Report to Congressional Committees

December 2020

INFORMATION TECHNOLOGY

DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule

Accessible Version

GAO-21-182

GAO Highlights

Highlights of GAO-21-182, a report to congressional committees

December 2020

INFORMATION TECHNOLOGY

DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule

Why GAO Did This Study

For fiscal year 2020, DOD requested approximately $36.1 billion for IT investments. Those investments included major IT programs, which are intended to help the department sustain key operations.

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, among other things, (1) describe the extent to which selected major IT programs have changed their planned costs and schedules since the programs' initial baselines; and (2) describe what selected software development and cybersecurity risks or challenges, if any, may impact major IT programs' acquisition outcomes.

GAO selected programs based on DOD's list of major IT programs, as of April 10, 2019. From this list, GAO identified 15 major IT programs that had established an initial acquisition program baseline and that were not fully deployed by December 31, 2019.

GAO compared the 15 programs' initial cost and schedule baselines to current acquisition program estimates. In addition, GAO aggregated DOD program office responses to a GAO questionnaire about software development approaches and cybersecurity practices used by the 15 programs.

GAO compared this information to leading practices to identify risks and challenges affecting cost, schedule, and performance outcomes.

This report is a public version of a "for official use only" report issued in June 2020.

View GAO-21-182. For more information, contact Kevin Walsh at (202) 512-6151 or w alshk@gao.gov

What GAO Found

GAO reported in June 2020 that, of the 15 major Department of Defense (DOD) information technology (IT) programs selected for review, 11 had decreased their cost estimates as of December 2019. The decreases in cost estimates ranged from a .03 percent decrease to a 33.8 percent decrease. In contrast, the remaining four programs experienced increases in their life-cycle cost estimates—two with increases exceeding 20 percent. Program officials reported several reasons for the increases, including testing delays and development challenges.

Ten of the 15 programs had schedule delays when compared to their original acquisition program baselines. Schedule delays ranged from a delay of 1 month to a delay of 5 years. Program officials reported a variety of reasons for significant delays (delays of over 1 year) in their planned schedules, including cyber and performance issues.

Regarding software development, officials from the 15 selected major IT programs that GAO reviewed reported using software development approaches that may help to limit risks to cost and schedule outcomes. For example, 10 of the 15 programs reported using commercial off-the-shelf software, which is consistent with DOD guidance to use this software to the extent practicable. Such software can help reduce software development time, allow for faster delivery, and lower life-cycle costs.

In addition, 14 of the 15 programs reported using an iterative software development approach which, according to leading practices, may help reduce cost growth and deliver better results to the customer. However, programs also reported using an older approach to software development, known as waterfall, which could introduce risk for program cost growth because of its linear and sequential phases of development that may be implemented over a longer period of time. Specifically, two programs reported using a waterfall approach in conjunction with an iterative approach, while one was solely using a waterfall approach.

With respect to cybersecurity, programs reported mixed implementation of specific practices, contributing to program risks that might impact cost and schedule outcomes. For example, all 15 programs reported developing cybersecurity strategies, which are intended to help ensure that programs are planning for and documenting cybersecurity risk management efforts.

In contrast, only eight of the 15 programs reported conducting cybersecurity vulnerability assessments—systematic examinations of an information system or product intended to, among other things, determine the adequacy of security measures and identify security deficiencies. These eight programs experienced fewer increases in planned program costs and fewer schedule delays relative to the programs that did not report using cybersecurity vulnerability assessments.

Contents

Letter 1

Background 6

Most Selected Major IT Programs Experienced Decreases in Cost Estimates, Delays in Schedules, and Achievement of Performance Targets 13

Most Major IT Programs Reported Utilizing Software Development Approaches That Can Limit Risks, While Mixed Implementation of Cybersecurity Practices May Increase Risks 21

Agency Comments and Our Evaluation 33

Appendix I: Objectives, Scope, and Methodology 36

Appendix II: Major IT Program Questionnaire Responses 42

Appendix III: Comments from the Department of Defense 65

Appendix IV: GAO Contact and Staff Acknowledgments 67

GAO Contact 67

Staff Acknowledgments 67

Appendix V: Accessible Data 68

Data Table 68

Agency Comment Letter 69

Tables

Table 1: Changes in Life-Cycle Cost and Schedule Estimates from First Acquisition Baseline Estimates and the Status of Technical Performance Targets Tested for 15 Selected Major DOD IT Programs, April 2007 through December 201915

Table 2: Iterative Software Development Approaches 24

Table 3: Cybersecurity Vulnerability Assessments That Program Officials Reported Conducting and Estimated Changes to Planned Life-Cycle Costs of Major DOD IT Business and Non-Business Programs, Program Initiation through December 2019 28

Table 4: Cybersecurity Vulnerability Assessments That Program Officials Reported Conducting and Schedule Delays of

Major DOD IT Business and Non-Business Programs, Program Initiation through December 2019 29
Table 5: Developmental and Operational Cybersecurity Testing That Program Officials Reported Conducting on Major DOD IT Business and Non-Business Programs, Program Initiation through December 2019 31
Table 6: Challenges for DOD IT Program Government and Contractor Software Development Staff, Program Initiation through December 2019 33
Table 7: Type of Software Major Department of Defense (DOD) Information Technology Programs Reported Using 43
Table 8: Software Development Processes Major Department of Defense Information Technology Programs Reported Using44
Table 9: Software Development Approaches Reported by Major Department of Defense Information Technology Programs 45
Table 10: Agile Frameworks That Major Department of Defense Information Technology Programs Reported Using 47
Table 11: Agile Techniques That Major Department of Defense Information Technology Programs Reported Using in Program Development 48
Table 12: Software Engineering Practices That Department of Defense Information Technology Programs Reported Using50
Table 13: Description of Tools and Metrics Used in Program Software Development 51
Table 14: Agile Tools and Metrics That Major Department of Defense Information Technology Programs Reported Using52
Table 15: Success Measures that Major Department of Defense Information Technology Programs Reported Using in Their Agile Software Development Efforts 53
Table 16: Agile Project Management Tools That Selected Major Department of Defense Information Technology Programs Reported Using 55
Table 17: Applications That Selected Major Department of Defense Information Technology Programs Reported Using to Support Agile Software Development 57
Table 18: Extent to Which Selected Major Department of Defense Information Technology Programs Reported Developing an Approved Cybersecurity Strategy 58

Table 19: Extent to Which Selected Major Department of Defense Information Technology Programs Reported Conducting Evaluations for Potential Cybersecurity Vulnerabilities 59
Table 20: Developmental and Operational Cybersecurity Testing That Major Department of Defense Information Technology Programs Reported Conducting 61
Table 21: Cost Increases and Schedule Delays That Department of Defense Information Technology Programs Reported Were Caused by Addressing System Cybersecurity Controls 62
Table 22: Metrics and Metrics That Major Department of Defense Information Technology Programs Reported Using and the Number of Programs Meeting Expected Values 63
Table 23: Challenges for Government and Contractor Software Development Staff Reported by Major Department of Defense Information Technology Programs 64

Figures

Figure 1: Department of Defense (DOD) Fiscal Year 2020 Information Technology Budget by Mission Area (projected) 6
Figure 2: Generic Acquisition Model from the DOD Defense Acquisition System Framework, as of December 2019 9
Figure 3: DOD's Business Capability Acquisition Cycle 11
Accessible Data for Figure 1: Department of Defense (DOD) Fiscal Year 2020 Information Technology Budget by Mission Area (projected) 68

Abbreviations

ACWS	Army Contract Writing System
AFIPPS Inc 1	Air Force Personnel and Pay System Increment 1
APB	acquisition program baseline
ATP	authority to proceed
CAC2S Inc 2	Common Aviation Command and Control System Increment 2
CANES	Consolidated Afloat Networks and Enterprise Services
CIO	chief information officer
CMO	chief management officer
COTS	commercial off-the-shelf
DAI Inc 3	Defense Agencies Initiative Increment 3

DCAPES Inc 2B	Deliberate and Crisis Action Planning and Execution Segments Increment 2B
DCGS-N Inc 2	Distributed Common Ground System - Navy Increment 2
DEAMS Inc 1	Defense Enterprise Accounting and Management System Increment 1
DevOps	development and operations
DevSecOps	development, security, and operations
DHMSM	Department of Defense Healthcare Management System Modernization
DOD	Department of Defense
IPPS-A Inc 2	Integrated Personnel and Pay System – Army Increment 2
ISPAN Inc 4	Integrated Strategic Planning and Analysis Network Increment 4
IT	information technology
MAIS	major automated information system
MDA	milestone decision authority
MROi	Maintenance Repair and Overhaul Initiative
Navy ePS	Navy Electronic Procurement System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PKI Inc 2	Public Key Infrastructure Increment 2
Teleport Gen 3	Teleport Generation 3

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

December 23, 2020

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, the department relies heavily on the use of information technology (IT). For fiscal year 2020, DOD requested approximately $36.1 billion for its IT investments.[1] These investments include its major IT programs,[2] which are intended to help the department sustain its key operations.[3] Collectively, these programs include business, communications, and command and control systems that support department business operations (e.g., financial management, human resource management, and health care) and provide the department and component officials with access to information used to organize, plan, direct, and monitor mission operations.

The *National Defense Authorization Act for Fiscal Year 2019* included a provision for GAO to conduct an assessment of selected DOD IT programs annually through March 2023.[4] This report is the first in the series of GAO annual assessments. Our specific objectives were to: (1)

[1] Department of Defense, *Information Technology and Cyberspace Activities Budget Overview: Fiscal Year 2020 President's Budget Request* (March 2019). This figure only refers to DOD's unclassified budget request.

[2] In this report, the term major IT programs refers to programs that have historically been referred to as major automated information system (MAIS) programs.

[3] A DOD IT investment (including the acquisition of an automated information system as either a product or a service) was designated as a MAIS program if it met certain cost thresholds defined in statute. The National Defense Authorization Act for Fiscal Year 2017 repealed the statutory definitions and requirements for MAIS programs. In January 2020, DOD issued a revised version of DOD Instruction 5000.02, which did not refer to MAIS programs. However, as of June 2020, DOD's transitional guidance, DOD Instruction 5000.02T, continued to refer to MAIS programs.

[4] 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. See *Defense Acquisitions Annual Assessment: Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight*, GAO-20-439 (Washington, D.C., June 3, 2020) for a companion report issued under this mandate, which includes information about major DOD IT systems and major defense acquisition and middle tier acquisition programs.

describe the extent to which selected major IT programs have changed their planned costs and schedules since the programs' initial baselines, and met technical performance targets; and (2) describe what selected software development and cybersecurity risks or challenges, if any, may impact major IT programs' acquisition outcomes.

In June 2020, we issued a report that addressed both of these objectives.[5] However, we designated that report as "for official use only" (FOUO) and did not release it to the general public because of the sensitive information it contained.

This subsequent report publishes the findings discussed in our June 2020 report, but we have removed all references to the sensitive information. Specifically, we deleted information that DOD officials determined was sensitive and requested we redact, and omitted one appendix that contained sensitive details about the programs we evaluated. We also provided a draft of this report to National Security Agency (NSA) officials to review and comment on the sensitivity of the information contained herein and to affirm that the relevant portions of the report can be made available to the public without jeopardizing the security of NSA's information systems and networks.

To address the first objective, we selected programs based on DOD's list of 29 major IT programs as of April 10, 2019. From this list, we identified those major IT programs that had an initial acquisition program baseline (APB)[6] that could be used to determine whether the programs had experienced changes in their planned costs and schedules. We also removed programs from our scope that were fully deployed by December

[5] GAO, *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, GAO-20-456SU (Washington, D.C.: June 9, 2020).

[6] The first acquisition program baseline is established after the program has assessed the viability of various technologies and refined user requirements to identify the most appropriate technology solution that demonstrates that it can meet users' needs.

31, 2019. This resulted in our selection of 15 programs.[7] Appendix I provides a more detailed discussion of our selection criteria.

This report focuses on major business IT programs and major non-business IT programs. The programs referred to as major business IT programs are governed by DOD Instruction 5000.75 and include programs that support key areas such as personnel, financial management, health care, and logistics.[8] This report refers to the remaining major IT programs as non-business programs. These non-business programs are governed by DOD Instruction 5000.02 and include programs that support key areas such as communications and information security.[9]

We compared each program's life-cycle cost (in fiscal year 2020 base-year dollars) and schedule estimates that were established in their first APB to their latest total life-cycle cost (in fiscal year 2020 base-year dollars) and schedule estimates. In addition, to determine whether the

[7] The 15 programs that we selected were: Army Contract Writing System, Integrated Personnel and Pay System-Army Increment 2, Air Force Integrated Personnel and Pay System Increment 1, Defense Enterprise Accounting and Management System -Increment 1, Maintenance Repair and Overhaul Initiative, Navy Electronic Procurement System, Department of Defense Healthcare Management System Modernization, Defense Agencies Initiative Increment 3, Deliberate and Crisis Action Planning and Execution Segments Increment 2B, Integrated Strategic Planning and Analysis Network Increment 4, Common Aviation Command and Control System Increment 1, Consolidated Afloat Networks and Enterprise Services, Distributed Common Ground System -Navy Increment 2, Teleport Generation 3, and Public Key Infrastructure Increment 2.

[8] Department of Defense, *Business Systems Requirements and Acquisition,* Instruction 5000.75 (Washington, D.C., Feb. 2, 2017). DOD issued an updated version in January 2020. This report refers to the February 2017 version of the instruction because it established the guidelines under which systems discussed in this report were operating as of December 2019. However, the business capability acquisition cycle described in the February 2017 version of the instruction remains unchanged.

