carahsoft

TECHNOLOGY BRIEF

Understanding CMMC for Implementation Today

Evolving methods of cyberattacks require evolving methods of security, from the smallest steps to larger process overhauls. For the Department of Defense, security is a two-way street—not only must agencies and organizations adhere to security protocols, but companies that provide technology to or host information for the DoD need to follow the same standard security strictness. However, not every company will have the same level of security in place, due to their size, budget, or other factors. Without a way to standardize and enforce cybersecurity standards, Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) is at risk of compromise across the Defense Industrial Base (DIB). As a result, the Department of Defense (DoD) drafted a solution in 2019 to unify and standardize cybersecurity requirements for all companies.

CMMC EXPLAINED

The Cybersecurity Maturity Model Certification, or CMMC, is a proposed cybersecurity standardization framework by the Department of Defense, which must be followed by any company engaged in business with the DoD. This framework features three compliance levels—Foundational, Advanced, and Expert—that follow the cybersecurity standards of the National Institute of Standards and Technology (NIST). The certification level that a company must achieve will be determined at the contract level depending on the sensitivity of the information handled in fulfilling the contract. Furthermore, assessments at each level help the DoD verify that a company complies with the requirements of the relevant maturity level.

While the CMMC is still under review, companies are moving forward with implementing the new security standards to proactively achieve CMMC compliance. A breakdown of the framework levels—while highlighting solutions that can aid with each capability domain—can make the transition to CMMC compliance simple to both understand and implement.

CMMC FRAMEWORK LEVELS OF MATURITY

LEVEL 1

This is the base, or Foundational, level of cyber hygiene, where organizations must perform basic security practices focused on protecting Federal Contract Information (FCI). Level 1 features 14 security practices to ensure basic safeguarding of assets that process, store, or transmit FCI. Additionally, an annual self-assessment with certification by company leadership is required at Level 1 demonstrate compliance with the DoD security standards.

LEVEL 2

This level is for Advanced cybersecurity methods, with DIB organizations engaging in 110 universally-accepted best practices aligned with NIST SP 800-171. Companies at Level 2 are broadly protecting CUI, with cybersecurity procedures that are both advanced and sophisticated. Assessment requirements are split into two groups for Level 2 certification. One group will perform an annual self-assessment with certification by company leadership, consistent with the Level 1 assessment requirement. The remaining companies will be required to conduct an assessment by a third-party assessment organization every three years. These third party organizations will be certified by the CMMC Assessment Board (CMMC-AB) and report all assessments to the DoD, while companies will be responsible for obtaining their assessment and level certification.

LEVEL 3

The final CMMC framework level, Level 3 is for Expert cyber hygiene. Cybersecurity at Level 3 is in-depth and highly advanced, as it includes all previous security requirements from Levels 1 and 2 while going beyond the 110 practices and will be based on NIST SP 800-172. Maturity Level 3 is focused on protection of CUI and reducing risk from Advanced Persistent Threats (APTs). At this level, the government conducts triennial assessments on companies to ensure that all outlined procedures are followed and adhered to. The DoD will expand on Level 3 information as the rulemaking process unfolds and they work towards creating assessment requirements suitable for critical information.

COUNT ON CARAHSOFT FOR CMMC

Many of Carahsoft's partners are equipped to handle CMMC needs, with coverage for all 14 capability domains across the 3 CMMC maturity levels. The following technology enables any company to adhere to CMMC compliance, while safeguarding the critical information and infrastructure that makes up their business.

Featured CMMC Technology Vendors →

CMMC Portfolio

Microsoft | RSA | Quzara Cloud. Security. Analytics. | FORESCOUT
BeyondTrust | CYTURUS | druva | f5
FORTINET | vmware | Infoblox | Lookout
zscaler | paloalto NETWORKS | proofpoint | qmulos
tenable | THALES Building a future we can all trust | TREND MICRO | Trustwave Government Solutions