




CMMC IN A SMALL BUSINESS



BY CORE BUSINESS SOLUTIONS
CO-FOUNDER AND PRESIDENT




Welcome! This guide is designed to give you a high-level overview of the CMMC process and to briefly explain how Core Business Solutions can help you achieve CMMC compliance.

For contractors already required to comply with NIST SP 800-171, per DFARS 252.204-7012, DoD is now increasing accountability, instituting an assessment and reporting system to verify compliance before new contracts can be awarded. The DoD encourages affected contractors to begin their self-assessments immediately.

SCOTT
DAWSON





The launch of the Cybersecurity Maturity Model Certification (CMMC) program serves as an important and necessary step in the advancement of our country's ability to protect its people, military, industry, and more. Threats to our country's information grow by the day, and adversaries are becoming more capable. For businesses working with the Department of Defense (DoD), the threat grows.

In order for companies to be awarded government projects, they will need to employ several information security solutions, and put policies into place that drive action for their organizations. The DoD's new cybersecurity certification will require technical and organizational upgrades and good enough won't be good enough.

The rapidly approaching deadline for implementation means that defense industry contractors and subcontractors can't wait to get started.



AN INTRODUCTION TO **CMMC**

WHAT IS CMMC?

CMMC refers to the Cybersecurity Maturity Model Certification, a set of practices created to protect government information. Federal Contract Information (FCI) is protected by CMMC Level 1 and Controlled Unclassified Information (CUI) is protected by CMMC Level 2. CMMC Level 3 exists to protect highly sensitive CUI.

Published in January 2020 and revised in November 2021, CMMC is the third set of requirements issued by the DoD to achieve high-level information security within government contracts. Following the initially poor adoption of the DFARS 252.204-7012 regulation and lack in accountability of the initial NIST-SP 800-171 requirements, CMMC v2.0 implements a formal compliance process based on self-assessments (Level 1 and lower-priority Level 2), third-party assessments (higher-priority Level 2), and government assessments (Level 3). Without this certification, companies will be ineligible for work on DoD projects.

CMMC adopts the NIST program's 110 security controls, and rewrites DFARS to make a legally binding commitment to contractual requirements with both the Defense Industrial base as well as general defense contracts.

WHO WROTE IT & WHY?

CMMC was written by the Department of Defense.

WHO USES IT?

CMMC must be implemented by any company of any size who wishes to secure work on defense contracts, and it will be required throughout the defense supply chain. Even small businesses not working directly with the DoD, but who may provide a product or service to DoD contractors, will need to certify to CMMC.



WHY WAS IT CREATED?

The program allows the DoD to protect all sensitive information shared with contractors and sub-contractors from our nation's adversaries.

Historically, other governments seek out our defense information to defend and protect themselves against our military actions and/or to replicate our technology. From military aircraft development to training and communications, each piece of our defense plan that can be accessed puts our country at risk.

Due to the size and depth of the government's supply chain, the DoD isn't able to execute every project as a classified program. CMMC will set safeguards in place for over 300,000 suppliers that take part in the development, manufacturing, and execution of DoD-required products and services.

WHAT ARE THE BENEFITS?

If organizations wish to work with the DoD, or provide products or services to DoD contractors, they will be at risk of losing that business if not following the practices of CMMC v2.0.

Working toward CMMC guarantees your place in the valuable defense supply chain, opening up your company to opportunities with other DoD contractors and sub-contractors, and with the DoD itself.

WHO ISSUES THE CERTIFICATE?

For Level 2 contractors requiring formal assessment, certificates will be issued by independent, third-party auditors called Certified Third-Party Assessor Organizations (C3PAOs). C3PAOs will be trained and accredited by the DoD's CMMC Accreditation Body (CMMC-AB). Qualified C3PAOs will be listed on the CMMC-AB's "CMMC Marketplace" (<https://www.cmmcab.org/marketplace>). These third-party assessments occur every three years.

Note that for Level 3 contractors, this triennial assessment is performed by the government itself—not by a C3PAO.



WHO NEEDS TO BE INVOLVED?

All companies who contract or sub-contract on DoD contracts will be required to comply with or be certified to CMMC. In addition, third-party providers, such as managed service providers (MSPs) or cloud providers, may also need to be compliant if they interact with or host sensitive defense-related information.

IS THIS THE ONLY CERTIFICATION?

The CMMC program addresses DoD-related technical information (FCI and CUI) specifically. It does not cover your company's information such as, financials, employee personal identifying information (PII), or customer proprietary information - it is only designed to protect information related to DoD contracts.

Because it is not a complete cybersecurity solution, programs like ISO 27001 and NIST Cyber Security Framework still have their place when it comes to company protection. When combined with CMMC, these programs create a robust and complete protection system to keep your company information secure.

