	☐	☐
i. Continuous integration tool	☐	☐
j. Wireframes	☐	☐
k. Product roadmapping	☐	☐
l. Requirements management tool	☐	☐
m. Release/deployment automation tool	☐	☐
n. Automated acceptance tool	☐	☐
o. Static analysis	☐	☐
p. Project & Portfolio management tool	☐	☐
q. Story mapping tool	☐	☐
r. Timecards	☐	☐
s. Index cards	☐	☐
t. Refactoring tool	☐	☐
u. Customer idea management tool	☐	☐
v. Other (*Please identify below*): Click or tap here to enter text.	☐	☐

12

35. Does the program use the following applications? *(Select all that apply)*

Applications	Yes	No
a. Axosoft	☐	☐
b. Bugzilla	☐	☐
c. DOORS	☐	☐
d. GitHub	☐	☐
e. GitLab	☐	☐
f. Google Docs	☐	☐
g. Hansoft	☐	☐
h. HP Agile Manager	☐	☐
i. HP QC/ALM	☐	☐
j. In-house/home-grown	☐	☐
k. Jira	☐	☐
l. LeanKit	☐	☐
m. Microsoft Excel	☐	☐
n. Microsoft Project	☐	☐
o. Microsoft TFS	☐	☐
p. Mingle	☐	☐
q. Pivotal Tracker	☐	☐
r. Rally	☐	☐
s. Rational Team Concert	☐	☐
t. Splunk	☐	☐
u. Target Process	☐	☐
v. Team Forge	☐	☐
w. VersionOne	☐	☐
x. Other (*Please identify below)*: Click or tap here to enter text.	☐	☐

13

36. GAO's report on DHS's adoption of Agile software development identifies leading practices and associated activities for Agile software development adoption, organized into the following three areas called organizational levels: agency environment, program processes, and team activities and dynamics. *See GAO's report on DHS's adoption of Agile software development (GAO-20-213), Appendices III, IV, and V for descriptions of these activities. In addition, see GAO's recently issued Agile Guide (GAO-20-590G) for further reference.*

I. To what extent is DOD implementing the following activities associated with the agency environment level? *Agency environment refers to leading practices related to an agency's processes, culture, and acquisition strategies.*

Agency Environment Level Activities	Great Extent	Moderate Extent	Some Extent	Little or No Extent	Don't Know	N/A, Not Relevant to Program
a. DOD has established appropriate life cycle activities that support Agile methods.	☐	☐	☐	☐	☐	☐
b. DOD has clearly aligned goals and objectives.	☐	☐	☐	☐	☐	☐
c. DOD has sponsorship for Agile software development that cascades throughout the agency.	☐	☐	☐	☐	☐	☐
d. DOD has sponsors that understand Agile software development.	☐	☐	☐	☐	☐	☐
e. DOD has established an environment supportive of Agile software development.	☐	☐	☐	☐	☐	☐
f. DOD has aligned incentives and rewards to Agile methods.	☐	☐	☐	☐	☐	☐
g. DOD has guidance that is appropriate for Agile acquisition strategies.	☐	☐	☐	☐	☐	☐

14

II. To what extent is DOD implementing the following activities associated with the program processes level? *Program processes refer to leading practices related to the program office and technical environment.*

Program Processes Level Activities	Great Extent	Moderate Extent	Some Extent	Little or No Extent	Don't Know	N/A, Not Relevant to Program
a. DOD has provided training to all program staff in Agile methods and is monitoring the training.	☐	☐	☐	☐	☐	☐
b. DOD has policy or guidance in place to help programs ensure Agile teams have the appropriate technical expertise needed to perform their roles.	☐	☐	☐	☐	☐	☐
c. DOD has policy or guidance that calls for technical and project support tools to be available to support Agile development.	☐	☐	☐	☐	☐	☐
d. DOD has policy or guidance that allows system design that supports iterative delivery.	☐	☐	☐	☐	☐	☐
e. DOD has policy or guidance that calls for Agile projects to establish and maintain a sustainable development pace and track and monitor that development pace.	☐	☐	☐	☐	☐	☐
f. DOD has policy or guidance in place for defining and incorporating non-functional requirements for Agile projects in development.	☐	☐	☐	☐	☐	☐
g. DOD has policy or guidance in place for defining and incorporating critical features for Agile projects in development.	☐	☐	☐	☐	☐	☐

