GAO@100 Highlights

Highlights of GAO-21-179, a report to congressional committees

March 2021

WEAPON SYSTEMS CYBERSECURITY

Guidance Would Help DOD Programs Better Communicate Requirements to Contractors

Why GAO Did This Study

DOD's network of sophisticated, expensive weapon systems must work when needed, without being incapacitated by cyberattacks. However, GAO reported in 2018 that DOD was routinely finding cyber vulnerabilities late in its development process.

A Senate report accompanying the National Defense Authorization Act for Fiscal Year 2020 included a provision for GAO to review DOD's implementation of cybersecurity for weapon systems in development. GAO's report addresses (1) the extent to which DOD has made progress in implementing cybersecurity for weapon systems during development, and (2) the extent to which DOD and the military services have developed guidance for incorporating weapon systems cybersecurity requirements into contracts.

GAO reviewed DOD and service guidance and policies related to cybersecurity for weapon systems in development, interviewed DOD and program officials, and reviewed supporting documentation for five acquisition programs. GAO also interviewed defense contractors about their experiences with weapon systems cybersecurity.

What GAO Recommends

GAO is recommending that the Army, Navy, and Marine Corps provide guidance on how programs should incorporate tailored cybersecurity requirements into contracts. DOD concurred with two recommendations, and stated that the third—to the Marine Corps—should be merged with the one to the Navy. DOD's response aligns with the intent of the recommendation.

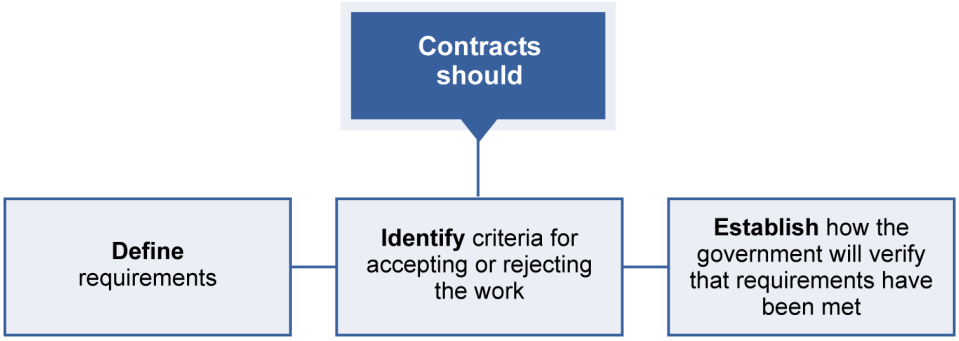
View GAO-21-179. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov.

What GAO Found

Since GAO's 2018 report, the Department of Defense (DOD) has taken action to make its network of high-tech weapon systems less vulnerable to cyberattacks. DOD and military service officials highlighted areas of progress, including increased access to expertise, enhanced cyber testing, and additional guidance. For example, GAO found that selected acquisition programs have conducted, or planned to conduct, more cybersecurity testing during development than past acquisition programs. It is important that DOD sustain its efforts as it works to improve weapon systems cybersecurity.

Contracting for cybersecurity requirements is key. DOD guidance states that these requirements should be treated like other types of system requirements and, more simply, "if it is not in the contract, do not expect to get it." Specifically, cybersecurity requirements should be defined in acquisition program contracts, and criteria should be established for accepting or rejecting the work and for how the government will verify that requirements have been met. However, GAO found examples of program contracts omitting cybersecurity requirements, acceptance criteria, or verification processes. For example, GAO found that contracts for three of the five programs did not include any cybersecurity requirements when they were awarded. A senior DOD official said standardizing cybersecurity requirements is difficult and the department needs to better communicate cybersecurity requirements and systems engineering to the users that will decide whether or not a cybersecurity risk is acceptable.

Incorporating Cybersecurity in Contracts



Source: GAO analysis of DOD information. | GAO-21-179

DOD and the military services have developed a range of policy and guidance documents to improve weapon systems cybersecurity, but the guidance usually does not specifically address how acquisition programs should include cybersecurity requirements, acceptance criteria, and verification processes in contracts. Among the four military services GAO reviewed, only the Air Force has issued service-wide guidance that details how acquisition programs should define cybersecurity requirements and incorporate those requirements in contracts. The other services could benefit from a similar approach in developing their own guidance that helps ensure that DOD appropriately addresses cybersecurity requirements in contracts.