WEAPON SYSTEMS CYBERSECURITY

Guidance Would Help DOD Programs Better Communicate Requirements to Contractors

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

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 incorporate 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.

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

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