GAO Highlights

Highlights of GAO-23-106701, a report to congressional committees

DHS Annual Assessment

Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification

Homeland Advanced Recognition Technology

Cross Border Tunnel Threat

Polar Security Cutter

Source (left to right): Office of Biometric Identity Management; U.S. Customs and Border Protection; and Halter Marine, Inc. | GAO-23-106701

Why GAO Did This Study

To help execute its many critical missions, DHS plans to spend more than $4 billion on its portfolio of major acquisition programs—those with life-cycle costs over $300 million—in fiscal year 2023.

For some DHS major acquisition programs, COVID-19 or changes implemented to address it have affected workforce availability or led to supply chain issues. In addition, DHS's major acquisition programs increasingly rely on software and IT systems, and cyberattacks can target any IT system.

The Explanatory Statement accompanying the DHS Appropriations Act, 2015, included a provision for GAO to review DHS's major acquisitions on an ongoing basis.

This report, GAO's eighth review, assesses the extent to which selected programs are (1) meeting baseline goals, (2) mitigating COVID-19 effects on delivery of capabilities, and (3) executing cybersecurity activities.

This is a public version of a sensitive report that issued in March 2023. Information that DHS deemed sensitive has been omitted.

View GAO-23-106701. For more information, contact Marie A. Mak at (202) 512-4841 or makm@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) invests billions of dollars annually to acquire systems that help secure the border, advance marine safety, screen travelers, improve disaster response, and execute a wide variety of other operations.

Most Programs Met Established Cost and Schedule Goals in Fiscal Year 2022

As of September 2022, 18 of the 25 selected DHS acquisition programs that GAO reviewed had a department-approved acquisition program baseline—a summary of measurable estimates indicating how the system will perform, when it will be delivered, and what it will cost. Most of the other programs were not yet required by policy to have an approved program baseline.

Of these 18 programs, three started the fiscal year either behind their approved schedule or over their approved budget, putting them in breach status. However, all three completed the process needed to get back on track, including revising their baseline estimates. By the end of fiscal year 2022, those programs met their revised cost and schedule goals. Four other programs also revised or were revising their baselines in fiscal year 2022 due to changes in the projects' scope, such as a change in the quantity being acquired.

In addition, eight of the 25 DHS acquisition programs completed the operational test and evaluation phase of the acquisition process during fiscal year 2022, according to a DHS official. After completing operational test and evaluation, those programs are on track to begin production and deliver new capabilities.

Five Programs Sought COVID-19 Baseline Adjustments

COVID-19 affected some of the 25 major acquisition programs GAO reviewed in a variety of ways, including supply chain issues and inflation. As of September 2022:

- Five programs were seeking approval to adjust their schedule or cost baselines due to COVID-19 effects. These programs have requested flexibilities offered in a July 2022 DHS memorandum to address the effects of COVID-19.
- Five other programs reported COVID-19 cost or schedule effects in fiscal year 2022, but were able to manage them within their baselines.

How GAO Did This Study

GAO assessed 25 major acquisition programs, including DHS's largest programs and those that GAO or DHS identified as at risk of poor outcomes to determine program status as of September 30, 2022. GAO assessed their progress in meeting cost, schedule and performance goals; and reviewed policy, memorandums, and information about the cost and schedule effects of COVID-19. GAO also reviewed DHS acquisition cybersecurity policy and assessed programs' cybersecurity risk management activities; and interviewed DHS officials.

What GAO Recommends

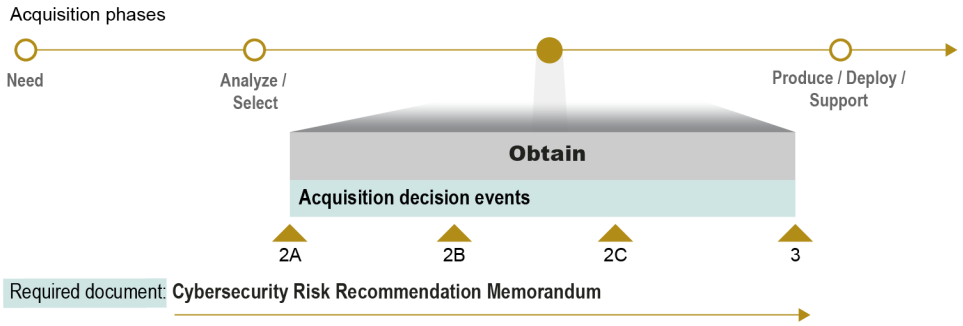
GAO is recommending that, as DHS updates its Instruction 102-01-012, it clarifies which major acquisition programs are required to have completed cybersecurity risk recommendation memorandums prior to acquisition decision events, and when exemptions apply. In the sensitive version of this report, GAO made one additional recommendation to DHS.

- The remaining 15 programs did not report schedule or cost effects related to COVID-19.

Selected Programs Have Not Prepared Cybersecurity Memorandums Ahead of Acquisition Decision Events

In addition, since the department's acquisition cybersecurity instruction was issued, none of the seven programs that had subsequent acquisition decision events completed a cybersecurity risk recommendation memorandum (CRRM). The instruction requires that major acquisition programs consider cybersecurity throughout the acquisition life cycle. Specifically, major acquisition programs are required to present a CRRM at acquisition decision events to identify the programs' cybersecurity status and their risk recommendation (high, medium, low).

Cybersecurity Risk Recommendation Memorandum Required in the Acquisition Life Cycle



Source: GAO analysis of Department of Homeland Security (DHS) documents. | GAO-23-106701

DHS officials told GAO that a CRRM was not applicable to them for various reasons. In one instance, a program provided documentation that this requirement was waived by DHS. The other six programs reported that other documentation was used instead, that the memorandum was not applicable to their program, or that they simply did not develop one. The instruction does not clarify when the CRRM requirement might be waived, is not applicable, or when or what other documentation may be used in its place. If DHS does not clarify when exemptions apply, programs may not prepare the memorandums when they are needed. As a result, DHS, in its oversight role, may not have information to effectively assess cybersecurity risk and ensure that risk mitigations are adequate.