15

III. To what extent is DOD implementing the following activities associated with the team activities and dynamics level? *Team activities and dynamics refer to practices for teams to successfully transition from processes using traditional software development methods to Agile methods.*

Team Activities and Dynamics Level Activities	Great Extent	Moderate Extent	Some Extent	Little or No Extent	Don't Know	N/A, Not Relevant to Program
a. DOD has policy or guidance that requires self-organizing Agile teams.	☐	☐	☐	☐	☐	☐
b. DOD has defined the role of a product owner.	☐	☐	☐	☐	☐	☐
c. DOD has policy or guidance that calls for Agile teams to create user stories to define work.	☐	☐	☐	☐	☐	☐
d. DOD has policy or guidance in place that calls for Agile teams to prioritize requirements in a backlog based on value.	☐	☐	☐	☐	☐	☐
e. DOD has policy or guidance in place that calls for Agile teams to estimate the relative complexity of user stories.	☐	☐	☐	☐	☐	☐
f. DOD has policy or guidance that calls for Agile teams to meet daily to review progress and discuss impediments.	☐	☐	☐	☐	☐	☐
g. DOD has policy or guidance in place that calls for observing end-iteration demonstrations.	☐	☐	☐	☐	☐	☐
h. DOD has policy or guidance in place that calls for observing end-iteration retrospectives.	☐	☐	☐	☐	☐	☐
i. DOD has policy or guidance in place that that defines and emphasizes the use of automated testing and continuous integration.	☐	☐	☐	☐	☐	☐
j. DOD has policy or guidance for an Agile project on ensuring the quality of code being developed.	☐	☐	☐	☐	☐	☐

16

37. Has the program experienced any of the following challenges related to implementing Agile software development? *(Select all that apply)*

Agile Software Development Challenges	Yes	No	Don't Know	Not Applicable
a. Teams had difficulty collaborating closely	☐	☐	☐	☐
b. Teams had difficulty transitioning to self-directed work	☐	☐	☐	☐
c. Staff had difficulty committing to more timely and frequent input	☐	☐	☐	☐
d. Agency had trouble committing staff	☐	☐	☐	☐
e. Timely adoption of new tools was difficult	☐	☐	☐	☐
f. Technical environments were difficult to establish and maintain	☐	☐	☐	☐
g. Agile guidance was not clear	☐	☐	☐	☐
h. Procurement practices may not support Agile projects	☐	☐	☐	☐
i. Customers did not trust iterative solutions	☐	☐	☐	☐
j. Teams had difficulty managing iterative requirements	☐	☐	☐	☐
k. Compliance reviews were difficult to execute within an iteration time frame	☐	☐	☐	☐
l. Federal reporting practices do not align with Agile	☐	☐	☐	☐
m. Traditional artifact reviews do not align with Agile	☐	☐	☐	☐
n. Traditional status tracking does not align with Agile	☐	☐	☐	☐
Please describe other significant software development staff challenges not included above that the program has faced: Click or tap here to enter text.				

Section V: Cybersecurity

38. Does the program have an approved cybersecurity strategy (by DOD CIO or Component CIO)?

☐ Yes
  a) Has the cybersecurity strategy been updated at subsequent milestones?
    ☐ Yes
    ☐ No
    ☐ N/A, no milestones since strategy approved

☐ No, but the program plans to have an approved cybersecurity strategy by:
Insert date: Click or tap here to enter text.

☐ No, the program will not have an approved cybersecurity strategy

☐ If no, please explain why not: Click or tap here to enter text.

17

39. If yes to question 38: Which of the following types of cybersecurity assessments has the program completed? *(Select all that apply)*

Assessment Types	Yes	No
a. Cooperative assessment	☐	☐
b. Adversarial assessment	☐	☐
c. Table top exercise	☐	☐
d. Penetration test	☐	☐
e. Assessment during developmental testing	☐	☐
f. Assessment during operational testing	☐	☐
g. Full system assessment	☐	☐
h. Component assessment	☐	☐
i. Other *(Please identify below)*: Click or tap here to enter text.	☐	☐

40. If you selected No for all of the assessment types in question 39, please explain the reason for your response. Click or tap here to enter text.

