Palantir

Cybersecurity Maturity Model Certification (CMMC) Fact Sheet

A CRITICAL REQUIREMENT FOR ALL DEFENSE CONTRACTS

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a program to enhance the cybersecurity posture of companies seeking to do business with the Department of Defense (DoD) and its contractors and subcontractors. The DoD employs CMMC to assess whether a company possesses the necessary security measures to handle defense-related contracts. This assessment is particularly crucial for companies that store, process, or transmit Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) for defense-related contracts.

Why 76K+ Companies Can't Ignore CMMC

CMMC is a crucial accreditation for any company involved in defense-related contracts, as it is required for those that store, process, or transmit Controlled Unclassified Information (CUI) or Federal Contract Information (FCI). ***This requirement extends to all prime contractors and subcontractors.***

DoD estimates that 76,598 companies will need to complete a Level 2 Certification Assessment. The scope of CMMC Accreditation is comprehensive, covering any location where CUI or FCI is held, stored, or processed, such as emails, internal corporate document repositories, physical office spaces, and any software employed to handle government CUI or FCI.

The significance of CMMC is reflected in the U.S. federal government's annual spending of approximately $100 billion on software. Holding this accreditation is necessary for companies seeking to win these contracts.

When Does CMMC Go into Effect?

CMMC is scheduled to begin its rollout this year. Beginning in Q3 2025, new contracts issued by DoD will incorporate a requirement for CMMC compliance.

It's important to note that the process to obtain CMMC accreditation can be both costly and time-consuming, likely exceeding the timeframe allocated for its implementation. Organizations should begin preparing well in advance to ensure they meet the necessary requirements by the time these compliance measures are enforced.

What Is the CMMC Process?

The CMMC process involves a rigorous evaluation that every defense contracting company must undergo with an authorized CMMC Third Party Assessment Organization (C3PAO). This assessment meticulously examines all locations where CUI and FCI are stored by the company in order to determine whether the necessary security and compliance controls have been met. ***For all cloud-hosted components used in processing CUI, these components effectively must be FedRAMP authorized, or they cannot be used.***

How to Successfully Navigate CMMC Compliance

To ensure your company remains competitive and compliant with DoD requirements, it is crucial to develop a strategic plan to meet CMMC standards. Failure to do so could jeopardize your current and future engagements with the DoD. If you are a cloud service provider, a significant hurdle will be achieving FedRAMP Authorization, which is required for SaaS applications under CMMC. Without this authorization, your ability to remain compliant and operational is at risk.

Palantir FedStart offers a streamlined solution, providing an expedited path to secure FedRAMP Authorization in as little as three months, compared to the average timeline of 18-24 months without FedStart. This accelerated approach is highly effective and may be the best option to achieve full CMMC compliance for your SaaS application within the current year. Typically, obtaining FedRAMP Authorization is time-consuming and costly, but FedStart significantly reduces both the time and financial investment required, ensuring your technology remains aligned with DoD standards efficiently and effectively.

Looking for CMMC compliance for your SaaS application? Get in touch with the Palantir FedStart team by emailing FedStart@palantir.com.