March 2022

DEFENSE ACQUISITIONS

Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities

GAO Highlights

Highlights of GAO-22-104695, a report to congressional committees

Why GAO Did This Study

The U.S. faces increasingly sophisticated cyber threats, such as the 2019 SolarWinds security breach. To mitigate these threats, DOD is continually developing new software-based capabilities. Cyber Command created the JCWA in 2019 to address these needs and synchronize cyber warfighting programs across DOD. The JCWA includes a range of software-enabled systems, sensors, and tools that the Army and Air Force are procuring for Cyber Command.

In November 2020, GAO reported shortfalls in the JCWA governance structure and interoperability goals and recommended that Cyber Command define roles and responsibilities for overseeing the JCWA programs and develop such goals.

A Senate report included a provision for GAO to review the status of the JCWA. This is GAO's second report. This report examines Cyber Command's progress in defining JCWA roles, responsibilities, and interoperability goals; and efforts to assess the JCWA acquisitions using outcome-based metrics. To conduct this work, GAO obtained and reviewed relevant documents and met with DOD officials.

What GAO Recommends

GAO is recommending that Cyber Command develop outcome-based metrics to inform future Value Assessments. DOD concurred with the recommendation and identified steps it is taking to develop metrics for future Value Assessments.

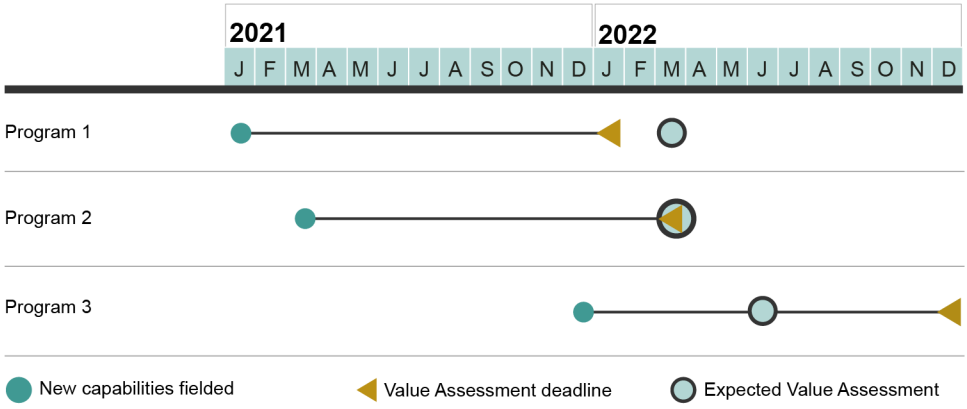
View GAO-22-104695. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov.

What GAO Found

In response to previous GAO recommendations, Cyber Command—the Department of Defense (DOD) command responsible for cyberspace operations—is maturing its Joint Cyber Warfighting Architecture (JCWA) to integrate systems that enable the cyber warfighting mission. In December 2020, the command identified JCWA roles and responsibilities, and, in September 2021, it approved a JCWA Concept of Operations to define interoperability goals and intended outcomes of the programs.

Cyber Command has initiated efforts to assess JCWA acquisitions. DOD policy requires outcome-based evaluations, called Value Assessments, for programs within 1 year of fielding capabilities to determine whether they result in mission outcomes that are worth the investment. DOD clarified its Value Assessment guidance after GAO raised Cyber Command's confusion regarding its role in scheduling these assessments. The command subsequently initiated the JCWA program Value Assessments, once it understood it was responsible for doing so, and these assessments were underway as of March 2022 (see figure).

Joint Cyber Warfighting Architecture Acquisition Program Value Assessment Timelines



Source: GAO review of program documents and interviews with program officials. | GAO-22-104695

Cyber Command has not yet developed required outcome-based metrics to support the Value Assessments. DOD policy and guidance call for such metrics to help programs understand mission improvements. For example, measuring improvements in the speed of operations could help Cyber Command determine whether programs are delivering intended outcomes. The command has been slow to determine metrics, in part because of inexperience conducting Value Assessments and the challenge of accounting for other factors—like new cyber operations tactics—on mission outcomes. Though this process is new, DOD guidance encourages experimentation and learning, so that metrics can continue to be refined over time. While the command is unlikely to have outcome-based metrics for the first three assessments that are underway, there is sufficient time for it to do so for those it has not yet initiated. If Cyber Command does not develop outcome-based metrics to inform future Value Assessments, it risks not being able to understand whether and how new capabilities benefit the cyber warfighting mission.