41. Has the program undergone any developmental testing?

☐ Yes
a) Did the developmental testing include the following events? *(Select all that apply)*
☐ Cooperative Vulnerability and Identification
☐ Adversarial Assessment (AA)
☐ Other (please explain): Click or tap here to enter text.
☐ No

42. Has the program undergone any <u>operational</u> testing?

☐ Yes
a) Did the operational testing include the following events? (*Select all that apply)*
☐ Cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA)
☐ Adversarial Assessment (AA)
☐ Other (please explain): Click or tap here to enter text.
☐ No

18

Section VI: Software Products and Metrics

43. Has the program identified a minimum deployable, minimum releasable, or minimum viable product?

☐ Yes (*Please describe*): Click or tap here to enter text.
☐ No (*Skip to question 47*)

44. If yes to question 43: Did the program complete its initial minimum deployable, releasable, or viable product?

☐ Yes
☐ No (*Skip to question 46*)

45. If yes to question 44: When did the program complete its initial minimum deployable, releasable or viable product? *Please enter date.* Click or tap here to enter text.

46. If no to question 44: When does the program expect to complete its initial minimum deployable, releasable or viable product? *Please enter date.* Click or tap here to enter text.

19

47. Is the program using the following metrics to assess the system's software effort progress and maturity? (*Select all that apply)*

Software Effort Progress and Maturity Metrics	Yes	No	Not Applicable
a. Earned value management (cost & schedule variances)	☐	☐	☐
b. Size of the software effort (amount of new, modified, and reused code)	☐	☐	☐
c. Number of software specification documents completed and approved	☐	☐	☐
d. Number of software requirements or features to be delivered	☐	☐	☐
e. Number of software structures and interfaces defined	☐	☐	☐
f. Number of software tests necessary to complete the software effort	☐	☐	☐
g. Number of software defects found during each phase or increment	☐	☐	☐
h. Number of software defects found after the phase or increment in which the related code was first developed	☐	☐	☐
i. Number of software defects found and fixed during the same phase or increment when the related code was first developed	☐	☐	☐
j. Number of software defects that require design or engineering changes	☐	☐	☐
k. Velocity – amount of work a team can complete during a single Sprint	☐	☐	☐
l. Time from program launch to deployment of useful functionality	☐	☐	☐
m. Other *(Please identify)*: Click or tap here to enter text.	☐	☐	☐

20

Section VII: Software Challenges and Risks

48. Have the government software staff of your program experienced the following challenges? (*Select all that apply)*

Government Software Staff Challenges	Yes	No	Don't Know	Not Applicable
a. Difficult to hire enough staff to complete software development	☐	☐	☐	☐
b. Difficult to find staff with the required expertise	☐	☐	☐	☐
c. Difficult to hire staff in time to perform planned work	☐	☐	☐	☐
d. Difficult to obtain necessary staff training	☐	☐	☐	☐
e. Concurrency/overlap in staff needed to complete software development, complete software testing activities, and/or revise code and address defects	☐	☐	☐	☐
f. Software engineering staffing plans were not realized as planned	☐	☐	☐	☐
g. Other government staff challenges *(Please describe)*: Click or tap here to enter text.	☐	☐	☐	☐

49. Have the contractor software staff of your program experienced the following challenges? *(Select all that apply)*

Contractor Software Staff Challenges	Yes	No	Don't Know	Not Applicable
a. Difficult to hire enough staff to complete software development	☐	☐	☐	☐
b. Difficult to find staff with the required expertise	☐	☐	☐	☐
c. Difficult to hire staff in time to perform planned work	☐	☐	☐	☐
d. Difficult to obtain necessary staff training	☐	☐	☐	☐
e. Concurrency/overlap in staff needed to complete software development, complete software testing activities, and/or revise code and address defects	☐	☐	☐	☐
f. Software engineering staffing plans were not realized as planned	☐	☐	☐	☐
g. Other contractor staff challenges *(Please describe)*: Click or tap here to enter text.	☐	☐	☐	☐

50. Has your program faced any significant non-staff challenges related to its software efforts?

☐ Yes *(Please describe):* Click or tap here to enter text.