[9] Department of Defense, *Operation of the Defense Acquisition System* , Instruction 5000.02 [incorporating change 4 (Aug. 2018)] (Washington, D.C., Jan. 7, 2015). The January 2015 instruction was replaced in January 2020. However, this report refers to the January 2015 instruction because it describes the acquisition framework applied in this report.

programs' technical performance targets[10] were tested and met, we identified from among the 15 major IT programs, those that had conducted performance tests—resulting in 10 programs. We then assessed each of these program's self-identified system performance targets against actual system performance metrics. Since we selected a nonprobability sample of major IT programs, the results of our analysis are not generalizable to all of DOD's major IT programs.

We analyzed the information we collected to complete a summary of each program's cost, schedule, and technical performance, and requested that program officials review and validate each summary. We also conducted interviews with program officials to obtain the reasons for any changes and performance shortcomings. We then aggregated and summarized the results of our analyses across programs. Since we selected a nonprobability sample of major IT programs, the results of our analysis are not generalizable to all major IT programs.

To address the second objective, we aggregated DOD program office responses to a questionnaire that we administered seeking information about the software development approaches and cybersecurity practices used by each of the 15 major IT programs assessed under our first objective. We selected the topics of software development approaches and cybersecurity practices to help ensure consistency of this review with companion work that GAO is conducting in response to the same provision in the *National Defense Authorization Act for Fiscal Year 2019* that is focusing on, among other things, the software development approaches and cybersecurity practices for DOD weapon programs.[11] We have previously reported on software development approaches and

[10] Many DOD programs refer to these technical performance targets as key performance parameters. According to DOD, key performance parameters are system performance attributes considered critical or essential to the development of an effective military capability. Failure of a system to meet a performance threshold value may result in an updated threshold value, modification of production increments, or a recommendation for program cancellation. Examples of technical performance targets include whether a program can process a specific percentage of inbound and outbound information or the degree to which data contained in one system is consistent with the same data contained in a different system.

[11] This report is a companion to GAO-20-439, also issued under this mandate. This report includes information about major DOD IT systems and major defense acquisition and middle tier acquisition programs.

cybersecurity practices that have the potential to introduce risks that can impact cost, schedule, and performance outcomes.[12]

We compared the aggregated information from program office responses to our questionnaires to relevant guidance and leading practices[13] to identify where programs were not following guidance or best practices. In doing so, we identified possible risks and challenges associated with not following guidance and leading practices that may affect outcomes relative to cost, schedule, and technical performance. We also reviewed the program responses of those that experienced cost and schedule changes that we identified in the first objective to identify instances where programs' execution of guidance or best practices might be related to cost and schedule changes.

To assess the reliability of the data we used to support the findings of this report, we corroborated program office responses with relevant program documentation and interviews with department officials. We determined that the data were sufficiently reliable for our reporting purposes. Appendix I provides a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from February 2019 to March 2020 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

[12] GAO*, FEMA Grants Modernization: Improvements Needed to Strengthen Program Management and Cybersecurity,* GAO-19-164 (Washington, D.C.: Apr. 9, 2019); *Software Development; Effective Practices and Federal Challenges in Applying Agile Methods,* GAO-12-681 (Washington, D.C., Jul. 27, 2012); *Immigration Benefits System: Better Informed Decision Making Needed on Transformation Program,* GAO-15-415 (Washington, D.C.: May.18, 2015); *Immigration Benefits System: U.S. Citizenship and Immigration Services Can Improve Program Management*, GAO-16-467 (Washington, D.C.: Jul. 15, 2016).

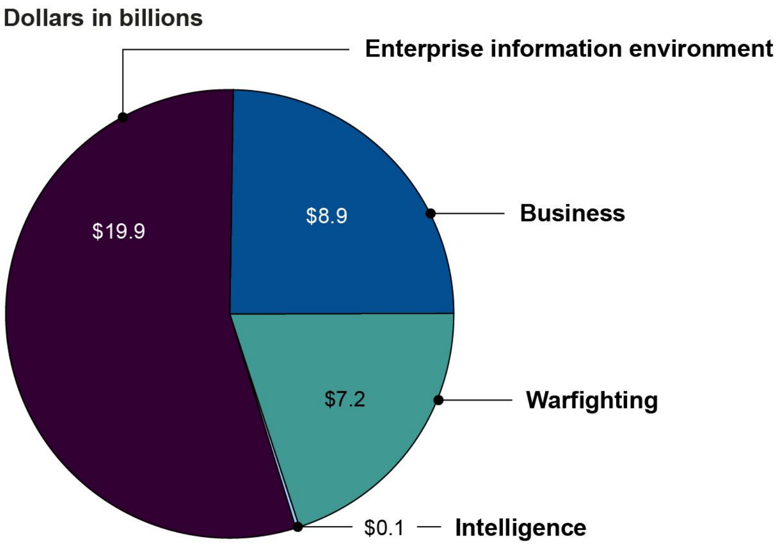
[13] Defense Science Board, *Design and Acquisition of Software for Defense Systems* (Washington D.C.: February 2018); Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Washington D.C.: May 2019); Department of Defense, *Cybersecurity Test and Evaluation Guidebook* version 2.0, (Washington, D.C., April 25, 2018); Department of Defense, *Operation of the Defense Acquisition System*, Instruction 5000.02 (Washington, D.C., Jan. 7, 2015); Department of Defense, Instruction 5000.75, *Business Systems Requirements and Acquisition,* Instruction 5000.75 (Washington, D.C., Feb. 2, 2017). DOD updated this instruction in January 2020; however, this report presents information as of December 2019.

conclusions based on our audit objectives. We subsequently worked from June 2020 to December 2020 to prepare this version of the original sensitive report for public release. This public version also was prepared in accordance with those standards.

Background

In support of its military operations, DOD manages many IT investments, including investments in business, communications, and command and control systems. The department'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 2020 IT budget (of $36.1 billion) that the department plans to spend on each of its mission areas.

Figure 1: Department of Defense (DOD) Fiscal Year 2020 Information Technology Budget by Mission Area (projected)



Source: GAO analysis of DOD information technology budget documentation. | GAO-21-182

Recent Legislative Changes to DOD's Organizational Structure

DOD's organizational structure includes the Office of the Secretary of Defense, the Joint Chiefs of Staff, the military departments, numerous defense agencies and field activities, and various unified combatant commands that contribute to the oversight of DOD's acquisition programs. Prior to February 2018, the former Under Secretary of Defense for Acquisition, Technology, and Logistics also served as the principal acquisition official of the department and was the acquisition advisor to the Secretary of Defense.

The former Under Secretary also served as the defense acquisition executive and was the official responsible for supervising the acquisition of major IT programs, formerly referred to as major automated information system (MAIS) programs. The former Under Secretary's authority included directing the military services and defense agencies on acquisition matters and making milestone decisions for major IT and other programs. This official also had policy and procedural authority for the defense acquisition system, which establishes the steps that DOD programs generally take to plan, design, acquire, deploy, operate, and maintain the department's information systems.

However, in February 2018, the department changed the way it conducts business and operations due to the statutory elimination of the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.[14] That statute also contained a provision that required DOD to establish a new Office of the Under Secretary of Defense for Research and Engineering, to serve as the chief technology officer with the mission of advancing technology for the armed services.

In addition, the statute created a new Office of the Under Secretary of Defense for Acquisition and Sustainment to focus on delivering proven technology more quickly. According to the conference report accompanying the statute, the priorities informing the reorganization

[14] The *National Defense Authorization Act for Fiscal Year 2017*, Pub. L. No. 114-328, § 901, 130 Stat. 2000, 2339 (Dec. 23, 2016) amended chapter 4 of title 10, United States Code, to eliminate the position of Under Secretary of Defense for Acquisition, Technology and Logistics and instead establish an Under Secretary of Defense for Research and Engineering, and Under Secretary of Defense for Acquisition and Sustainment, effective on February 1, 2018.

included elevating the mission of advancing technology and innovation within DOD, and fostering distinct technology and acquisition cultures.[15]

Further, the statute also established the position of Chief Management Officer (CMO), eliminating the position of Deputy Chief Management Officer and assigning the duties of the Chief Management Officer that were formerly assigned to the Deputy Secretary of Defense, to the new Chief Management Officer position. This was intended to maximize the efficiency and effectiveness of the department's business operations.[16] DOD first implemented the CMO position in February 2018. In December 2017, the *National Defense Authorization Act for Fiscal Year 2018*[17] assigned the CMO with the role of DOD chief information officer (CIO) for business systems beginning in January 2019. In December 2019, Congress passed legislation changing the role of the CMO again by revoking the CMO's authority as the CIO for business systems and returning that authority back to the DOD CIO.[18]

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

In January 2015, DOD updated its guidance outlining the framework for, among other things, major IT programs (which historically have been referred to as MAIS programs) through the DOD Instruction 5000.02.[19] According to this instruction, major IT programs were those designated as such by the milestone decision authority or those meeting certain dollar thresholds, in constant fiscal year 2014 dollars. Specifically, the guidance generally established the thresholds as estimated dollar values exceeding (1) $40 million for all program costs in a single year, (2) $165 million for

[15] H.R. Rep. No. 114-840, at 1129-1131 (2016) (Conf. Rep.).

[16] See Pub. L. No. 114-328, § 901 (2016); the *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, § 910, 131 Stat. 1283, 1516 (Dec. 12, 2017), and the *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Pub. L. No. 115-232, § 921, 132 Stat. 1636, 1926 (Aug. 13, 2018) and codified as amended at 10 U.S.C. § 132a.

[17] Pub. L. No. 115-91, § 910, 131 Stat. 1283, 1516-1517 (Dec. 12, 2017).

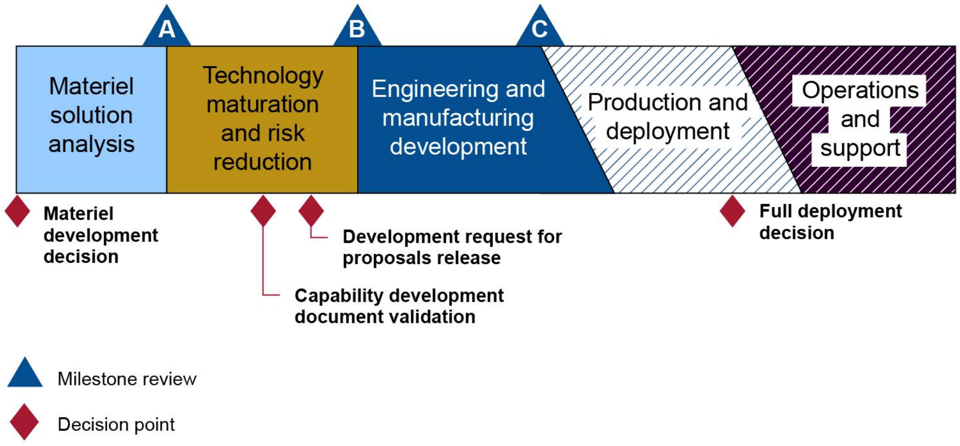
[18] The *National Defense Authorization Act for Fiscal Year 2020*, Pub. L. No. 116-92 § 903, 133 Stat. 1198, 1555 (Dec, 20, 2019) amended section 142(1) and section 132(a) of title 10, United States Code, to return the responsibility for business systems and related matters to the DOD chief information officer.

[19] DOD Instruction 5000.02.

all program acquisition costs for the entire program, or (3) $520 million for the total life-cycle costs of the program (including operation and maintenance costs).

According to the January 2015 instruction, DOD's acquisition framework for IT programs consisted of six models for acquiring and deploying a program, including two hybrid models that each described how a program may be structured based on the type of product being acquired (e.g., software-intensive programs and hardware-intensive programs).[20] Figure 2 shows a generic model of the framework components, including program life-cycle phase and key decision points.

Figure 2: Generic Acquisition Model from the DOD Defense Acquisition System Framework, as of December 2019


A
B
C
Materiel solution analysis
Technology maturation and risk reduction
Engineering and manufacturing development
Production and deployment
Operations and support
Materiel development decision
Capability development document validation
Development request for proposals release
Full deployment decision
Milestone review
Decision point

Source: GAO analysis based on Department of Defense data. | GAO-21-182

The phases of acquiring and deploying a program described in the January 2015 instruction were:

Materiel solution analysis. Refine the initial system solution (concept) and create a strategy for acquiring the solution. A decision—referred to as Milestone A—is made at the end of this phase to authorize entry into the technology maturation and risk reduction phase.

Technology maturation and risk reduction. Determine the preferred technology solution and validate that it is affordable, satisfies program

[20] The DOD acquisition framework is a generic description of acquisition phases and decision points that could apply to almost any product life cycle, DOD or otherwise.

requirements, and has acceptable technical risk. A decision—referred to as Milestone B—is made at the end of this phase to authorize entry of the program into the engineering and manufacturing development phase and award development contracts. An APB is first established at the Milestone B decision point.[21]

Engineering and manufacturing development. Develop a system and demonstrate through testing that the system meets all program requirements. A decision—referred to as Milestone C—is made during this phase to authorize entry of the system into the production and deployment phase or into limited deployment in support of operational testing.

Production and deployment: Achieve an operational capability that meets program requirements, as verified through independent operational tests and evaluation, and implement the system at all applicable locations.

Operations and support: Operationally sustain the system in the most cost-effective manner over its life cycle.

Business System Acquisitions

In February 2017, DOD issued updated acquisition guidelines in *Business Systems Requirements and Acquisition*, DOD Instruction 5000.75,[22] which superseded Instruction 5000.02 for all business system acquisition programs that were not designated as major defense acquisition programs.[23] Instruction 5000.75 also specifically established policy for the use of the five-phase business capability acquisition cycle for business system requirements and acquisition.

