How new CMMC requirements will affect your organization

The Department of Defense Office of the Undersecretary of Defense for Acquisition and Sustainment has developed a new certification framework to address the risks posed by contractors with inadequate cybersecurity controls. The new Cybersecurity Maturity Model Certification (CMMC) provides a five-level, maturity-based approach to designating cybersecurity requirements. The DoD will begin including CMMC requirements in sections L and M of its requests for information in June 2020 and requests for proposals in September 2020, with implementation in contracts requiring CMMC certification spanning across the next few years.

Regardless, all DoD contractors and subcontractors within the defense industrial base, estimated to be around 300,000 organizations, will eventually be required to be independently audited and certified against one of the five CMMC maturity levels. Therefore, organizations should begin identifying gaps against their target maturity level and work to close those gaps to ensure they are ready in time for certification and minimize the risk of potential disqualifications if they are not certified when critical contract bids are released.

In this article, we outline some of what you should know about CMMC and what you should start doing to align your security processes, practices and controls with the CMMC requirements.

How does the CMMC work?

The CMMC provides a cohesive mechanism for the DoD to enforce its existing Defense Federal Acquisition Regulation Supplement requirements for safeguarding covered defense information and cyber incident reporting (DFARS clause 252.204-7012) across all contracts. While modeled after requirements from different frameworks, the CMMC continues to center around the National Institute of Standards and Technology Special Publication 800-171, the current standard for protecting controlled unclassified information (CUI).

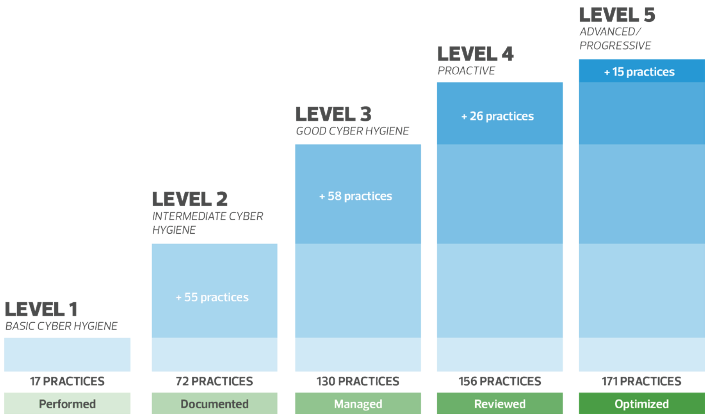
However, CMMC builds on NIST SP 800-171 by adding additional controls from other cybersecurity frameworks (e.g., 48 CFR 52.204-21, NIST CSF v1.1, ISO 27001, CIS 20 v7.1, CERT RMM v1.2) and providing a method for the DoD to certify an organization's cybersecurity maturity level from a range of 1—5.

The DoD's contracting agency will assign a CMMC level to each contract. The levels will be determined based on the technical practices and process maturity that the agency feels are necessary to protect the in-scope information and information systems. The CMMC organizes 171 cybersecurity controls across the five maturity levels, which are divided into 17 domains. These domains should be familiar to organizations that have aligned with NIST SP 800-171 or Federal Information Processing Standards 200 requirements in the past.

DoD CMMC domains				
Access control	Asset management	Audit and accountability	Awareness and training	Configuration management
Identification and authentication	Incident response	Maintenance	Media protection	Personal security
Physical protection	Recovery	Risk management	Security assessment	Situational awareness
System and communications protections				System and information integrity

Organizations will become certified based on the level of risk to CUI and federal contract information (FCI) by maintaining the full set of controls at the desired level. In order to pursue a new DoD contract, organizations will be required to be certified at or above the level specified in the contract. Organizations handling CUI and already subject to DFARS or NIST 800-171 requirements will be expected to be certified for at least CMMC level 3.

The following chart outlines the CMMC maturity level requirements:



What if we already comply with existing DFARS or NIST 800-171 requirements?

Organizations that already meet the requirements within NIST 800-171 are well-positioned to become certified at CMMC level 3. At 130 controls, this level will use the existing NIST 800-171 requirements and add 20 more controls across a range of areas including:

- Identifying, categorizing, labeling and handling of all CUI data
- Collecting and reviewing audit logs in a centralize repository
- Detecting, analyzing, triaging and reporting of events
- Developing predefined procedures for responding to incidents
- Storing data backups off-site and offline, and regularly testing the backups
- Reviewing code of internally-developed enterprise software
- Receiving and responding to cyberthreat intelligence from information sharing sources
- Requiring encrypted sessions when managing network devices
- Implementing domain name system (DNS) filtering
- Employing email protections including spam filtering, email encryption and sandboxing of potentially malicious email

What should our organization do to prepare for CMMC?

Doing nothing is not an option if you currently do business with the DoD or plan on doing so in the near future. Although there is still some uncertainty around CMMC, many details have already been published in the requirements, appendices and presentations by the DoD. This information is enough for the industry to begin preparing for CMMC while the remaining details are being finalized in the spring of 2020. We recommend that you take the following actions in the coming weeks and months:

- Identify the business processes, applications, supporting systems and databases that support your DoD-related contracts and seek to consolidate the processes and data onto as few systems as practical to reduce your compliance footprint of in-scope systems.
- If you are a subcontractor, reach out to your customer(s) to see if they have received guidance on what certification level they anticipate will be required for your contracts. If you handle CUI or covered defense information (CDI) and already must comply with DFARS, you should anticipate at least level 3-maturity certification.
- Conduct a detailed gap assessment between your current cybersecurity governance practices and technical capabilities and your anticipated maturity level requirements.
- Develop and execute a plan to remediate the identified gaps.

How can a third party assist your compliance with CMMC requirements?

With potentially 300,000 organizations falling under scope for CMMC, you are not alone in navigating the process changes and costs associated with complying with a new framework. However, the assistance and government contracting insight from an experienced third party can help you understand CMMC and turn aligning your information security posture into a more a manageable task.

A qualified CMMC advisor can help you build a repeatable, efficient process for achieving and sustaining compliance. This helps assure federal clients that you protect CUI in nonfederal systems, enabling you to maintain current and win new government contracts.

For example, the right advisor can help you with the following to not only get you ready for CMMC certification but also to identify opportunities to minimize scope and right-size your cybersecurity program:

- Assess and consult on:
  - Business processes that are related to storage, transmission and processing of CUI, FCI and other covered defense information
  - How data flows through the environment to identify and advise on tailoring your scope of systems that must be certified
  - The design and implementation of security practices and controls against your anticipated CMMC maturity level requirements
- Provide remediation steps and activities to set you on the path towards increasing maturity
- Develop and implement policies, processes and technologies required to close any compliance gaps that you've identified

We recommend that you take a look at whether you are currently handling CUI and your strategic goals regarding DoD contracts. If you plan to pursue a DoD contract in the future, an outside advisor is often a key element to set your company on a smooth path towards CMMC maturity.

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM