GAO@100 Highlights

Highlights of GAO-22-104679, a report to congressional committees

December 2021

DEFENSE CONTRACTOR CYBERSECURITY

Stakeholder Communication and Performance Goals Could Improve Certification Framework

Why GAO Did This Study

DOD relies on thousands of defense contractors for goods and services ranging from weapon systems to analysis to maintenance. In doing business with DOD, these companies access and use sensitive unclassified data. Accordingly, the department has taken steps intended to improve the cybersecurity of this defense industrial base.

A Senate report included a provision for GAO to review DOD's implementation of CMMC. This report addresses (1) what steps DOD took to develop CMMC, (2) the extent to which DOD made progress in implementing CMMC, including communication with industry, and (3) the extent to which DOD has developed plans to assess the effectiveness of CMMC.

GAO reviewed DOD documents related to the design and implementation of CMMC and interviewed DOD officials involved in designing and managing it. GAO also interviewed representatives from defense contractors, industry trade groups, and research centers.

What GAO Recommends

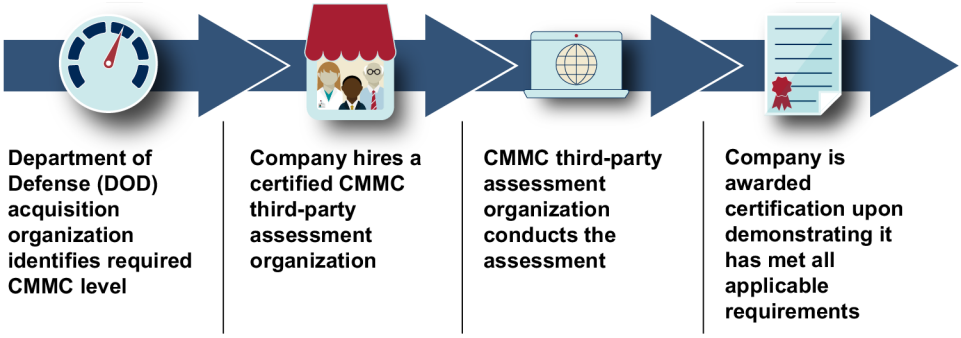
GAO is making three recommendations to DOD to improve communication to industry, develop a plan to evaluate the pilot, and develop outcome-oriented performance measures. DOD concurred with the recommendations and outlined plans to address them in CMMC 2.0.

View GAO-22-104679. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov, Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov, or Jennifer R. Franks at (404) 679-1381 or franksj@gao.gov.

What GAO Found

For years, malicious cyber actors have targeted defense contractors to access sensitive unclassified data. In response, since 2019, the Department of Defense (DOD) has engaged with a range of stakeholders to develop and refine a set of cybersecurity practices and processes for contractors to use to help assure security of the data. For relevant contracts, this Cybersecurity Maturity Model Certification (CMMC) requires that defense contractors implement these practices and processes on their information systems and networks.

Key Steps in CMMC Verification Process



Source: GAO summary of DOD's Cybersecurity Maturity Model Certification (CMMC) implementation activities. | GAO-22-104679

DOD began CMMC implementation with an interim rule that took effect in November 2020, but the rollout of the 5-year pilot phase is delayed. For example, DOD planned to pilot the CMMC requirement on up to 15 acquisitions in fiscal year 2021 but has not yet included the requirement in any acquisitions, in part due to delays in certifying assessors. Industry—in particular, small businesses—has expressed a range of concerns about CMMC implementation, such as costs and assessment consistency. DOD engaged with industry in refining early versions of CMMC, but it has not provided sufficient details and timely communication on implementation. Until DOD improves this communication, industry will be challenged to implement protections for DOD's sensitive data.

DOD has identified plans to assess aspects of its CMMC pilot, including high-level objectives and data collection activities, but these plans do not fully reflect GAO's leading practices for effective pilot design. For example, DOD has not defined when and how it will analyze its data to measure performance. Further, GAO found that DOD has not developed outcome-oriented measures, such as reduced risk to sensitive information, to gauge the effectiveness of CMMC. Without such measures, the department will be hindered in evaluating the extent to which CMMC is increasing the cybersecurity of the defense industrial base.

In November 2021, DOD announced CMMC 2.0, which includes a number of significant changes, including eliminating some certification levels, DOD-specific cybersecurity practices, and assessment requirements. DOD also announced that it intended to suspend the current CMMC pilot and initiate a new rulemaking period to implement the revised framework.