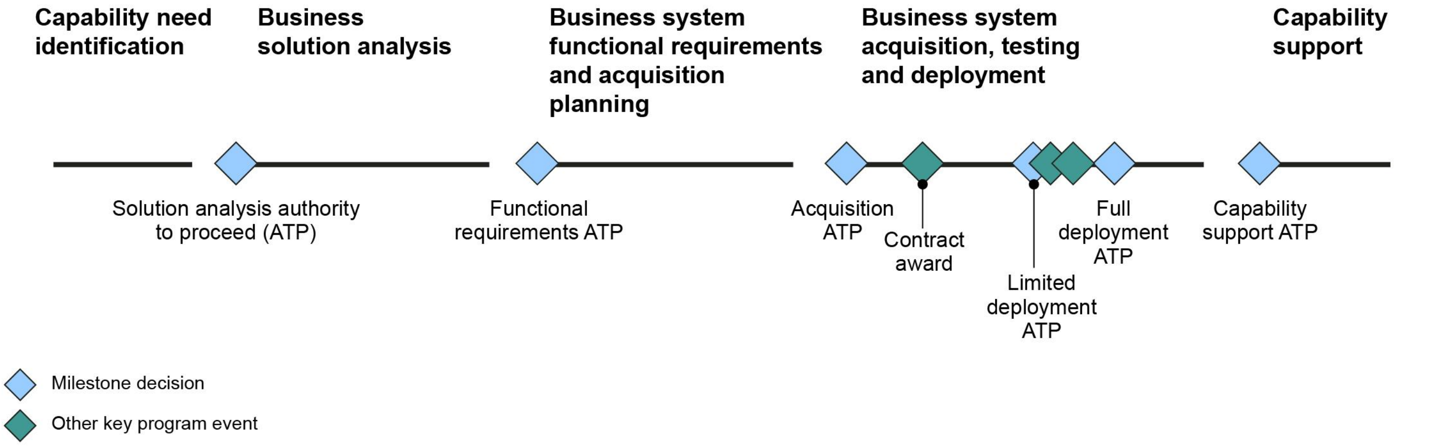
[21] A program's first acquisition program baseline contains the original life-cycle cost estimate (which includes acquisition and operations and maintenance costs), the schedule estimate (which consists of major milestones and decision points), and performance parameters that were approved for that program by the milestone decision authority. The first baseline is established after the program has refined user requirements and identified the most appropriate technology solution that demonstrates that it can meet users ' needs.

[22] DOD Instruction 5000.75.

[23] A major defense acquisition program, defined at 10 U.S.C. § 2430, is a program that meets or exceeds cost thresholds defined in the statute or is designated as a major defense acquisition program by the Secretary of Defense.

Under the instruction, DOD business system acquisitions are to be aligned to commercial best practices and are to minimize the need for customization of commercial products to the maximum extent possible. The instruction also calls for thorough industry analysis and market research of both process and IT solutions using commercial off-the-shelf (COTS) and government off-the-shelf software.[24] In addition, the instruction calls for authority to proceed (ATP) decision points, which are milestone-like events, to be tailored as necessary to contribute to successful delivery of business capabilities. Figure 3 shows DOD's business capability acquisition cycle.

Figure 3: DOD's Business Capability Acquisition Cycle


Capability need identification
Business solution analysis
Business system functional requirements and acquisition planning
Business system acquisition, testing and deployment
Capability support
Solution analysis authority to proceed (ATP)
Functional requirements ATP
Acquisition ATP
Contract award
Limited deployment ATP
Full deployment ATP
Capability support ATP
Milestone decision
Other key program event

Source: Department of Defense Instruction 5000.75. | GAO-21-182

According to the DOD Instruction 5000.75 framework, ATP decision points are to be informed by measures that assess the readiness to proceed to the next phase of the process. Decision-making is to focus on the executability and effectiveness of planned activities, including cost, schedule, acquisition strategy, incentive structure, and risk. In the decision point process, the functional sponsor (i.e., business sponsor) is the senior leader with business function responsibility seeking to improve mission performance. The standard ATP decision points and phases include:

[24] COTS software is sold in substantial quantities in the commercial marketplace and is purchased without modification, or with minimal modification, to its original form. Government off-the-shelf software is developed for the government to meet a specific government purpose. It is not commercially available to the general public.

Capability need identification. The business sponsor is to lead this phase with guidance and support from the CMO. The objective of this phase is to establish a clear understanding of needed business capabilities so that the business sponsor and milestone decision authority (MDA) can decide to invest time and resources into investigating business solutions.

Solution analysis ATP. The CMO, with input from the business sponsor, is to approve the capability requirements, approve the work planned for the next phase, and verify the capability is aligned with the business enterprise architecture as well as organizational strategy and IT portfolio management goals.[25]

Business solution analysis. The business sponsor is to lead this phase with guidance from the CMO and support from the CMO or component acquisition executive or designee. The objective of this phase is to determine high-level business processes supporting the future capabilities so that the business sponsor and component acquisition executive or designee can maximize use of existing business solutions and minimize creation of requirements that can be satisfied by a business system.

Functional requirements ATP. The CMO is to validate that sufficient business process reengineering has been conducted to determine that a business system is required. The MDA is to approve execution of the implementation plan. The business sponsor is to provide full funding available to support all of the business process activities being approved.

Business system functional requirements and acquisition planning. The business sponsor is to lead execution of business process actions in the implementation plan, definition of IT functional requirements, and determination of overall solution approach (e.g., COTS, government off-the-shelf software, legacy modernization, or new development). Meanwhile, the MDA is to oversee development of an acquisition strategy. An objective of this phase is to establish the acquisition strategy that will support functional requirements.

[25] DOD has developed a business enterprise architecture that is intended to serve as a blueprint to guide and constrain the implementation of interoperable defense business systems. The architecture does so by, among other things, documenting the department's business functions and activities.

Acquisition ATP. The MDA is to authorize acquisition of the business system and approve continued execution of the updated implementation plan. The CMO is to approve initial CMO certification based on the chosen solution approach. The MDA is to require full funding for the program to be available to support all of the acquisition activities approved at this decision.

Business system acquisition, testing and deployment. The component acquisition executive or designee is to lead the execution of contract award, supplier management, establishment of baselines, delivery of the business system, and risk management. Meanwhile, the business sponsor is to lead training and deployment. The objective of this phase is to achieve organizational change through business process changes and delivery of the supporting business system, with minimal customization.

Limited deployment ATP(s). The MDA, in conjunction with the business sponsor, is to consider the results of developmental and operational testing and approve deployment of the release to limited groups of end users.

Full deployment ATP. The MDA, with the support of the business sponsor and CMO, is to consider the results of limited deployment(s) and operational testing and approve deployment to the entire user community.

Capability support ATP. The business sponsor is to accept full deployment of the system and approve transition to capability support.

Capability support. The business sponsor is to lead this phase with support from the component acquisition executive or designee. The objective of this phase is to provide enduring support for the capability established by the business system. This includes active engagement in both functional and technical opportunities for continuous process improvement to maintain the relevance of the capability, the supporting technology, and the hosting solution.

Most Selected Major IT Programs Experienced Decreases in Cost Estimates, Delays in

Schedules, and Achievement of Performance Targets

As of December 2019, 11 of the 15 selected major IT programs had experienced decreases in their life-cycle cost estimates, while 10 had experienced delays in their planned schedules when comparing the first acquisition program baseline to the most recent cost and schedule estimates. Changes in program life-cycle cost estimates ranged from a decrease of 33.8 percent to an increase of 150.6 percent. Schedule delays ranged from a delay of 1 month to a delay of 5 years.

Ten of 14 selected programs reported conducting testing on at least some technical performance targets. Testing data for one program were classified. Program officials from eight of the 10 programs reported meeting all of their performance targets. Four programs had not yet conducted any testing activities. Table 1 provides an overview of the extent of changes in planned life-cycle cost and schedule estimates for the selected major IT programs since the first baseline estimate, as well as the number of technical performance targets tested and met.

Table 1: Changes in Life-Cycle Cost and Schedule Estimates from First Acquisition Baseline Estimates and the Status of Technical Performance Targets Tested for 15 Selected Major DOD IT Programs, April 2007 through December 2019

Program type and name	Original acquisition program baseline date	Estimated change in cost (dollars in millions, %)	Estimated schedule change (delay)	Technical performance targets tested and met (number)
Business: Army: Army Contract Writing System	August 2018	-$229 (-33.8%)	10 months	Performance tests not yet conducted
Business: Army: Integrated Personnel and Pay System-Army Increment 2	February 2015	$1379.8 (72%)	No change	5 of 5
Business: Air Force: Air Force Integrated Personnel and Pay System Increment 1	April 2018	-$12.6 (-1.5%)	No change	Performance tests not yet conducted
Business: Air Force: Defense Enterprise Accounting and Management System-Increment 1	February 2012	-$61.5 (-4%)	5 years	4 of 4
Business: Air Force: Maintenance Repair and Overhaul Initiative	April 2018	-$0.2 (-.03%)	6 months	Performance tests not yet conducted
Business: Navy: Navy Electronic Procurement System	March 2019	-$42.8 (-7.3%)	No change	Performance tests not yet conducted
Business: Defense Health Agency: Department of Defense Healthcare Management System Modernization	May 2016	$1267.5 (15.7%)	2 years, 5 months	0 of 3
Business: Defense Logistics Agency: Defense Agencies Initiative Increment 3	January 2018	-$36.6 (-3.1%)	No change	5 of 5
Non-Business: Air Force: Deliberate and Crisis Action Planning and Execution Segments Increment 2B	July 2017	-$40.2 (-14%)	6 months	9 of 9
Non-Business: Air Force: Integrated Strategic Planning and Analysis Network Increment 4	August 2014	-$4 (-2.1%)	3 months	Testing data were classified
Non-Business: Marine Corps: Common Aviation Command and Control System Increment 1	November 2010	-$402.1 (-17.2%)	1 month	2 of 2
Non-Business: Navy: Consolidated Afloat Networks and Enterprise Services	January 2011	-$701.1 (-5.7%)	2 years, 5 months	8 of 8
Non-Business: Navy: Distributed Common Ground System-Navy Increment 2	November 2016	$43.3 (1.5%)	No change	5 of 8
Non-Business: Defense Information Systems Agency: Teleport Generation 3	September 2010	-$116.6 (-19.6%)	3 years, 2 months[a]	12 of 12

Program type and name	Original acquisition program baseline date	Estimated change in cost (dollars in millions, %)	Estimated schedule change (delay)	Technical performance targets tested and met (number)
Non-Business: National Security Agency: Public Key Infrastructure Increment 2	April 2009	$Redacted (150.6%)[b]	1 year, 6 months	1 of 1

Source: GAO analysis of Department of Defense data. | GAO-21-182

[a] A program official stated that the program's schedule dates w ere updated after December 2019. The most recent approved schedule dated January 2020, indicates a full deployment date of November 2021.

[b] The program w as re-baselined in 2015; costs in this table are based on the original development APB. According to the PKI program manager, the program w ill exceed the re-baselined cost by less than three percent of the APB parameter.

Most of the Selected Major IT Programs Had Decreases in Their Planned Life-Cycle Cost Estimates

Eleven of the 15 selected major IT programs had decreases in their life-cycle cost estimates. These decreases ranged from $200,000 for the Maintenance Repair and Overhaul Initiative (MROi) program (.03 percent decrease) to $229 million (33.8 percent decrease) for the Army Contract Writing System (ACWS). Two of the 11 programs with cost decreases experienced cost decreases greater than or almost equal to 20 percent.[26]

Program officials reported a variety of reasons for the overall range of decreases in planned life-cycle cost estimates, including:

- **Lower than expected costs.** Marine Corps officials attributed the 17.2 percent decrease in life-cycle costs for the Common Aviation Command and Control System Increment 1 (CAC2S Inc 1) program to lower than expected actual contract and travel costs during program installment.
- **Program management.** Navy officials stated that they were able to lower the program’s overall cost estimate by 5.7 percent for the Consolidated Afloat Networks and Enterprise Services (CANES) program through good program management, including bi-weekly monitoring of program costs.
- **Contract cost revisions:** Air Force officials for the Air Force Integrated Personnel and Pay System Increment 1 (AFIPPS Inc 1)

[26] Teleport Generation 3 experienced a cost decrease of $116.6 million (19.6 percent) and Army Contract Writing System had a cost decrease of $229 million (33.8 percent).

program stated that in 2019, they re-phased (revised or updated) contract costs according to how each contract was progressing, as well as other program costs due to various schedule changes, resulting in a 1.5 percent life-cycle cost estimate decrease.

In contrast, four of the 15 programs experienced increases in their life-cycle cost estimates, two of them over 20 percent. The overall cost increases ranged from 1.5 percent for the Navy's Distributed Common Ground System-Navy Increment 2 (DCGS-N Inc 2) program to 150.6 percent for the NSA's Public Key Infrastructure Increment 2 (PKI Inc 2) program.

Program officials from the two programs that experienced significant increases in their life-cycle cost estimates (over 20 percent) reported a variety of reasons for these increases, including:

- **Testing delays**. NSA officials indicated that the PKI Inc 2 program experienced a 150.6 percent increase in its life-cycle cost estimates when comparing its current cost estimates to the program's first APB. According to the officials, testing delays due to system stability issues, requirements changes, and software fixes caused these increases. However, the program was re-baselined in 2015 and the increase in cost is based on the original development APB, not the updated APB. According to the PKI program manager, the program is expected to exceed the re-baseline cost by less than 3 percent of the APB parameter.
- **Development challenges.** Army officials stated that Agile development challenges, not using firm fixed price contracts, and delays in development due to working with another agency were reasons for the Integrated Personnel and Pay System-Army Increment 2 (IPPS-A Inc 2) program's 72 percent life-cycle cost increase.

