December 2020

INFORMATION TECHNOLOGY

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

GAO Highlights

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

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 walshk@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.