GAO

Highlights

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

June 2022

BUSINESS SYSTEMS

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

Why GAO Did This Study

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

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

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

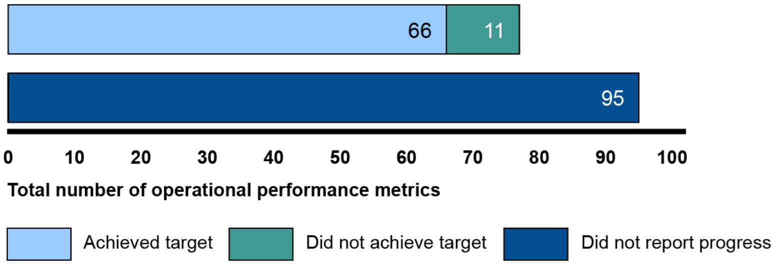
View GAO-22-105330. For more information, contact Kevin Walsh at 202-512-6151 or walshk@gao.gov.

What GAO Found

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

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

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



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

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

As of February 2022, DOD program officials from all 11 (of the 25) major IT business programs that we considered to be actively developing new software functionality reported using recommended iterative development practices that can limit risks of adverse cost and schedule outcomes. Officials from eight of the 11 programs reported using Agile software development, which can support continuous iterative software development. Officials for five of the programs also reported delivering software functionality every 6 months or less, as called for in OMB guidance. Officials for three programs reported a frequency greater than 6 months and officials from the remaining three did not indicate a frequency.

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

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

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

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

What GAO Recommends

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

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

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

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

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

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

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

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

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

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

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

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

Regarding actions to implement legislative and policy changes, the National Defense Authorization Act (NDAA) for FY 2021 eliminated the DOD chief management officer (CMO) position. This position previously had broad oversight responsibilities for DOD business systems. In September 2021, the Deputy Secretary of Defense directed a broad realignment of the responsibilities previously assigned to the CMO. GAO will continue to monitor DOD's efforts to redistribute the roles and responsibilities formerly assigned to the CMO.