Program officials also reported a variety of reasons for smaller changes (less than 20 percent) in life-cycle cost estimates, including:

- **Awards process.** A Defense Logistics Agency official reported that the Defense Agencies Initiative Increment 3 (DAI Inc 3) program experienced a minimal decrease (3.1 percent) due to conducting a competitive awards process, which resulted in more favorable contract proposals than had been anticipated.
- **Scope reduction:** Air Force officials stated that a reduction in the scope of the Defense Enterprise Accounting and Management

System-Increment 1 (DEAMS Inc 1) program led to a 4 percent decrease in its planned life-cycle cost.

Ten of the Selected Major IT Programs Had Delays in Their Planned Schedules

Ten of the 15 selected major IT programs exceeded their planned schedules, with delays ranging from 1 month for the Marine Corps' CAC2S Inc 1 to 5 years for the Air Force's Defense Enterprise Accounting and Management System-Increment 1. The five remaining programs experienced no delays in their planned schedules—Army's IPPS-A, Inc 2, Air Force's AFIPPS Inc 1, Navy Electronic Procurement System (ePS), Defense Logistic Agency's DAI Inc 3, and Navy's DCGS-N Inc 2.

Program officials from the five programs that experienced significant delays (i.e., delays of over 1 year) in their planned schedules reported a variety of reasons for the delays, including:

- **Cybersecurity and system performance issues.** NSA officials cited several issues that caused schedule delays for the PKI Inc 2 program. Specifically, system changes were required prior to the program entering into an operational test; thus, they needed to delay the schedule until a Plan of Action and Mitigations was in place and high-level category findings were fixed. Additionally, the officials stated that the delays were due to requirement changes, high priority discrepancies reports, and software fixes. Further, Defense Information Systems Agency officials stated that the need to fix significant cybersecurity and performance issues, which arose during developmental and penetration test events, required additional development for Teleport Gen 3 and led to the 3 year and 2 month schedule delay and the need to re-baseline.
- **Maintenance and budget approval process.** Program officials for the Navy's Consolidated Afloat Networks and Enterprise Services program attributed its schedule slippage of 2 years and 5 months to a longer than expected maintenance period for the test platform and to a lengthy budget approval process, which delayed the deployment date. We previously reported on the delays in this program in 2018.[27]

[27] 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).

Officials responsible for programs that experienced less significant delays (i.e., delays of under 1 year) in their planned schedules and for programs that did not experience any delays in their planned schedules reported a variety of reasons for having minimal or no delays, including:

- **Clear communication.** Army officials stated that clearly communicating roles and responsibilities with contractors beforehand helped them minimize changes in IPPS-A Inc 2 program schedules.
- **Realistic schedules.** A Defense Logistics Agency official stated that the DAI Inc 3 program experienced no schedule delays because the program is keeping the process in-house (i.e., not hiring contractors to support the scheduling process) and developing realistic schedules.
- **Government acting as the system integrator.** A Defense Logistics Agency official reported that the government acting as the system integrator helped the DAI Inc 3 program to stay on schedule.

Most of the Selected Major IT Programs Reported Having Tested and Met Their Performance Targets

Among other information, DOD uses key performance parameters[28] as metrics to report on programs' progress toward meeting technical performance targets. This information includes a description of the performance characteristics, the objective and threshold value for each target, and whether the target has been met in demonstrating performance.

As of December 2019, eight of the 10 selected major IT programs that had tested[29] their then-current technical performance targets[30] reported having met all of their targets. Program officials cited a variety of reasons for meeting their performance targets, including:

[28] Not all programs use the term key performance parameter to refer to their technical performance targets.

[29] Testing data for one program were classified.

[30] GAO did not evaluate changes to performance targets that have occurred since each program's initial acquisition program baseline.

- **Using a proven product:** A Defense Logistics Agency official cited using a proven product that had already been tested as a factor for helping the DAI Inc 3 program meet all of its performance targets.
- **Process and planning:** Marine Corps officials for the CAC2S Inc 1 program stated that using an iterative process and making sure planning and decision making occurred prior to getting to the test venue helped the program achieve all of its performance targets.
- **Staff resources:** Army officials stated that receiving full-time support from red team cybersecurity testers and the program office pushing system integrators to meet targets in a timely manner helped the IPPS-A Inc 2 program to effectively achieve performance targets.[31]

As of December 2019, four programs had not yet conducted testing activities—Army's ACWS, Air Force's AFIPPS Inc 1, Air Force's MROi, and Navy ePS. Testing data for one program, Air Force's ISPAN Inc 4, were classified. Program officials reported a variety of reasons for having not yet conducted testing activities for any of their performance targets. For example, according to program officials, AFIPPS, MROi, and Navy ePS had not tested performance targets because their programs were still in the early build phase.

[31] According to the Department of Defense *Cybersecurity Test and Evaluation Guidebook* version 2.0, a red team is a team of people who are National Security Agency-certified and U.S. Cyber Command-accredited to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The red team's objective is to improve a program's enterprise cybersecurity posture by demonstrating the impacts of successful cyberattacks and by demonstrating what works for the defenders (i.e., the blue team) in an operational environment. Department of Defense, *Cybersecurity Test and Evaluation Guidebook* version 2.0 (Washington, D.C., April 25, 2018). DOD issued a revised version of the *Cybersecurity Test and Evaluation Guidebook* on February 10, 2020. This report refers to the 2018 version of the guidebook because this report evaluates program performance through December 31, 2019.

Most Major IT Programs Reported Utilizing Software Development Approaches That Can Limit Risks, While Mixed Implementation of Cybersecurity Practices May Increase Risks

In October 2019, officials from the 15 selected major IT programs we reviewed reported using software development approaches that may help to limit risks to cost and schedule outcomes. For example, major business IT programs reported using COTS software. In addition, most programs reported using an iterative software development approach and using a minimum deployable product. With respect to cybersecurity practices, all the programs reported developing cybersecurity strategies, but programs reported mixed experiences with respect to conducting cybersecurity testing. Most programs reported using operational cybersecurity testing, but less than half reported conducting developmental cybersecurity testing.[32] In addition, programs that reported conducting cybersecurity vulnerability assessments[33] experienced fewer increases in planned program costs and fewer schedule delays. Programs also reported a variety of challenges associated with their software development and cybersecurity staff.

[32] According to DOD's *Cybersecurity Testing and Evaluation Guidebook*, operational cybersecurity testing provides information that helps to resolve operational cybersecurity issues, identify vulnerabilities in a mission context, and describe operational effects of discovered vulnerabilities. Developmental testing identifies cybersecurity issues and vulnerabilities early in the system lifecycle in order to facilitate the remediation and reduction of impact on cost schedule and performance. DOD *Cybersecurity Test and Evaluation Guidebook* version 2.0.

[33] NIST SP 800-53 Rev. 4 defines a vulnerability assessment as a systematic examination of an information system or product to determine the adequacy of s ecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations,* revision 4 (Washington, D.C., January 22, 2015).

Most Major DOD IT Programs Reported Using Approaches to Software Development That Can Limit the Risk of Adverse Cost and Schedule Outcomes

Major Business IT Programs Reported Using COTS Software; Major Non-Business IT Programs Reported Using a Variety of Software Types

According to DOD Instruction 5000.75, *Business Systems Requirements and Acquisition*, business system programs should use COTS and government off-the-shelf solutions, to the extent practicable.[34] Specifically, the use of COTS 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. DOD Instruction 5000.02, *Operation of the Defense Acquisition System*, does not specify a certain software type for major non-business IT programs.

Consistent with DOD guidance, each of the eight major business IT programs reported using commercial software with DOD-specific customizations. By leveraging commercial software, the business programs have positioned themselves to limit some of the risks inherent in other approaches and leverage the benefits of using commercial software.

DOD Instruction 5000.75 also states that DOD business system acquisitions should minimize the need for customization of commercial products to the maximum extent possible.[35] Further, the Defense Acquisition Guidebook notes that modifying COTS software places programs at risk for losing the ability to use product upgrades and finding it difficult to acquire a suitable replacement for the product from other commercial sources.[36]

In contrast to business system programs, which perform more common functions such as human resources management, non-business programs may perform more specialized functions, thus limiting the

[34] DOD Instruction 5000.75.

[35] We did not evaluate the extent to which programs customized off-the-shelf software.

[36] Department of Defense, *Defense Acquisition Guidebook*, (Washington, D.C: February 2017).

availability of off-the-shelf solutions. The seven major non-business IT programs included in our review reported using a variety of software types: four used custom software with commercial hardware, two used commercial software with DOD specific customizations, and one used another kind of software.[37] DOD does not prescribe any specific approach for its major non-business IT systems.

Most Programs Reported Using an Iterative Software Development Approach

In February 2018, the Defense Science Board[38] recommended that DOD acquisitions programs implement continuous iterative software development approaches.[39] The Defense Science Board describes iterative approaches as a way of breaking down the software development of a large application into smaller chunks. Agile, DevOps and DevSecOps, and incremental software development support continuous iterative development. Table 2 describes these iterative approaches.[40]

[37] GAO asked programs to select from the following list of software types: COTS software without DOD-specific modifications or maintenance over the life cycle of the product; commercial software with DOD-specific customization needed; custom software running on commercial hardware and standard operating system; custom software running on custom hardware; and other.

[38] 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.

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

[40] Some respondents selected multiple software development categories on this question, and we contacted certain respondents to clarify their answers.

Table 2: Iterative Software Development Approaches

Approach	Description
Agile	Software is delivered in increments throughout the project, but built iteratively by refining or discarding portions as required based on user feedback.
DevOps	This approach combines "development" and "operations," emphasizing communication, collaboration, and continuous integration between both software developers and users.
DevSecOps	This model combines "development," "security," and "operations," and emphasizes communication, collaboration, and continuous integration between software developers and users.
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.
Mixed	This approach is a combination of two or more different approaches.

Source: Defense Science Board. | GAO-21-182

Note: These approaches are not mutually exclusive. A program may use more than one approach or may combine these approaches w ith a more traditional development approach.

According to the Defense Science Board, continuous iterative software development allows programs 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, known as waterfall. A waterfall 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.

Fourteen of the 15 programs included in our review reported using some kind of approach that supports continuous, iterative development. For example, seven programs reported using Agile development.[41] Additionally, seven reported using incremental development. Three reported using DevOps and two reported using DevSecOps. Two programs reported using a waterfall approach in conjunction with an iterative approach, while one reported solely using a waterfall approach.

[41] The software development approaches are not mutually exclusive, and some programs reported using multiple software development approaches.

In May 2019, the Defense Innovation Board[42] concluded that iterative software development may reduce cost growth compared to a waterfall approach.[43] Accordingly, the three programs using waterfall could be at risk for greater cost growth. However, two of these programs, ACWS, and Navy ePS, also reported using another, iterative, approach, which could help reduce these programs' risk for greater cost growth.[44] DEAMS was the only program that reported only using a waterfall approach.

Most of the 15 Assessed Programs Used a Minimum Deployable Product

In February 2018, the Defense Science Board recommended that all DOD acquisition programs deliver a minimum deployable product.[45] 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.

Consistent with the Defense Science Board's recommendation, 11 of the 15 programs reported that they are delivering a minimum deployable product. The remaining four programs are not developing software using a minimum deployable product and are potentially at risk of being less informed about the extent to which their software is meeting user needs earlier in the software development cycle. By not developing a minimum deployable product, the programs could be at an increased risk of a program failure due to product issues being found late in the development cycle. In addition, by not using a minimum deployable product, programs risk taking a longer amount of time to deliver value to users.

[42] 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.

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

[44] ACWS reported using both Agile and waterfall and Navy ePS reported using both incremental and waterfall.

[45] Defense Science Board, *Design and Acquisition of Software for Defense Systems*. 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.

Major DOD IT Programs Reported Mixed Use of Cybersecurity Practices, Contributing to Program Risks That Might Impact Cost and Schedule Outcomes

In October 2019, the programs included in our review reported incorporating a variety of cybersecurity practices into their software development efforts. This included practices related to cybersecurity strategies, vulnerability assessments, and developmental and operational cybersecurity testing. Programs that are not conducting these cybersecurity practices introduce risks that might impact their cost, schedule, and performance outcomes.

All Programs Reported Using an Approved Cybersecurity Strategy

DOD Instruction 8500.01, *Cybersecurity*, requires that DOD major non-business and business IT programs have approved cybersecurity strategies.[46] These approved strategies are to include information such as cybersecurity and resilience requirements and key system documentation for cybersecurity testing and evaluation analysis and planning. The strategies are intended to help ensure that programs are planning for and documenting cybersecurity risk management efforts, which should begin early in the programs life cycle. If cybersecurity risk management is not undertaken early in the system development, programs are at risk of increased cost and schedule delays, as well as negative impacts to the performance of the system.

Each of the 15 programs included in our assessment reported using an approved cybersecurity strategy. While we did not assess the content of these strategies, incorporating cybersecurity practices early in the development cycle makes it easier and less costly for a program to effectively manage cybersecurity risks.

Programs That Reported Using Cybersecurity Vulnerability Assessments Experienced Fewer Increases in Planned Program Costs and Fewer Schedule Delays

DOD Instructions 5000.02 and 5000.75 require that major non-business and business IT programs conduct cybersecurity vulnerability

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

assessments.[47] Assessments for potential cybersecurity vulnerabilities are to be included in programs' cybersecurity testing and assessment processes. These assessments are to include cooperative vulnerability identification, typically conducted around Milestone A, and a cooperative vulnerability and penetration assessment, typically conducted around Milestone B.[48] Eight of the 15 programs we assessed reported conducting a cybersecurity vulnerability assessment. Six programs reported not conducting a cybersecurity vulnerability assessment, and one program reported that they did not know if they had conducted a cybersecurity vulnerability assessment.[49]

The programs that reported conducting a vulnerability assessment generally reported experiencing better cost outcomes than those that reported not performing a vulnerability assessment. Specifically, seven of the eight programs that reported conducting a vulnerability assessment experienced a cost decrease. Our research design did not enable us to determine whether vulnerability assessments did, in fact, cause improved cost outcomes. Table 3 summarizes cybersecurity vulnerability assessments that program officials reported conducting and any changes to the programs' initial planned life-cycle cost expectations.