DOES IT APPLY TO ME?

With the far-reaching nature of the defense industry - from parts and production to services and intellectual property - there are more than 300,000 businesses that will need to comply with the CMMC program.

An easy signifier of the need to comply with CMMC is if a company receives any income for a defense-related contract whether as a prime contractor or subcontractor at any "level" of the supply chain. It's imperative for companies to carefully read their contracts to understand if and how they play a role in the whole defense supply chain.

Second, if a company is part of a DoD prime contract or subcontract through the handling of sensitive technical information (FCI or CUI), they too must comply with CMMC. Here, it's important for companies to understand what information is considered publicly available, and to have a firm understanding of what constitutes as program-defined FCI or CUI. Things like drawings, specifications, and procedures that may impact government work should be protected as such. If you have a question, or are unsure, speaking with your Contracting Officer would be a good first step.

Finally, in current contract review, if a company were to find reference to the DFARS 252.204-7012 - which requires compliance with NIST SP 800-171 - they too will be required to comply with CMMC and possibly receive third-party assessment.





WHAT REQUIREMENTS ARE INCLUDED?

CMMC v2.0 is divided into three levels of compliance. At the very least, DoD contractors who handle Federal Contract Information (FCI) must meet the 17 practices of Level 1 and submit a yearly self-assessment score to the Supplier Performance Risk System (SPRS) with affirmation from company leadership.

Level 1 involves foundational cybersecurity practices, and most companies will find that they already meet or almost meet these requirements.

CMMC Level 2 involves advanced cybersecurity. This is required by companies handling FCI and CUI. This level includes 110 practices to protect CUI, identical to the 110 controls of NIST SP 800-171.

CMMC Level 3 involves expert cybersecurity, and it requires an even larger set of controls, including a subset from NIST SP 800-172. These practices exist to protect highly sensitive CUI, and very few contractors will require this strict level of cybersecurity.

WHEN DOES THIS TAKE EFFECT?

The timeline isn't set in stone. These requirements could begin to appear in contracts as early as August 2022 or as late as November 2023. However, SPRS score submission should start immediately if you have contracts in place or on the horizon. For more information about or help with determining and submitting your score, you can contact Core Business Solutions for assistance.

NOW WHAT?

Preparing for CMMC can be a hefty to-do list, and you shouldn't wait to get started. Begin by performing an audit on your contracts and information you handle so that you're able to identify the information you will need to protect.

Most small businesses will benefit from the help of a consulting partner who has been trained on the CMMC process through the CMMC-AB. These Registered Provider Organizations (RPOs) can effectively and efficiently set up organizations with practical solutions to meet DoD requirements.



CMMC 1 LEVEL

CMMC Level 1 contains 17 practices. These represent good cyber hygiene for any business and may already be a part of your business practices whether you are CMMC compliant or not.

1 Use passwords and PINs to restrict log-on

Requirement text: "Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)."

2 Assign user access privileges to accounts

Requirement text: "Limit information system access to the types of transactions and functions that authorized users are permitted to execute."

3 Know the network you are connecting to and make sure it is secure

Requirement text: "Verify and control/limit connections to and use of external information systems."

4 Limit who and where you share/post information

Requirement text: "Control information posted or processed on publicly accessible information systems."

5 Make accounts for each employee

Requirement text: "Identify information system users, processes acting on behalf of users, or devices."

6 Use password authentication

Requirement text: "Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems."



7

Crush it, shred it, or overwrite it before you trash it

Requirement text: "Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse."

8

For your eyes only

Requirement text: "Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals."

9

No unauthorized entry and supervise visitors

Requirement text: "Escort visitors and monitor visitor activity."

10

Who accessed what information and when

Requirement text: "Maintain audit logs of physical access."

11

Know who has physical access, keep track

Requirement text: "Control and manage physical access devices."

12

Keep your computers inside the firewall

Requirement text: "Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems."

13

Setup/use a secure network for internet access

Requirement text: "Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks."

14

Install updates and run patches

Requirement text: "Identify, report, and correct information and information system flaws in a timely manner."

15

Use antivirus systems appropriately

Requirement text: "Provide protection from malicious code at appropriate locations within organizational information systems."

16

Subscribe for threat protection

Requirement text: "Update malicious code protection mechanisms when new releases are available."

17

Enable antivirus scans

Requirement text: "Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed."



CMMC LEVEL 2

CMMC Level 2 contains the 110 cybersecurity controls of NIST SP 800-171. Previous versions of CMMC included 20 additional practices, but these have been removed.