☐ No

21

51. **What is the current CIO Rating (i.e. risk level) the program is reporting on the Federal IT Dashboard?** *See list of individual investments at https://itdashboard.gov/drupal/summary/007. In addition, please provide the program's current risk management plan and risk register.*

☐ 1 (Red)
☐ 2 (Red)
☐ 3 (Yellow)
☐ 4 (Green)
☐ 5 (Green)

52. **If the program is reporting 1, 2, or 3 (i.e. red or yellow) in question 51, what are the most significant program risks that contribute to this CIO Rating (i.e. risk level)?** *Please describe.* Click or tap here to enter text.

Section VIII: COVID-19 Impacts

53. **Has the program office experienced any of the following challenges as a result of COVID-19?** (*Select all that apply)*

COVID-19 Program Office Challenges	Yes	No
a. Staff worked fewer hours or were temporarily furloughed	☐	☐
b. Software development was temporarily shut down	☐	☐
If yes to b, what was the duration of the software development shutdown (in weeks)? Click or tap here to enter text.		
c. Software development was temporarily slowed	☐	☐
If yes to c, what was the duration of the software development slowdown (in weeks)? Click or tap here to enter text.		
d. Other COVID-19 challenges *(Please describe below)*: Click or tap here to enter text.	☐	☐

22

54. Has the program's contractor(s) reported the following challenges as a result of COVID-19? (*Select all that apply)*

COVID-19 Contractor Challenges	Yes	No
a. Staff worked fewer hours or were temporarily furloughed	☐	☐
b. Software development was temporarily shut down	☐	☐
If yes to b, what was the duration of the software development shutdown (in weeks)? Click or tap here to enter text.		
c. Software development was temporarily slowed	☐	☐
If yes to c, what was the duration of the software development shutdown (in weeks)? Click or tap here to enter text.		
d. Contractor(s) went out of business	☐	☐
If yes to d, which contractor(s) went out of business? Click or tap here to enter text.		
e. Other COVID-19 challenges *(Please identify below)*: Click or tap here to enter text.	☐	☐

55. Do any of the following statements about COVID-19 impacts apply to the challenges identified in Question 53 and 54? *(Select all that apply)*

COVID-19 Impacts	Yes	No
a. No schedule impact	☐	☐
b. Schedule delay occurred or will occur	☐	☐
c. Schedule impact is to be determined *(Please explain)*: Click or tap here to enter text.	☐	☐
d. No cost impact	☐	☐
e. Cost impact occurred or will occur	☐	☐
f. Cost impact is to be determined *(Please explain)*: Click or tap here to enter text.	☐	☐
g. Other impact *(Please identify below)*: Click or tap here to enter text.	☐	☐

56. If the schedule is delayed, what is the estimated duration of the delay (in weeks)? Click or tap here to enter text.

57. What methodology did you use to calculate the schedule delay? Click or tap here to enter text.

58. If cost is impacted, what is the estimated amount of program cost increase in base year dollars? *Please provide amount and specify base year.* Click or tap here to enter text.

23

59. What methodology did you use to calculate the cost increase? Click or tap here to enter text.

60. Has the government program office taken any of the following actions to help the program address COVID-19 impacts? (*Select all that apply)*

Program Office Actions	Yes	No
a. Approved expanded telework arrangements	☐	☐
b. Designated contractors essential critical infrastructure workers	☐	☐
c. Expedited release of withheld funding to the prime contractor	☐	☐
d. Expedited new contract awards	☐	☐
e. Increased progress payment percentages for completed work and future production	☐	☐
f. Modified contract delivery dates	☐	☐
g. Removed penalties for missing performance targets	☐	☐
h. Other (please identify below): Click or tap here to enter text.	☐	☐

Section IX: Governance

61. To what extent are roles and responsibilities of DOD-wide and military department software governance entities clear?

☐ Great Extent (*Skip to question 63*)
☐ Moderate Extent
☐ Some Extent
☐ Little or No Extent
☐ Don't Know (*Skip to question 63*)

62. If you selected Moderate Extent, Some Extent, or Little or No Extent in question 61, please explain the reason for your response below.

Click or tap here to enter text.

Section X: Additional Comments

63. What, if any, additional comments would you like to share?

Click or tap here to enter text.