[47] As noted earlier in this report, DOD issued new versions of DOD Instruction 5000.02 and 5000.75 in January 2020. However, due to the time period covered by this assessment, this report refers to versions of DOD Instruction 5000.02 and 5000.75 that were issued in January 2015 and February 2017, respectively.

[48] Some programs included in our review may not have reached the appropriate phase of program development life cycle to complete a vulnerability assessment at the time they completed the software and cybersecurity questionnaire.

[49] An official from this program stated that, at the time they responded to the questionnaire, they were not aware of any planned cybersecurity vulnerability assessments.

Table 3: Cybersecurity Vulnerability Assessments That Program Officials Reported Conducting and Estimated Changes to Planned Life-Cycle Costs of Major DOD IT Business and Non-Business Programs, Program Initiation through December 2019

Cybersecurity vulnerability assessment	Experienced a cost estimate Increase	Experienced a cost decrease	Experienced no change in cost	Total number of programs
Performed	1	7	0	**8**
Did not perform	3	3	0	**6**
Do not know if performed[a]	0	1	0	**1**

Source: GAO analysis of Department of Defense IT program data. | GAO-21-182

[a] An official from this program stated that, at the time they responded to the questionnaire, they w ere not aw are of any planned cybersecurity vulnerability assessments.

Similarly, the programs that reported conducting a vulnerability assessment also reported experiencing better schedule outcomes. Four of the eight programs that reported conducting a vulnerability assessment experienced a schedule delay, with two of the four reporting a delay of more than 1 year and two reporting a delay of less than 1 year. Our research design did not enable us to determine whether vulnerability assessments did, in fact, cause improved schedule outcomes. The other four programs that reported conducting a cybersecurity vulnerability assessment experienced no schedule delays. Five of the six programs that did not conduct a vulnerability assessment experienced schedule delays.

Officials from one program reported that they did not know if their program had conducted a vulnerability assessment.[50] This program reported a schedule delay of less than 1 year. Table 4 summarizes the cybersecurity vulnerability assessments that program officials reported conducting and any changes to the programs' initial schedule expectations.

[50] As noted previously, an official from this program stated that, at the time they responded to the questionnaire, they were not aware of any planned cybersecurity vulnerability assessments.

Table 4: Cybersecurity Vulnerability Assessments That Program Officials Reported Conducting and Schedule Delays of Major DOD IT Business and Non-Business Programs, Program Initiation through December 2019

Cybersecurity vulnerability assessment	Experienced schedule delay of more than 1 year	Experienced schedule delay of less than 1 year	Experienced no delay in schedule	Total number of programs
Performed	2	2	4	**8**
Did not perform	3	2	1	**6**
Do not know if performed[a]	0	1	0	**1**

Source: GAO analysis of Department of Defense IT program data. | GAO-21-182

[a]An official from this program stated that, at the time they responded to the questionnaire, they w ere not aw are of any planned cybersecurity vulnerability assessments.

Six Programs Reported Conducting Developmental Cybersecurity Testing; Twelve Reported Conducting Operational Cybersecurity Testing

DOD Instructions 5000.75 and 5000.02 require that DOD major business and non-business IT programs complete both developmental and operational cybersecurity testing. Developmental cybersecurity testing and evaluation is intended to identify cybersecurity vulnerabilities before program deployment in order to help facilitate remediation of cybersecurity vulnerabilities and reduce the risk of a negative impact on cost, schedule, or performance. Developmental testing includes cooperative vulnerability and penetration assessments[51] and adversarial cybersecurity developmental testing.[52] Cybersecurity operational testing evaluates the program for effectiveness, suitability, and survivability.

[51] Department of Defense instructions and guidance require programs to use a cooperative vulnerability identification during developmental testing. This term is similar to a cooperative vulnerability and penetration assessment. Our questionnaire used the term cooperative vulnerability and penetration assessment. A developmental cooperative vulnerability and penetration assessment 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.

[52] An adversarial cybersecurity developmental test is a cybersecurity developmental test and evaluation activity that uses realistic threat exploitation techniques in representative operating environments.

Operational testing includes cooperative vulnerability and penetration assessments[53] and adversarial assessments.[54]

The 15 programs included in our review reported conducting operational cooperative vulnerability and penetration assessments, and adversarial assessments more than developmental cooperative vulnerability identification and adversarial assessments.[55] In particular, six of the 15 total programs reported conducting a cooperative vulnerability and penetration assessment or adversarial assessment during developmental testing. More specifically, two of the eight major business IT programs and four of the eight major non-business IT programs reported conducting a cooperative vulnerability and penetration assessment or an adversarial assessment during developmental testing.

Eleven of the 15 programs reported conducting a cooperative vulnerability and penetration test or adversarial assessment during operational testing. All seven major non-business IT programs and four of the eight business programs reported conducting a cooperative vulnerability and penetration test or adversarial assessment during operational testing. Table 5 identifies the extent to which program officials reported conducting cybersecurity developmental and operational testing.

[53] An operational cooperative vulnerability and penetration assessment examines a system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities.

[54] An adversarial assessment evaluates the ability of a system to support its mission while withstanding cyber threat activity representative of an actual adversary.

[55] Some programs may not have reached the developmental or operational stages of cybersecurity testing and may not have reported the use of these kinds of testing. In addition, some programs reported using both operational and developmental cybersecurity testing.

Table 5: Developmental and Operational Cybersecurity Testing That Program Officials Reported Conducting on Major DOD IT Business and Non-Business Programs, Program Initiation through December 2019

Program type	Developmental cybersecurity testing	Operational cybersecurity testing
Major business IT programs completing	2	4
Major non-business IT programs completing	4	7
Total programs	6	11

Source: GAO analysis of Department of Defense IT program data. | GAO-21-182

According to the DOD *Cybersecurity Test and Evaluation Guidebook*, programs that do not perform developmental testing are at an increased risk of cost and schedule growth and poor program performance.[56] In addition, according to the guidebook, programs that do not perform operational testing are at risk of not resolving operational cybersecurity of the operational effects of discovered vulnerabilities.

DOD Officials Are Aware of Challenges Associated with Their Software Development and Cybersecurity Staff

Program officials reported challenges associated with their software development and cybersecurity staff. Specifically, 12 of the 15 programs included in our assessment reported that they faced challenges with government and contractor software development staff.[57] In May 2019, the Defense Innovation Board also emphasized this challenge and stated that defense software programs face challenges in recruiting, retaining, managing, and developing a software development workforce.[58] In addition, nine of the 15 programs reported difficulty in finding staff with the requisite expertise. Further, seven programs reported difficulty hiring enough staff to complete development; seven also found it difficult to hire staff in time to perform planned work. Six programs reported that software engineering staff plans not being realized as expected was a challenge.

[56] DOD *Cybersecurity Test and Evaluation Guidebook* version 2.0.

[57] Programs provided responses to a list of specific challenges. Programs were also provided the opportunity to identify challenges that were not already listed.

[58] Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage.*

Table 6 summarizes programs' reported challenges with government and contractor software development staff. Appendix II includes additional information on software development and cybersecurity experiences reported by the 15 major IT programs.

Table 6: Challenges for DOD IT Program Government and Contractor Software Development Staff, Program Initiation through December 2019

Challenge	Number of programs
Difficult to find staff with required expertise	9
Difficult to hire enough staff to complete software development	7
Difficult to hire staff in time to perform planned work	7
Software engineering staff plans were not realized as expected	6

Source: GAO analysis of Department of Defense IT program data. | GAO-21-182

DOD officials are aware of department-wide challenges with IT and cyber staff. In 2018, the department issued its DOD Cyber Strategy. Among other things, this strategy describes a line of effort aimed at improving the DOD cyber workforce, which includes IT program and contractor staff. This effort includes investing in future talent, identifying and recruiting sought-after talent, and retaining the current cyber workforce; and it is intended to help ensure that DOD's cyber requirements are filled by an optimal mix of military service members, civilian employees, and contractors. The department also has developed and is monitoring progress against an action plan associated with this line of effort.

Agency Comments and Our Evaluation

DOD provided written comments on a draft of this report, which are reprinted in appendix III. In its comments, the department stated that it continues to evolve its acquisition processes to reduce software development time, allow for faster delivery of capabilities, and lower life-cycle costs. The department also stated that it remains committed to acquisition reform and noted that it issued new guidance for its Adaptive Acquisition Framework in January 2020. The department indicated that this guidance includes two acquisition pathways directly related to the major IT programs reviewed in the draft report: defense business systems and software acquisition.

Further, while our report made no new recommendations, the department stated that the report highlighted opportunities for continued improvement in its efforts to acquire IT capabilities. According to the department, that implementation and wider adoption of the software acquisition pathway will assist in reducing risks and challenges, as will continued implementation of the DOD Cyber Strategy, which includes a line of effort aimed at improving the DOD cyber workforce by investing in future talent, identifying and recruiting sought-after talent, and retaining the current cyber workforce.

DOD also provided technical comments, which we have incorporated as appropriate.

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

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

Kevin Walsh

Kevin Walsh
Director, Information Technology and Cybersecurity

List of Committees

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

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

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Pete Visclosky
Chairman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The *National Defense Authorization Act for Fiscal Year 2019* included a provision for GAO to conduct an assessment of selected Department of Defense (DOD) information technology (IT) programs annually through March 2023.[1] Our objectives are to: (1) describe the extent to which selected major IT programs changed their planned costs and schedules and met technical performance targets and (2) describe what selected software development and cybersecurity risks or challenges, if any, may impact major IT programs' acquisition outcomes.

To address the first objective, we selected programs based on DOD's list of 29 major business and non-business IT programs, as of April 10, 2019. Programs on the DOD list included those that have historically been designated as major automated information system (MAIS) programs and were listed in the Defense Acquisition Management Information Retrieval System.[2] Of the 29 programs, we identified the 15 business and non-business major IT programs that had established an initial acquisition program baseline (APB) that could be used as a reference point for evaluating cost, schedule, and technical performance characteristics and that were not fully deployed by December 31, 2019.[3] This resulted in our selection of 15 programs.

[1] Pub. L. No 115-232, § 833, 132 Stat. 1636, 1858 (Aug. 13, 2018). This report is a companion to GAO-20-439, also issued under this mandate, which discusses major DOD IT systems and DOD weapon programs.

[2] The Defense Acquisition Management Information Retrieval System is a repository for program data.

[3] The 15 programs that were assessed are: Army Contract Writing System, Integrated Personnel and Pay System-Army Increment 2, Air Force Integrated Personnel and Pay System Increment 1, Defense Enterprise Accounting and Management System-Increment 1, Maintenance Repair and Overhaul Initiative, Navy Electronic Procurement System, Department of Defense Healthcare Management System Modernization, Defense Agencies Initiative Increment 3, Deliberate and Crisis Action Planning and Execution Segments Increment 2B, Integrated Strategic Planning and Analysis Network Increment 4, Common Aviation Command and Control System Increment 1, Consolidated Afloat Networks and Enterprise Services, Distributed Common Ground System -Navy Increment 2, Teleport Generation 3, and Public Key Infrastructure Increment 2.

This report focuses on major business IT programs and major non-business IT programs. The programs referred to as major business IT programs are governed by DOD Instruction 5000.75 and include programs that support key areas such as personnel, financial management, health care, and logistics.[4] This report refers to the remaining major IT programs as non-business programs, governed by DOD Instruction 5000.02. These programs support key areas such as communications and information security.

We collected and analyzed key documents, reports, and artifacts pertaining to each program's estimated cost, schedule, and technical performance targets, including each program's latest status in meeting those estimated targets. This included information such as APBs, DOD's MAIS annual and quarterly reports, and information reported in prior GAO reports.[5] For each program, we analyzed and compared the initial APB life-cycle cost estimate (in fiscal year 2020 base-year dollars) to the most recent estimate available to us as of December 2019 (in fiscal year 2020 base-year dollars) to determine the extent to which planned program costs had changed.[6] We calculated the dollar amount for the estimated change in cost in millions by subtracting the original planned total life-cycle cost from the current planned total life-cycle cost. For each program we assessed, all cost information is presented in fiscal year 2020 base-year dollars. We converted cost information to fiscal year 2020 dollars

[4] Department of Defense, *Business Systems Requirements and Acquisition,* Instruction 5000.75 (Washington, D.C., Feb. 2, 2017). DOD updated this instruction in January 2020; however, this report presents information as of December, 2019.

[5] 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); *DOD Major Automated Information Systems: Improvements Can Be Made in Applying Leading Practices for Managing Risk and Testing* , GAO-17-322 (Washington, D.C.: Mar. 30, 2017); *DOD Major Automated Information Systems: Improvements Can Be Made in Reporting Critical Changes and Clarifying Leadership Responsibility*, GAO-16-336 (Washington, D.C.: Mar. 30, 2016); *Defense Major Automated Information Systems: Cost and Schedule Commitments Need to Be Established Earlier*, GAO-15-282 (Washington, D.C.: Feb. 26, 2015); *Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practices*, GAO-14-309 (Washington, D.C.: Mar. 27, 2014); and *Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practices*, GAO-13-311 (Washington, D.C.: Mar. 28, 2013).