The CMMC model covers a wide range of cybersecurity topics across all three levels, such as:

- Access Control
- Audit & Accountability
- Awareness & Training
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System & Communication Protection
- System & Information Integrity

For Level 2, companies will self-assess or receive third-party assessment on their ability to meet and demonstrate all 110 practices. This will include technical architecture and solutions, along with written policies and procedures.

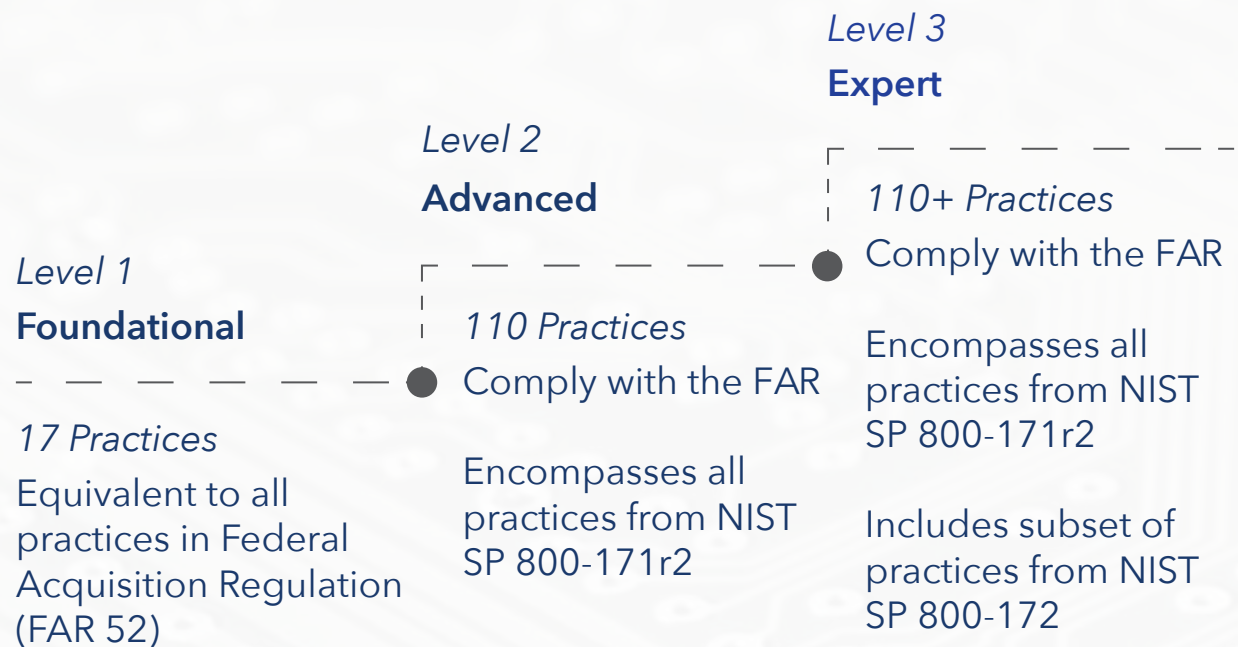
Organizations that are in the Defense Industrial Base and handle CUI must comply with at least CMMC Level 2.

CMMC LEVEL 3

CMMC Level 3 is for organizations that handle more confidential information and require a high level of security. Most companies will fall into either Level 1 or Level 2.



THE STRUCTURE OF CMMC (v2.0)



KEY POINTS ABOUT CMMC CERTIFICATION

- An RFP for the DoD will list the “CMMC Level” required on a contract by contract basis, with higher levels of compliance and security implementation required for jobs handling increasingly sensitive data.
- Level 1 contracts and lower-priority Level 2 contracts will require a yearly self-assessment with affirmation from company leadership. Higher-priority Level 2 contracts will require third-party assessments every three years.
- Plans of Action and Milestones (POAMS) will be allowed on a time-bound basis, but not for the highest weighted requirements.
- Waivers will be allowed on a limited basis and will require senior DoD approval
- Requirements for DoD contractors are continually changing, so check with us regarding the latest updates of what is required relating to CMMC.



CORE BUSINESS SOLUTIONS

— OFFERS COMPLETE —

CMMC CONSULTING SERVICES

Our **modular approach** breaks the CMMC v2.0 requirements down into organizational and technical aspects.

We assist you in a **guided self-assessment**, provide expert **online or onsite consulting services** to help you **develop your System Security Plan and POAM** and **lay out a roadmap and budget** for successful implementation and remediation.

Our goal is to help you implement a **sustainable cybersecurity system** that meets **CMMC requirements at the level you need**. Contact us today to learn more!





If you are interested in pursuing CMMC,
contact Core Business Solutions to talk to an
CMMC consultant today!



© Core Business Solutions, Inc.
Lewisburg, PA

866-354-0300 | info@thecoresolution.com
www.thecoresolution.com