FORTIFY

White Paper | 2025

Cybersecurity Maturity Model Certification

+ Mandate and Implementation Overview

Managing Partner | Co-Founder
Tyler Imig

Partner | Co-Founder
Blake Meyer

Partner | Co-Founder
David Borsodi

224-334-1399
www.fortifycompliance.com

SITUATION

Cybersecurity threats are increasing exponentially. The US Government sees this as a threat to their internal data. Their internal IT systems are tightly controlled and are still attacked and penetrated, daily, by private and nation-state adversaries.

The US GOV uses the services and products of over 70,000 private businesses which necessitates the transfer of information between the government entities and private vendors. A wide spectrum of data becomes vulnerable when it leaves the US GOV IT infrastructure, and this information can include tech data for lethal defense technology, shipping information, or other data critical to the security of the United States. For a multitude of reasons, all of this information is sensitive.

The Cybersecurity Maturity Model Certification (CMMC) has been implemented by the US GOV in order to safeguard information that passes between US GOV and private business vendors. There are five tiers of security standards that are dictated by the agency or entity that is the government touchpoint with the vendor. For example, a lethal technology company could be required to maintain CMMC LVL 2, due to the sensitive technology transfer. Any business that is in a federal contract, whether for services or acquisition of goods, has a minimum requirement to meet CMMC LVL1 standards in order to protect Federal Contract Information (FCI).

Compared to the large, prime contractors such as Lockheed Martin or Boeing, small businesses with relevant products, technology, or services will be disproportionally affected. Smaller-scale contractors are required to bear the same CMMC burden as the larger, prime contractors but small companies do not typically have large, in-house IT teams, nor do they have large, discretionary funds for unforeseen compliance requirements. These mandates have the potential to crush small businesses.

CHALLENGE

Achieving CMMC standards takes a substantial amount of time and money to complete. As an example, consider a business that is approximately 10 employees and does not already have an IT Security system in place. Approximate figures are $150k for CMMC LVL 1 and $800k for CMMC LVL 2. Furthermore, CMMC LVL1 takes approximately 9-12 months to complete, while LVL 2 requires an additional year after that. The timeline is proportionate to the size of the business and their ability to adopt the system.

The requirement for CMMC LVL 1 Compliance is required by Q2 2025. CMMC LVL 2 compliance is required by October 1st, 2025. The project duration for LVL 2 is approximately 12 months, in addition to the LVL 1 processes. To further exacerbate the problem, there are a highly limited number of professionals that are qualified to manage or certify the CMMC compliance process. If a business is not compliant by the deadline, the government may freeze or cancel their contracts. A business will not win a new contract if they are not compliant.

Within the next 2-5 years, there is going to be a significant cybersecurity demand, creating a bottleneck within the small community of firms who provide these services. Costs for CMMC services will increase and timelines will extend as queues lengthen. Creating additional strain, approximately 90% of the 70,000 businesses are unaware of the mandate, or even of the existence of CMMC. This means they have not budgeted for this significant expense that is required to continue doing business with the government.

SOLUTION

Fortify Complianc serves as a liaison between defense contractors and Socium IT Solutions, in order to provide the most streamlined path to compliance. The CMMC effort has both active and passive phases. The IT Security Specialists will do the bulk of the work in the background, without any major daily inputs from contractors or their teams. Some steps of the process, however, require behavioral changes from teams, leadership, and staff in order to maintain compliance in case of an audit.

We are also working to establish financing options for the CMMC efforts for businesses that cannot allocate significant portions of their budget to this process with little-to-no notice.

The CMMC project, no matter which level, has easily defined project milestones and endpoints.