[6] A program's first APB contains the original life-cycle cost estimate, schedule estimate, and performance parameters that were approved for that program by the milestone decision authority. The first APB is established after the program has assessed the viability of various technologies and refined user requirements to identify the most appropriate technology solution that demonstrates that it can meet users' needs.

using conversion factors from the DOD Comptroller's National Defense Budget Estimates for Fiscal Year 2020 to adjust for inflation.[7]

Similarly, to determine the extent to which these programs experienced schedule delays, we compared each program's first APB schedule to the most recent approved schedule. Specifically, we used the first, or initial, baseline estimates for each milestone (e.g., Milestone B, Milestone C, full deployment decision, and full deployment) and compared those estimates to the latest estimates. If there were changes to these baseline estimates, we identified the most notable delay.[8] For two programs that each experienced 1-month delays in planned milestones but that also achieved subsequent planned milestones without any delays, we assessed these programs as having no change to their schedules. To determine whether system performance targets were tested and met, we identified that 10 of 14 major IT programs had conducted performance tests. Testing data for one program were classified. For the 10 programs, we analyzed each program's self-identified system performance targets and compared them against actual system performance metrics.

We analyzed the information we collected to complete a summary of each program's cost, schedule, and technical performance, and requested that program officials review and validate each summary. In accordance with our request, all programs reviewed and validated our summaries. In addition, for programs we identified as having a year or more delay in schedule baselines, a 20 percent increase or decrease in cost baselines, and programs that were not meeting their performance goals, we conducted interviews with program officials to obtain the reasons for the changes and performance shortcomings. We then aggregated and summarized the results of our analyses across programs. Since we selected a nonprobability sample of major IT programs, the results of our analysis are not generalizable to all major IT programs.

To address the second objective, we aggregated DOD program office responses to a questionnaire we developed and administered seeking information about the software and cybersecurity practices used by each of the IT programs assessed under our first objective. We selected the

[7] Department of Defense, Undersecretary of Defense, *National Defense Budget Estimates for Fiscal Year 2020*, Green Book Table 5-9 (Washington, D.C: May 2019), 66.

[8] The most notable delay is the most significant delay in any single milestone date. For example, if Milestone C is delayed by 1 month and FDD is delayed by 3 months, the most notable delay is 3 months.

topics of software development approaches and cybersecurity practices to help ensure consistency with companion work being conducted under this same provision in the *National Defense Authorization Act for Fiscal Year 2019* that focuses on the software development approaches and cybersecurity practices of DOD weapons programs. We have previously reported on software development approaches and cybersecurity practices that may have the potential to introduce risks that can impact cost, schedule, and performance outcomes.[9]

We compared the aggregated information from the program office responses to our questionnaires to relevant guidance and leading practices[10] to identify where programs were not following guidance or best practices. In doing so, we identified possible risks and challenges associated with not following guidance and leading practices that may affect outcomes relative to cost, schedule, and technical performance. We also compared program responses to the cost and schedule changes we identified in the first objective to identify instances where programs' execution of guidance or best practices may be related to cost and schedule changes. The questionnaire allowed respondents to submit their answers electronically. We received responses from all of the programs we assessed during October 2019.

Our identification of risks or challenges that might impact acquisition outcomes focused on the 15 programs' responses to the questionnaire. We did not validate the data provided by the program offices, although we

[9] GAO*, FEMA Grants Modernization: Improvements Needed to Strengthen Program Management and Cybersecurity,* GAO-19-164 (Washington, D.C.: Apr. 9, 2019); *Software Development; Effective Practices and Federal Challenges in Applying Agile Methods,* GAO-12-681 (Washington, D.C., Jul. 27, 2012); *Immigration Benefit System: Better Informed Decision Making Needed on Transformation Program,* GAO-15-415 (Washington, D.C.: May.18, 2015); *Immigration Benefit System: U.S. Citizenship and Immigration Services Can Improve Program Management*, GAO-16-467 (Washington, D.C.: Jul. 7, 2016).

[10] 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* (Washington D.C.: May 2019); Department of Defense, *Cybersecurity Test and Evaluation Guidebook* version 2.0, (Washington, D.C., April 25, 2018); Department of Defense, *Operation of the Defense Acquisition System*, Instruction 5000.02 (Washington, D.C., Jan. 7, 2015); Department of Defense, Instruction 5000.75, *Business Systems Requirements and Acquisition,* Instruction 5000.75 (Washington, D.C., Feb. 2, 2017). DOD updated this instruction in January 2020; however, this report presents information as of December, 2019.

followed up with programs when responses were unclear or inconsistent. Where we discovered discrepancies, we clarified the data accordingly.

We aggregated the information provided by the programs in their questionnaires and analyzed it by focusing on: overall responses, major business IT program responses, major non-business IT program and DOD component responses. We also compared selected questionnaire responses to program cost, schedule and performance information and included selected observations in this report. In addition, we included a more comprehensive summary of questionnaire responses in appendix II.

To assess the reliability of the data we used to support the findings of our first objective, we corroborated program office responses with relevant program documentation and interviews with department officials. We determined that the data were sufficiently reliable for our reporting purposes. Since we selected a nonprobability sample of major IT programs, the results of our analysis are not generalizable to all major IT programs.

To ensure the reliability of the data collected through our questionnaire, we took steps to reduce measurement error and non-response error. Specifically, we conducted two pretests of the questionnaire to ensure that the questions were clear, unbiased, and consistently interpreted. The pretests allowed us to obtain initial program feedback and helped to better ensure that officials within each program understood each question. Our pretests were conducted with two programs—one business program and one non-business major IT program. We determined that the data were reliable for the purposes of this report.

To develop the definitions for Agile software development and project management practices included in appendix III, we first reviewed existing work being performed by GAO to develop generally accepted definitions, tentatively referred to as the draft *GAO Agile Assessment Guide*.[11] In developing this guide, GAO reviewed information related to Agile software development practices and compiled a draft of leading practices commonly mentioned across different sources, and sent this draft set of Agile adoption leading 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

[11] Draft *GAO Agile Assessment Guide,* as of January 31, 2020. To develop the draft Agile guide, we have worked closely with Agile experts in the public and private sector.

more than 200 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 draft *GAO Agile Assessment Guide* with information from the Project Management Institute's *Agile Practice Guide*.[12] The *Agile Practice Guide* was developed by experts from the Project Management Institute and the Agile Alliance. We also used information from Carnegie Mellon, Software Engineering Institute, the National Institute of Standards and Technology reports and prior GAO reports to develop definitions.[13]

We conducted this performance audit from February 2019 to March 2020 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. We subsequently worked from June 2020 to December 2020 to prepare this version of the original release. This public version was also prepared in accordance with those standards.

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

[13] 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* (Washington D.C.: May 3, 2019).

Appendix II: Major IT Program Questionnaire Responses

Programs reported information related to software development approaches and cybersecurity practices in response to questionnaires provided to them by GAO. Program responses to many of the questions in our questionnaire were not mutually exclusive and some programs reported multiple responses to a single question. This appendix provides a summary of information programs reported on a questionnaire that was administered between September 2019 and October 2019. The information included in this appendix was self-reported and was not validated by GAO.

Programs Reported Using a Variety of Software Development Practices

Programs reported information about the types of software they used, their software development processes, and their associated approaches.

Programs Reported Using a Variety of Software Types

Programs reported using a variety of software types in their software development efforts. Commercial software with DOD-specific customizations was the most common software type, with 10 of the 15 programs included in our assessment reporting using this type. Four of 15 programs reported using custom software operating on commercial hardware or a standard operating system. One program reported using an “other” type of software not specifically described in our questionnaire. Table 7 summarizes the types of software that programs reporting using.

Table 7: Type of Software Major Department of Defense (DOD) Information Technology Programs Reported Using

Category	Commercial off the shelf software with no DOD-specific modifications or maintenance over the life cycle of the product	Commercial software with DOD-specific customization needed	Custom software running on commercial hardware and standard operating system	Custom software running on custom hardware	Other
Number of programs	0 of 15	10 of 15	4 of 15	0 of 15	1 of 15

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Programs Reported Using a Variety of Software Development Processes

Programs reported using a variety of software development processes. The most commonly used process that programs reported was software documentation, with 11 of 15 programs reporting using it. Nine of 15 programs reported using continuous iterative development. Nine of 15 programs reported delivering a minimum viable product followed by a successive next viable product.[1] Table 8 summarizes program reported processes used in software development.

[1] Minimum viable product is defined as the simplest version of a product that can be released. A minimally viable product should have enough value that it is still usable, demonstrates future benefit early on to retain user buy in, and provides a feedback loop to help guide future development.

Table 8: Software Development Processes Major Department of Defense Information Technology Programs Reported Using

Category	Software factory	Delivery of minimum viable product, followed by successive next viable product	Continuous iterative development	Iterative development training for program managers and staff	Software documentation	Independent verification and validation for machine learning	None
Number of programs	2 of 15	9 of 15	9 of 15	2 of 15	11 of 15	2 of 15	2 of 15

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Programs Reported Using a Variety of Software Development Approaches

Programs reported using a variety of software development approaches. Programs reported using Agile and incremental software development approaches more frequently than any of the other approaches. Specifically, seven of 15 programs reported using Agile and seven of 15 also reported using an incremental approach. Three of 15 programs reported using a waterfall software development approach. One program reported their approach as an “other” approach not specifically described in our questionnaire. Table 9 summarizes programs’ reported software development approaches.

Table 9: Software Development Approaches Reported by Major Department of Defense Information Technology Programs

Category	Agile	Waterfall	Incremental	Mixed	DevOps	DevSecOps	Other
Number of programs	7 of 15	3 of 15	7 of 15	6 of 15	3 of 15	2 of 15	1 of 15

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Programs Reported a Variety of Agile-Specific Software Development Practices

Programs that reported using Agile-specific reported various information about the Agile frameworks, techniques, engineering practices, tools and metrics, success measurements, project management tools, and applications they were using.

Programs Reported Using a Variety of Agile Frameworks

Programs that reported using Agile reported using a variety of Agile frameworks. The Agile framework that programs included in our assessment reported using the most is Scrum,[2] with five of the seven programs reporting using Scrum. Four of seven reported using Scaled Agile Framework.[3] Four of seven programs reported using Kanban[4] and one program reported using another type of Agile framework not

[2] Scrum defines the team by three core roles: product owner, development team, and scrum master. Development is broken down into time boxed iterations called sprints, where teams commit to complete specific requirements. During the sprint, teams meet for daily standup meetings. At the end of the sprint, teams demonstrate the completed work to the product owner for acceptance. A retrospective meeting is held after the sprint to discuss any changes to the process.

[3] Scaled Agile Framework is a framework for implementing Agile at scale. The framework provides guidance for roles, inputs, and processes that can include four configurations (essential, large solution, portfolio, and full) configurable to each unique context. There are nine principles: 1) take an economic view, 2) apply systems thinking, 3) assume variability, 4) build incrementally in cycles, 5) base milestones on evaluation of working systems, 6) visualize and limit work in progress, 7) apply cadence, 8) unlock motivation of workers, and 9) decentralize decision making.

[4] Kanban seeks to limit "work in progress" in order to alleviate bottlenecks throughout development. Team members "pull" work when they are able to, as opposed to work being "pushed" down to them, to smooth the flow of work and eliminate unevenness.

described in our questionnaire. Table 10 summarizes the Agile frameworks that programs reported using.

Table 10: Agile Frameworks That Major Department of Defense Information Technology Programs Reported Using

Category	Scrum	Scaled agile framework	Extreme Programming[a]	Lean software development[b]	Kanban	Other
Number of programs	5 of 7	4 of 7	0 of 7	0 of 7	4 of 7	1 of 7

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

[a] Extreme Programming, or XP, is a process born out of the idea of taking software best practices to the extreme. XP processes incorporate five key values: 1) communication, 2) feedback, 3) simplicity, 4) courage, and 5) respect. XP values constant communication betw een customers, developers, and management as w ell as having a simple and clean design. Pair programming and 100 percent unit testing are some examples of key practices of XP.

[b] Lean software development applies principles from lean manufacturing to software development. There are seven key principles: 1) eliminate w aste, 2) amplify learning, 3) deliver fast, 4) decide late, 5) empow er the team, 6) build integrity in, and 7) optimize the w hole product.

Programs Reported Using a Variety of Agile Techniques in Their Software Development Efforts

The seven programs that reported using Agile reported using various Agile techniques for software development. The most commonly reported technique was a backlog, with all seven programs using it.[5] Six of seven reported using user stories.[6] Six of seven reported using daily stand up meetings.[7] Six of seven programs reported using sprint or iteration planning.[8] Six of seven programs used end of iteration review demonstrations. Six of seven programs used end of iteration retrospectives. Table 11 summarizes the Agile techniques programs reported using in program software development.

[5] The backlog is a list of features, user stories and/or tasks to be addressed by the team, program or portfolio. If new requirements or defects are discovered, these are stored in the backlog to be addressed.

[6] A user story is a brief description of deliverable value for a specific user. It is a promise for a conversation to clarify details.

[7] A daily standup is a brief, daily communication and planning forum where the development team and other relevant stakeholders evaluate the health and progress of the iteration. Attendees also discuss any impediments to their planned progress.

[8] Sprint or iteration planning is a collaborative event in Scrum in which the Scrum team plans the work for the current sprint or iteration.

Table 11: Agile Techniques That Major Department of Defense Information Technology Programs Reported Using in Program Development

Agile technique	Number of programs
Backlog	7 of 7
User stories	6 of 7
Daily standup meetings	6 of 7
Sprint or iteration planning	6 of 7
End-iteration review or demos [a]	6 of 7
End-iteration retrospective[b]	6 of 7
Dedicated customer or product owner[c]	5 of 7
Cross functional teams	5 of 7
Definition of done or definition of readiness[d]	5 of 7
Minimum viable product	5 of 7
Integrated teams (integrated development and testing)	4 of 7
Story mapping[e]	3 of 7
Planning poker or team estimation[f]	3 of 7
Co-located teams (common work area)	2 of 7
Short iterations	3 of 7
Agile portfolio planning	2 of 7

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

[a] A review or demo is a demonstration of a w orking product to the product ow ner who has the opportunity to accept or decline stories.