24

Appendix III: Comments from the Department of Defense

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

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

Dear Mr. Walsh:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-21-351, 'SOFTWARE DEVELOPMENT: DoD Faces Risk and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices,' dated March 30, 2021 (GAO Code 104440).

The Department remains committed to acquisition reform and in January 2020 released guidance for the six pathways that make up the Adaptive Acquisition Framework (AAF). By October 2020, specific DoD Instructions for all six pathways were approved. These DoD Instructions provide the underlying policy implementation support for the AAF so that acquisition transformation can be enabled. DoD is also implementing knowledge-based acquisition practices in all of its pathways, including the Defense Business Systems and Software Acquisition. Training programs in modern acquisition best practices are underway and the modern software acquisition practices encouraged are in the early stages of adoption and implementation by our acquisition programs.

Consistent with your recommendations (see enclosure), DoD CIO plans to examine and understand GAO risk ratings analysis for the programs where the DoD CIO risk ratings indicated less risk than the GAO assessment. In addition, OUSD(A&S) is implementing the "Acquisition and Sustainment Data and Analytics Strategic Implementation Plan (December 2020)" which aligns with the GAO recommendation to define, collect, automate, and share with appropriate level of visibility, the metrics necessary for stakeholders to monitor acquisitions and critical to the department's ability to assess acquisition performance.

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

Sincerely,

CADMAN.DAVID.S.1229303615

Digitally signed by CADMAN.DAVID.S.1229303615
Date: 2021.05.13 15:35:42 -04'00'

David S. Cadman
Acting Deputy Assistant Secretary of Defense
Acquisition Enablers

Enclosure:
As stated

GAO DRAFT REPORT DATED MARCH 30, 2021
GAO-21-351 (GAO CODE 104440)

"SOFWARE DEVELOPMENT: DOD FACES RISK AND CHALLENGES IN IMPLEMENTING MODERN APPROACHES AND ADDRESSING CYBERSECURITY PRACTICES"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Government Accountability Office (GAO) recommends that the Secretary of the Defense should direct the Chief Information Officer (CIO) to revisit program risk ratings for its next submission to federal IT Dashboard for the programs where DoD CIO's program risk ratings indicated less risk than GAO's assessment of program risk. (Recommendation 1)

DoD RESPONSE: **CONCUR**. DoD CIO agrees with the recommendation. To further inform risk ratings prior to the next submission to the federal IT Dashboard, DoD CIO will examine and consider GAO risk ratings analysis for the programs where the DoD CIO risk ratings indicated less risk than the GAO assessment.

RECOMMENDATION 2: The GAO recommends that the Secretary of the Defense should direct the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) in consultation with appropriate internal and external stakeholders, to ensure the data strategies and data collection efforts for the business system and software acquisitions pathways define, collect, automate, and share with appropriate level of visibility, the metrics necessary for stakeholders to monitor acquisitions and critical to the department's ability to assess acquisition performance. (Recommendation 2)

DoD RESPONSE: **CONCUR**. The Department has identified and is currently promulgating reporting information standards for all pathways. The Defense Business System standard and the Software Acquisition Pathway (SWP) draft have recently been established and are currently in staffing for final issuance by the Department. OUSD(A&S) is working with the components and recently agreed on an initial set of reporting metrics for the SWP pathway to pilot and assess their viability for long term implementation. Finally, A&S is collaborating with the Services on short and long-term plans for automation of data implementation and collection for all Adaptive Acquisition Framework pathway core data standards with ultimate implementation in Defense Acquisition Visibility Environment and visualization using the analytics and data visualization tools in OUSD(Comptroller)'s ADVANA.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact name above, the following staff also made key contributions to this report: Michael Holland (Assistant Director), Tyler Mountjoy (Analyst in Charge), Gerard V. Aflague, Bea Alff, Logan Arkema, Tommy Baril, David Blanding, Chris Businsky, Erin Carson, Lorraine Ettaro, Jennifer Leotta, Noah Levesque, Anne McDonough, Shelby Oakley, Monica Perez-Nelson, Scott Pettis, Chanetta Reed, Priscilla Smith, Whitney Starr, Hai Tran, Adam Vodraska, and Marilyn Wasleski.

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

Orice Williams Brown, Managing Director, WilliamsO@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, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548