Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Strategy to Get Started with an Information Security Program

The CMMC is here:
What you need to know about Dept. of Defense Contractor Cybersecurity Requirements

Patrick Rost prost@dopkins.com

KEY TAKEAWAYS IF YOUR TIME IS SHORT:

A new Cybersecurity protocol is headed its way to Department of Defense Contractors. Even entities that were previously compliant with the Department of Defense contract requirements may have work to do before being able to become CMMC Certified. Those that were not previously compliant have an even longer road ahead.

4 key considerations:

1. CMMC certification is not the same as DFARS/NIST 800-171.
2. Will you be CMMC Certified in time to be awarded DoD contracts?
3. Even with practices implemented, contractors will be required to have processes to support them.
4. CMMC will be rolled out between now and 2026, you may need that time to prepare.

Introduction

Published September 26, 2021 –If your business is a Department of Defense Contractor, you may have heard about a new cybersecurity certification in effect. In essence, your organization will soon be required to be in compliance with new guidance**. Being certified is critical, or else you might lose some opportunities for lucrative government contracts.**

Known as the Cybersecurity Maturity Model Certification, CMMC was developed by the United States Department of Defense (DoD). **The rollout phases went into effect on November 30, 2020**.

The CMMC is meant to protect against the theft of intellectual property and sensitive information within the Defense Industrial Base (DIB). In effect as of last November, the CMMC will be implemented using a **phased rollout between 2021 and 2026** with all contractors within the DIB needing to be certified by **2026 at the latest**. CMMC is based on, and **replaces the previous requirements** of, Defense Federal Acquisition Regulation Supplement (DFARS) and National Institute of Standards and Technology (NIST) 800-171.

Going forward, **contractors will now need to be certified** at the required CMMC Level **prior to receiving contracts** from the DoD. CMMC Levels 1-5 replace all prior self-reporting guidelines, including the prior list of 110 requirements you might be familiar with from the current governance.

If your company provides any goods or services to the Department of Defense, this post highlights what the CMMC is, why it's important, and what you need to do to prepare for it.

Certification – Before & After

First, a little of the technical backstory might be helpful to explain the current protocols that are being phased out. Before CMMC was introduced:

- Contractors were governed by (1) Federal Acquisition Regulations (FAR) for government contracts and additionally by (2) Defense Federal Acquisition Regulations Supplement (DFARS) for defense contracts.
- When a contractor signed a contract that dealt with Federal Contract Information (FCI) they were to "self-certify" they were compliant with FAR. The same situation was to occur for contracts that dealt with Controlled Unclassified Information (CUI) "self-certifying" with DFARS which includes NIST 800-171. Contractors that signed a contract with the federal government were to state they are following these regulations even if there is not wording in the contracts around FCI/CUI. This is known as the Christian Doctrine, where the contract clause can be included even if it is excluded from the contract itself. Any contractor that was later found to not be compliant with FAR/DFARS would be assessed treble damages after the fact.

That was the old way. Here's where Certification is headed under the CMMC:

The Department of Defense decided that just collecting fines for noncompliance after the fact was no longer acceptable, which led to the creation of CMMC. New contracts will have CMMC requirements and contractors will not be awarded the contract unless they are already certified at the appropriate Level 1-5. Certification must occur before being awarded a contract. For example, contractors that handle FCI will now need to be certified at CMMC Level 1 and contractors that handle CUI will now need to be certified at CMMC level 3 or above. The chart below identifies the five (5) CMMC Levels:

CMMC Level 1 – Safeguard Federal Contract Information (FCI)
- Processes are performed
- Practices are considered "Basic Cyber Hygiene"

CMMC Level 2 – Transition to Level 3
- Processes are documented
- Practices are considered "Intermediate Cyber Hygiene"

CMMC Level 3 – Protect Controlled Unclassified Information (CUI)
- Processes are managed
- Practices are considered "Good Cyber Hygiene"

CMMC Level 4 – Additional protection of CUI and reduce risk of Advanced Persistent Threats (APTs)
- Processes are reviewed
- Practices are considered "Proactive"

CMMC Level 5 – Additional protection of CUI and reduce risk of Advanced Persistent Threats (APTs)
- Processes are optimized
- Practices are considered "Proactive/Advanced"

Maturity

Another way that CMMC is different is with the addition of maturity, which is used to track progression through the five levels:

- Progression is measured against **practices**, like under NIST 800-171, and will also add processes as a new requirement
- **Processes** are defined as the way in which practices are implemented, documented and maintained. They help assure that the contractor will maintain the level of security they are certified at for the duration of the three-year certification.

In addition, being CMMC certified not only states that a contractor has implemented the practices, but that they have implemented methods to repeat them consistently. Needless to say, this is a very complex process!

1. CMMC level 1 does not have any processes and only requires the practices at that level are implemented.
2. CMMC level 2 adds two processes that require implementation of a policy to cover each domain and to document the practices that implement the policy.
3. CMMC level 3 adds a process that requires establishing a plan that covers each domain.
4. Level 4 and 5 are advanced levels and each have an additional process.

Key Takeaway

While many contractors may be performing a large number of the practices required by FAR/DFARS/NIST 800-171, there is a high likelihood that most do not have sufficient documentation to support the process requirements of CMMC. This means that execution of the practices is not consistent or repeatable. ***Without implementing the processes, a contractor cannot become CMMC certified and will not be able to be awarded contracts.***

Additional controls/practices

CMMC is also more complicated because it adds further controls/practices to the current regulatory governance. **Contractors that are currently compliant with all of the controls in FAR/DFARS/NIST 800-171 will still have additional practices to evaluate.** The table below explains the number of new controls require for CMMC Levels 1, 2, and 3.

ORIGNAL-pre CMMC		NEW, Under CMMC		
Original Governance	**Original Number of Controls**	**CMMC Type**	**Number of controls**	**Total Number of controls**
FAR	15	Level 1	Original 15 (FAR) **+ 2 NEW**	**17**
		Level 2	"Stepping Stone" to Level 3	**72**
NIST 800-171	110	Level 3	Original 110 (NIST) **+ 20 NEW**	**130**

Putting it all Together

The pathway to CMMC is a detailed process, and definitely one you want to get right in order to maintain your current inflow of government projects. To navigate this system, DoD contractors are recommended to work with a Registered Provider Organization (RPO) to begin the process to become CMMC compliant.

If you would like to have a conversation about the implications of CMMC for your organization, please contact ***Patrick Rost, CISSP, CMMC-AB RP*** *(prost@dopkins.com). Check out our CMMC page for more information about CMMC and how we can assist your evaluation and preparation.*

Dopkins is a CMMC Registered Provider Organization (RPO) for companies doing business with the United States Department of Defense (DoD).