[b] A retrospective is a team meeting that occurs at the end of every iteration to review lessons learned and to discuss how the team can improve the process and team dynamics.

[c] Product ow ner is defined as the person responsible for maximizing the value of the product, the w ork of the development team, and the backlog. How this is accomplished may vary widely across organizations, Scrum teams, and individuals.

[d] Definition of done or readiness is a predefined set of criteria defined and displayed by the customer that must be met before a w ork item is considered complete. This set of criteria serves as a checklist that is used to check each w ork item for completeness and used as the w ork item's artifact.

[e] Story mapping is a visual technique to prioritize stories by creating a "map" of users, their activities, and the stories needed to implement the required functionality.

[f] Planning poker is a consensus based technique used to estimate the relative effort required to perform a certain amount of w ork. This is related to a group estimation technique know n as w ide-band Delphi from traditional planning.

Programs Reported Using a Variety of Software Engineering Practices in Their Agile Software Development Efforts

The programs that reported using Agile reported various Agile software engineering practices (i.e., technical practices) in their software development efforts. All seven programs reported conducting unit testing[9] while six of seven programs reported using coding standards.[10] Five programs reported using continuous integration in program software development.[11] Table 12 summarizes program software engineering practices used in their software development efforts.

[9] Unit testing is software testing in which individual units of source code, sets of one or more computer program modules together with associated control data, usage procedures, and operating procedures are tested to determine whether they are fit for use.

[10] Coding standards are an agreed upon approach for programming style, practices and methods. Coding standards keep the code consistent and easy for the entire team to read and refactor.

[11] Continuous integration has two objectives: (1) minimize the duration and effort required by each integration episode; (2) be able to deliver at any moment a product version suitable for release. In practice, this dual objective requires an integration procedure which is reproducible at the very least, and in fact largely automated. This is achieved through version control tools, team policies and conventions, and tools specifically designed to help achieve continuous integration.

Table 12: Software Engineering Practices That Department of Defense Information Technology Programs Reported Using

Engineering practice	Number of programs
Unit testing	7 of 7
Coding standards	6 of 7
Continuous integration	5 of 7
Refactoring[a]	3 of 7
Test driven development	2 of 7
Sustainable pace	2 of 7
Continuous delivery[b]	1 of 7
Automated acceptance testing[c]	1 of 7
Continuous deployment[d]	0 of 7
Pair programming[e]	0 of 7
Collective code ownership[f]	0 of 7
Behavior driven development[g]	0 of 7
Emergent design[h]	0 of 7

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

[a] Refactoring is defined as modifying or revising code to improve performance, efficiency, readability, or simplicity without affecting functionality.

[b] Continuous delivery is the practice of delivering feature increments immediately to customers, often through the use of small batches of work and automation technology.

[c] Acceptance testing is formal testing conducted to determine whether or not a user story satisfies its acceptance criteria and so that the customer can decide whether to accept it.

[d] Continuous deployment builds upon continuous delivery and is a software delivery practice in which the release process is fully automated in order to have changes promoted to the production environment with little no human intervention.

[e] Pair programming is defined as the technique of pairing two team members to work simultaneously on the same programming item.

[f] Collective code ownership is the explicit convention that “every” team member is not only allowed, but in fact has a positive duty, to make changes to any code file as necessary: either to complete a development task, to repair a defect, or even to improve the code’s overall structure.

[g] Behavior driven development is a system design and validation practice that uses test-first principles and English-like scripts.

[h] Emergent design encourages lean solutions and avoids over-engineered features and software architectures. The goal is to deliver a system that meets its requirements using an approach that is as streamlined as possible.

Programs Reported Using a Variety of Tools and Metrics in Their Program Software Development Effort

The programs that reported using Agile reported using varying tools and metrics in their Agile software development efforts. Table 13 describes these tools and metrics.

Table 13: Description of Tools and Metrics Used in Program Software Development

Tool or metric	Description
Velocity	The average amount of work a team completes during a sprint.
Sprint burndown	Tracks the completion of work throughout the sprint.
Epic and release burndown	Tracks the progress of development over a larger body of work than a sprint.
Automated test coverage	The percent of certain elements of code that have been exercised by automated tests.
Cumulative flow diagram	Shows whether the flow of work across the team is consistent.
Mean time to restore	How long it takes to restore an application or platform when an unplanned outage occurs.
Control chart	Shows the cycle time for a given process (e.g., product, version, or sprint).
Lead time	Time it takes from code commit to running in production successfully.
Deployment frequency	Frequency of software deployment to production.
Change fail rate	Percentage of changes made to applications/platform once pushed to production.

Source: GAO analysis. | GAO-21-182

The most common of these metrics and tools that programs reported using was velocity, with all seven programs that reported using Agile software development reporting using it. Five of seven programs reported using sprint burndowns and four of seven programs also reported using epic release burndowns. Table 14 summarizes the tools and metrics programs reportedly used.

Table 14: Agile Tools and Metrics That Major Department of Defense Information Technology Programs Reported Using

Tool or metric used	Number of programs
Velocity	7 of 7
Sprint burndown	5 of 7
Epic and release burndown	4 of 7
Automated test coverage	2 of 7
Cumulative flow diagram	1 of 7
Mean time to restore	1 of 7
Control chart	0 of 7
Lead time	0 of 7
Deployment frequency	0 of 7
Change fail rate	0 of 7

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Programs Reported Using a Variety of Methods for Measuring the Success of Agile Development Efforts

The seven programs that reported using Agile also reported various methods for measuring success of their Agile software development efforts. They most commonly reported measuring the program's budget against the program's actual costs. Specifically, six of seven programs reported using this measurement. Five of seven programs reported measuring program success through customer or user satisfaction. Four of seven programs reported measuring success through defect resolution rates. Four of seven also reported measuring program success by comparing planned versus actual stories per iteration. Table 15 summarizes the methods for measuring programs' reported success of their Agile software development efforts.

Table 15: Success Measures that Major Department of Defense Information Technology Programs Reported Using in Their Agile Software Development Efforts

Success measurement	Number of programs
Budget vs. actual costs	6 of 7
Customer or user satisfaction	5 of 7
Velocity	4 of 7
Planned vs. actual number of stories per iteration	4 of 7
Defect resolution	4 of 7
Iteration burndown[a]	3 of 7
Burn-up chart[b]	4 of 7
Release burndown	3 of 7
Earned value[c]	3 of 7
Operational value delivered	3 of 7
Work in progress	2 of 7
Estimation accuracy	2 of 7
Mean time to restore	1 of 7
Change failure rate	1 of 7
Cumulative flow chart	1 of 7
Product utilization	1 of 7
Individual hours per iteration/or week	1 of 7
Planned vs. actual user stories per a release date	0 of 7
Cycle time	0 of 7
Customer retention	0 of 7
Revenue/sales impact	0 of 7
Change of scope in a release	0 of 7
Deployment frequency	0 of 7

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

[a] A burndown is defined as a visual tool displaying progress via a simple line chart representing the remaining work (vertical axis) over time (horizontal axis). It shows where the team stands regarding completing the tasks that comprise the backlog items that are intended to achieve the goals of the iteration. A burndown chart is related to the burn-up chart, except burndown charts display remaining work instead of work accomplished.

[b] A burn-up chart is defined as a visual tool displaying progress via a simple line chart representing work accomplished (vertical axis) over time (horizontal axis). Burn-up charts are also typically used at a release level and iteration levels. They are related to the burndown chart, except they display accomplished work instead of remaining work.

[c] Earned value management is a tool for measuring a project's progress by comparing the value of work accomplished with the amount of work expected to be completed, and is based on variances from cost and schedule baselines.

Programs Reported Using a Variety of Agile Project Management Tools

The programs that reported using Agile reported using a variety of Agile project management tools. Specifically, all seven programs reported using a requirements management tool. In addition, six of seven programs reported using a spreadsheet for Agile project management. Six of seven programs also reported using an Agile project management tool to manage their programs. Table 16 summarizes the tools programs reported using to manage their programs.

Table 16: Agile Project Management Tools That Selected Major Department of Defense Information Technology Programs Reported Using

Project management tools	Number of programs
Requirements management tool	7 of 7
Spreadsheet	6 of 7
Agile project management tool	6 of 7
Unit test[a] tool	6 of 7
Kanban board[b]	4 of 7
Wiki	4 of 7
Automated build tool	4 of 7
Static analysis[c]	4 of 7
Product roadmapping[d]	3 of 7
Bug tracker	3 of 7
Continuous integration tool	2 of 7
Release/deployment automation tool	2 of 7
Wireframes[e]	2 of 7
Story mapping tools	2 of 7
Task board[f]	1 of 7
Project and portfolio management tool	1 of 7
Timecards	1 of 7
Automated acceptance tool	0 of 7
Index cards[g]	0 of 7
Refactoring tool	0 of 7
Customer idea management tool	0 of 7
Other	0 of 7

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

[a] Unit test coverage is defined as the number of lines of code covered by unit tests divided by the total number of lines of code.

[b] A Kanban board is a tool used to track the flow of work and make w ork visible by showing work in queue and w ork in progress.

[c] Static analysis tools are tools that can scan software source code, identify root causes of software security vulnerabilities and correlate and prioritize results

[d] A product roadmap is a high-level strategic plan to guide organization vision and align product ow ner and stakeholder expectations for future development.

[e] Wireframes are a tool used to visualize the identified system requirements and establish content and functionality in the form of a simplified graphical user interface.

[f] A task board is a w all chart (or digital equivalent) w ith markers (cards, sticky notes, etc.) used to track stories' progress for each iteration.

[9] Index cards are defined as a tool used to set the direction on the next piece of functionality w hich is usually small.

Programs Reported Using a Variety of Applications to Support Agile Software Development

The programs that reported using Agile reported using various applications to support Agile software development.[12] All seven programs that reported using Agile software development reported using Microsoft Excel to support their software development efforts. All seven programs also reported using Microsoft Project. Six of seven programs reported using Jira, and four of seven programs reported using another type of application for Agile software development not described in our questionnaire. Table 17 summarizes the applications that the programs used for Agile software development.

[12] These applications are programs or software used to aid Agile software development.

Table 17: Applications That Selected Major Department of Defense Information Technology Programs Reported Using to Support Agile Software Development

Application	Number of programs
Microsoft Excel	7 of 7
Microsoft Project	7 of 7
Jira	6 of 7
Other	4 of 7
HP QC/ALM	4 of 7
DOORS	2 of 7
GitHub	2 of 7
Splunk	2 of 7
GitLab	1 of 7
HP Agile Manager	1 of 7
Inhouse/homegrown	1 of 7
Team Forge	1 of 7

Source: GAO analysis of Department of Defense questionnaire responses. | GAO-21-182

Programs Reported a Variety of Cybersecurity Practices

Selected programs reported information about the their use of an approved cybersecurity strategy, the types of cybersecurity assessments they used, the completion of an evaluation for potential cybersecurity vulnerabilities, the use and documentation of NIST cybersecurity controls, and cost and schedule changes due to addressing cybersecurity controls.

All Programs Reported Developing an Approved Cybersecurity Strategy

All 15 programs included in our review reported developing an approved cybersecurity strategy. These strategies are to include information such as cybersecurity and resilience requirements and key system documentation for cybersecurity testing and evaluation analysis and planning. The strategies are intended to help ensure that programs are planning for and documenting cybersecurity risk management efforts. Table 18 summarizes the programs' reported development of an approved cybersecurity strategy.

Table 18: Extent to Which Selected Major Department of Defense Information Technology Programs Reported Developing an Approved Cybersecurity Strategy

Program response	Number of programs
Yes	15 of 15
No	0 of 15

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Most Programs Reported Evaluating Their Systems for Potential Cybersecurity Vulnerabilities

More than half of the programs included in our review reported evaluating their systems for potential cybersecurity vulnerabilities. Eight of 15 programs reported evaluating for potential cybersecurity vulnerabilities. Six of 15 programs reported that they did not evaluate their systems for potential cybersecurity vulnerabilities and one reported that they did not know if they evaluated their system for potential cybersecurity vulnerabilities.[13] Table 19 summarizes program reporting of the evaluation of potential cybersecurity vulnerabilities.

[13] An official from this program stated that at the time they responded to the questionnaire they that were not aware of any planned cybersecurity vulnerability assessments.

Table 19: Extent to Which Selected Major Department of Defense Information Technology Programs Reported Conducting Evaluations for Potential Cybersecurity Vulnerabilities

Evaluated for potential cybersecurity vulnerabilities	Number of programs
Yes, evaluated for potential cybersecurity vulnerabilities	8 of 15
No, did not evaluate for potential cybersecurity vulnerabilities	6 of 15
Program did not know[a]	1 of 15
Received a waiver	0 of 15

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

[a] An official from this program stated that at the time they responded to the questionnaire they w ere not aw are of any planned cybersecurity vulnerability assessments.

Most Programs Reported Using Operational Cybersecurity Testing; Fewer Programs Reported Using Developmental Cybersecurity Testing

Most programs reported using an operational cooperative vulnerability and penetration assessment[14] or adversarial assessment.[15] Ten of 15 programs reported using an operational cooperative vulnerability and penetration assessment. Nine of 15 programs reported using an operational adversarial assessment. None of the programs reported using an operational cybersecurity assessment other than a cooperative vulnerability and penetration assessment or adversarial assessment. Three of 15 programs reported using no operational cybersecurity testing at all. Table 20 summarizes program reported use of developmental and operational cybersecurity testing.

