GAO Highlights

DEFENSE CONTRACTOR CYBERSECURITY

DOD Should Address External Factors That Could Impede Program Implementation

GAO-26-107955 March 2026

A report to congressional committees.

For more information, contact: Joseph W. Kirschbaum at KirschbaumJ@gao.gov; Vijay A. D'Souza at DsouzaV@gao.gov; or W. William Russell at RussellW@gao.gov.

What GAO Found

The Department of Defense (DOD) established the Cybersecurity Maturity Model Certification (CMMC) program in 2020 to ensure that defense industrial base (DIB) companies comply with cybersecurity requirements. In response to concerns about the complexity of the program's initial framework, in 2024 DOD streamlined requirements and revised program implementation plans.

DOD plans to implement this program over the next 3 years. Although DOD does not have a strategic plan for the CMMC program recorded in a single document, it has developed several planning documents to guide implementation. GAO found that DOD's implementation plans addressed six of seven key elements of a comprehensive strategy, as shown in the figure below.

Extent That DOD's Plans for the CMMC Program Rollout Addressed Key Elements of a Comprehensive Strategy, as of September 2025

Elements of a comprehensive strategy	GAO assessment
Mission statement	✓
Problem definition, scope, and methodology	✓
Goals and objectives	✓
Activities, milestones, and performance measures	✓
Resources and investments	✓
Organizational roles, responsibilities, and coordination	✓
Key external factors that could affect goals	!

✓ Addressed: DOD documentation includes evidence that satisfies the element.

! Partially addressed: DOD documentation includes evidence that satisfies some, but not all, of the element.

✗ Not addressed: DOD documentation includes no evidence that satisfies any of the element.

Sources: GAO analysis of Department of Defense (DOD) information, and all icon illustrations. | GAO-26-107955

DOD partially addressed the element related to identifying key external factors that could affect the program's ability to meet its goals. While DOD has taken steps to develop strategies to address program risks, it has not systematically assessed and documented the external factors that could affect the department meeting its goals. For example, the department relies on private sector stakeholders to conduct assessments of DIB companies to determine if they comply with the program's requirements. However, DOD did not assess and document how it intends to mitigate the risk of private sector capacity being insufficient to meet its needs for assessments, according to DOD officials.

Although DOD officials told GAO that department leaders can issue waivers if external factors cause significant challenges, such waivers would not address underlying challenges. Additionally, depending on the frequency and number of waivers DOD uses, the process could undermine the long-term viability of the CMMC program and its intent to verify that companies are implementing federal cybersecurity requirements. By assessing and documenting key external factors and developing approaches to address them, DOD would better understand program implementation risks and be better positioned to take action to mitigate those risks.

Why GAO Did This Study

DOD relies on hundreds of thousands of private companies for goods and services, ranging from weapon systems to maintenance. In doing business with DOD, these companies often use and store sensitive information in their computer systems. Malicious cyber actors have targeted defense contractors' networks and systems to access sensitive DOD data.

Senate Report 118-188, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2025, includes a provision for GAO to review DOD's implementation of the revised CMMC program. GAO's report evaluates, among other things, the extent to which DOD has a comprehensive strategy to guide implementation.

GAO reviewed DOD's CMMC policies and planning documentation and interviewed DOD officials involved in implementing and managing this program. GAO also interviewed DOD officials and industry representatives who support DIB companies to implement CMMC requirements.

What GAO Recommends

GAO recommends that DOD document key external factors that could significantly affect the CMMC program and develop approaches to address these factors. DOD concurred with the recommendation.