[14] A cooperative vulnerability and penetration assessment examines a system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities.

[15] An adversarial assessment assesses the ability of a system to support its mission while withstanding cyber threat activity representative of an actual adversary.

Most programs did not report using a developmental cooperative vulnerability and penetration assessment[16],[17] or adversarial assessment.[18] Five of 15 programs reported using a developmental cooperative vulnerability and penetration assessment. Three of 15 programs reported using a developmental adversarial assessment. Five of 15 programs reported using a developmental cybersecurity assessment other than a cooperative vulnerability and penetration assessment or adversarial assessment. Three of 15 programs reported using no developmental cybersecurity testing at all.

[16] Department of Defense Instructions and guidance require programs to use a cooperative vulnerability identification during developmental testing. This term is similar to a cooperative vulnerability and penetration assessment. Our questionnaire used the term cooperative vulnerability and penetration assessment.

[17] A developmental cooperative vulnerability and penetration assessment 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.

[18] An adversarial cybersecurity developmental test is a cybersecurity developmental test and evaluation activity that uses realistic threat exploitation techniques in representative operating environments.

Table 20: Developmental and Operational Cybersecurity Testing That Major Department of Defense Information Technology Programs Reported Conducting

Phase of testing	Assessment conducted	Number of programs
Developmental testing	Cooperative vulnerability and penetration assessment	5 of 15
Developmental testing	Adversarial assessment	3 of 15
Developmental testing	Other kind of assessment	5 of 15
Operational testing	Cooperative vulnerability and penetration assessment	10 of 15
Operational testing	Adversarial assessment	9 of 15
Operational testing	Other kind of assessment	0 of 15
No developmental or operational testing		3 of 15

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Most Programs Reported No Cost and Schedule Changes Due to Addressing System Cybersecurity Controls

Most of the selected programs did not report experiencing any cost or schedule changes due to addressing system cybersecurity controls. Eight of 15 programs reported that addressing cybersecurity controls did not affect program cost or schedule. Four of the 15 programs included in our scope reported that addressing cybersecurity controls caused the programs to experience a cost increase. Two of these programs reported a cost increase of less than 20 percent of the program’s total cost estimate. The other two programs reported a cost increase of more than 20 percent but less than 40 percent.

Additionally, four of 15 programs reported experiencing a schedule increase due to addressing cybersecurity controls. One of these four programs reported an increase to the program schedule of less than 20 percent. Three of these programs reported experiencing a cost increase of more than 20 percent but less than 40 percent. Table 21 summarizes program cost and schedule changes due to addressing cybersecurity controls.

Table 21: Cost Increases and Schedule Delays That Department of Defense Information Technology Programs Reported Were Caused by Addressing System Cybersecurity Controls

Cost or schedule change	Percent	Number of programs
Cost increase	Less than 20 (or 0-20)	2 of 15
Cost increase	More than 20 but less than 40	2 of 15
Cost increase	More than 40 but less than 60	0 of 15
Cost increase	More than 60 but less than 80	0 of 15
Cost increase	More than 80 (or 80-100)	0 of 15
Cost increase	More than 100	0 of 15
Schedule delay	Less than 20 (or 0-20)	1 of 15
Schedule delay	More than 20 but less than 40	3 of 15
Schedule delay	More than 40 but less than 60	0 of 15
Schedule delay	More than 60 but less than 80	0 of 15
Schedule delay	More than 80 (or 80-100)	0 of 15
Schedule delay	More than 100	0 of 15
No, addressing cybersecurity requirements but have not experienced cost or schedule growth due to those cyber requirements		8 of 15
No, not addressing cybersecurity		0 of 15
Other		1 of 15

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Programs Reported Using a Variety of Software Development Metrics to Assess the System's Software Effort Progress and Maturity

Programs reported using a variety of software development metrics. The most commonly used metric was the number of software requirements or features to be delivered, with 12 of 15 programs reporting using this metric. Of the 12 programs that reported using this metric, eight are expected to meet the values set for the metric. Ten of 15 programs reported using the number of software defects found during each phase or increment as a metric to assess the entire system. Of the 10 programs using this metric, nine programs reported that they expected to meet the values set for the metric. Table 22 summarizes the metrics that programs were using and if they expected to meet the values of those metrics, as of October 2019.

Table 22: Metrics and Metrics That Major Department of Defense Information Technology Programs Reported Using and the Number of Programs Meeting Expected Values

Software development metric	Number of programs using the metric	Number of programs meeting expected values of metrics
Number of software requirements or features to be delivered	12 of 15	8 of 12
Number of software defects found during each phase or increment	10 of 15	9 of 10
Earned value management (cost and schedule variances)	8 of 15	5 of 8
Number of software structures and interfaces defined	8 of 15	7 of 8
Number of software defects found after the phase or increment in which the related code was first developed	8 of 15	8 of 8
Number of software defects found and fixed during the same phase or increment when the related code was first developed	7 of 15	7 of 7
Number of software tests necessary to complete the software effort	7 of 15	6 of 7
Number of software specification documents completed and approved	6 of 15	6 of 6
Velocity, amount of work a team can complete during a single Sprint	6 of 15	3 of 6
Size of the software effort (amount of new, modified, and reused code)	5 of 15	4 of 5
Number of software defects that require design or engineering changes	6 of 15	5 of 6
Time from program launch to deployment of useful functionality	6 of 15	4 of 6
Other metric	1 of 15	0 of 1

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Programs Reported Challenges Associated with Government and Contractor Software Development Staff

The selected programs reported experiencing challenges regarding government and contractor software development staff. The most commonly reported challenge was difficulty finding staff with the required expertise, with 9 of the 15 programs included in our scope reporting this challenge. Seven of 15 reported difficulty hiring enough staff to complete software development. Seven of 15 reported difficulty hiring staff in time to perform planned work. Table 23 summarizes programs' reported challenges for software development staff.

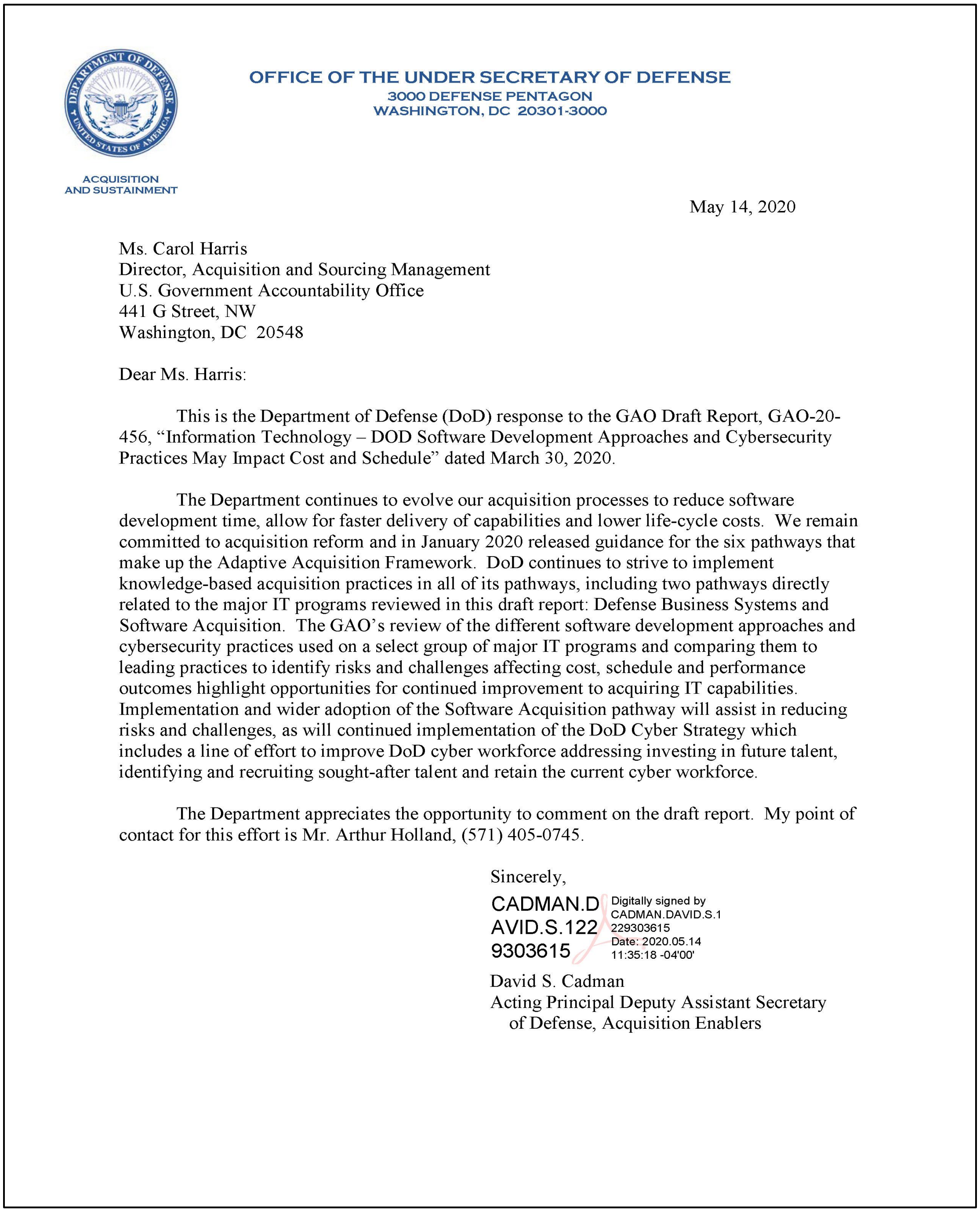
Table 23: Challenges for Government and Contractor Software Development Staff Reported by Major Department of Defense Information Technology Programs

Challenge	Yes	No	Not applicable	Don’t know
Difficult to find staff with the required expertise	9	4	2	0
Difficult to hire enough staff to complete software development	7	6	2	0
Difficult to hire staff in time to perform planned work	7	6	2	0
Software engineering staffing plans were not realized as planned	6	6	2	1

Source: GAO analysis of DOD questionnaire responses. | GAO-21-182

Appendix III: Comments from the Department of Defense

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

May 14, 2020

Ms. Carol Harris
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-20-456, "Information Technology – DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule" dated March 30, 2020.

The Department continues to evolve our acquisition processes to reduce software development time, allow for faster delivery of capabilities and lower life-cycle costs. We remain committed to acquisition reform and in January 2020 released guidance for the six pathways that make up the Adaptive Acquisition Framework. DoD continues to strive to implement knowledge-based acquisition practices in all of its pathways, including two pathways directly related to the major IT programs reviewed in this draft report: Defense Business Systems and Software Acquisition. The GAO's review of the different software development approaches and cybersecurity practices used on a select group of major IT programs and comparing them to leading practices to identify risks and challenges affecting cost, schedule and performance outcomes highlight opportunities for continued improvement to acquiring IT capabilities. Implementation and wider adoption of the Software Acquisition pathway will assist in reducing risks and challenges, as will continued implementation of the DoD Cyber Strategy which includes a line of effort to improve DoD cyber workforce addressing investing in future talent, identifying and recruiting sought-after talent and retain the current cyber workforce.

The Department appreciates the opportunity to comment on the draft report. My point of contact for this effort is Mr. Arthur Holland, (571) 405-0745.

Sincerely,

CADMAN.DAVID.S.1229303615

Digitally signed by CADMAN.DAVID.S.1229303615
Date: 2020.05.14 11:35:18 -04'00'

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

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: Carol Harris (Director), Michael Holland (Assistant Director), Neha Bhatt (Analyst in Charge), Christy Abuyan, Joseph Andrews, Anna Bennett, Alina Budhathoki, Chris Businsky, Melissa Melvin, Gabriel Nelson, Priscilla Smith, and Jessica Waselkow.

Appendix V: Accessible Data

Data Table

Accessible Data for Figure 1: Department of Defense (DOD) Fiscal Year 2020 Information Technology Budget by Mission Area (projected)

Enterprise information environment (dollar in billions)	Business (dollars in billions)	Warfighting (dollars in billions)	Intelligence (dollars in billions)
19.9	8.9	7.2	0.1

Agency Comment Letter

Accessible Text for Appendix III Comments from the Department of Defense

May 14, 2020

Ms. Carol Harris
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-20-456, "Information Technology - DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule" dated March 30, 2020.

The Department continues to evolve our acquisition processes to reduce software development time, allow for faster delivery of capabilities and lower life-cycle costs. We remain committed to acquisition reform and in January 2020 released guidance for the six pathways that make up the Adaptive Acquisition Framework. DoD continues to strive to implement knowledge-based acquisition practices in all of its pathways, including two pathways directly related to the major IT programs reviewed in this draft report: Defense Business Systems and Software Acquisition. The GAO's review of the different software development approaches and cybersecurity practices used on a select group of major TT programs and comparing them to leading practices to identify risks and challenges affecting cost, schedule and performance outcomes highlight opportunities for continued improvement to acquiring IT capabilities. Implementation and wider adoption of the Software Acquisition pathway will assist in reducing risks and challenges, as will continued implementation of the DoD Cyber Strategy which includes a line of effort to improve DoD cyber workforce addressing investing in future talent, identifying and recruiting sought-after talent and retain the current cyber workforce.

The Department appreciates the opportunity to comment on the draft report. My point of contact for this effort is Mr. Arthur Holland, (571) 405-0745.

Sincerely,

David S Cadman
Acting Principal Deputy Assistant Secretary
of Defense, Acquisition Enablers

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/fraudnet/fraudnet.htm

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 Sanford, Acting Managing Director, spel@gao.gov, (202) 512-9715
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548