




CMMC IN A SMALL BUSINESS



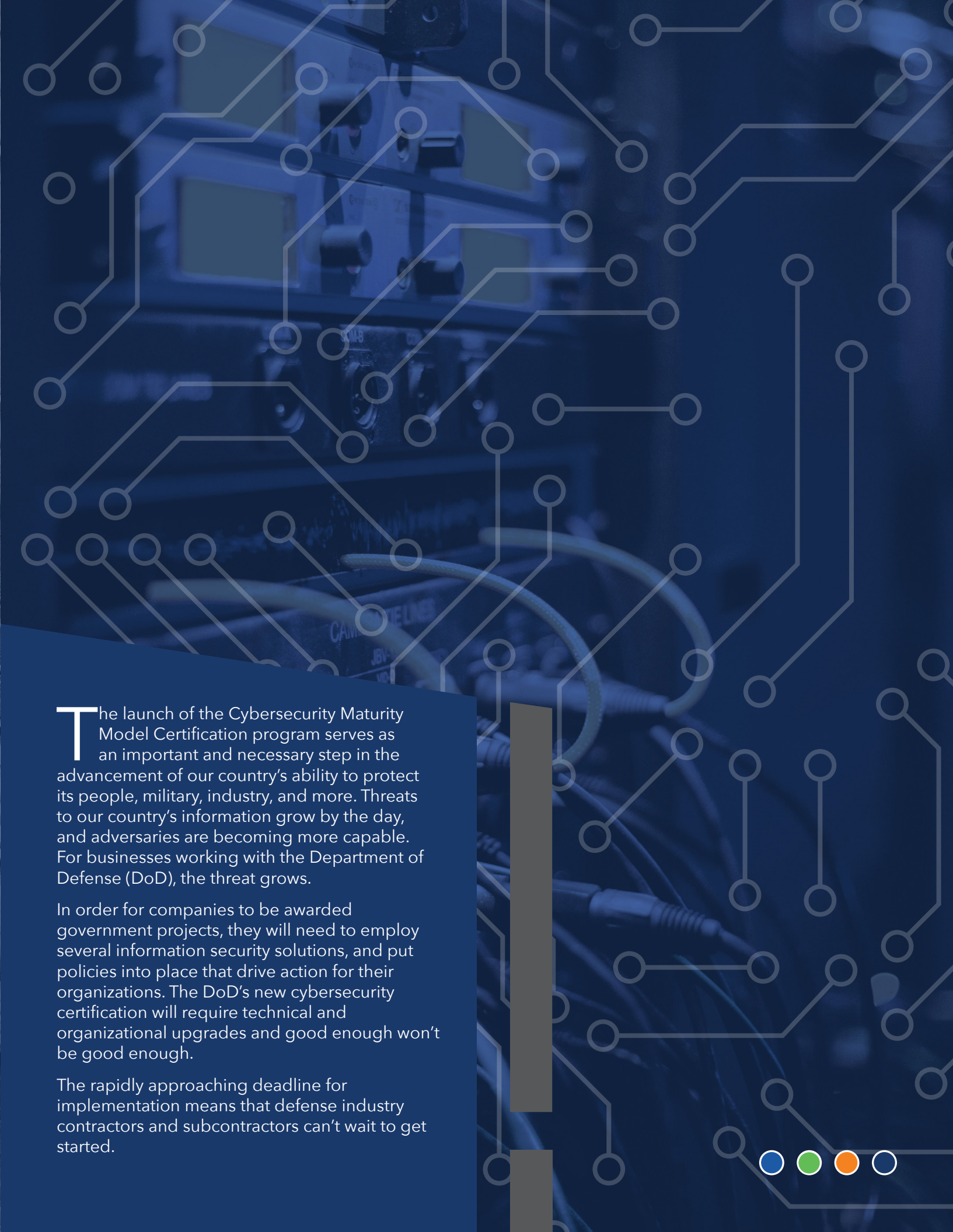
BY CORE BUSINESS SOLUTIONS
CO-FOUNDER AND PRESIDENT



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 holding contractors accountable, instituting an assessment and reporting system to verify compliance before new contracts can be awarded. While the new requirement is for information to be provided prior to contract award, DoD encourages affected contractors to begin their self-assessments immediately.

SCOTT
DAWSON



The launch of the Cybersecurity Maturity Model Certification 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 standards created and implemented to oversee the security of and protect government information. Specifically, Federal Contract Information (FCI) is controlled by CMMC Level 1 certification and Controlled Unclassified Information (w) is protected by CMMC certifications Levels 3-5.

Published in January of 2020, it 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 addresses these deficiencies and implements a formal certification - without which companies will be ineligible for work on government projects.

CMMC adds 20 new requirements to 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?

The 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 governmental defense contracts, and 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 contract will need to certify to CMMC.

WHY WAS IT CREATED?

The program allows the DoD to protect all sensitive information shared with contracts 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?

As early as January of 2021, government defense contracts will begin to require full compliance to CMMC. If organizations wish to work with the DoD, or provide products or services to contractor or subcontractor who works with the DoD, they will be at risk of losing that business if they are not CMMC certified.

Working toward CMMC certification 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?

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>).

Once a company has been audited, they will need to make any necessary corrections before receiving their certificate. Certification stands for three years at which time a re-evaluation of the company's controls will be performed by the third-party auditor. Unlike an ISO audit, annual audits are not required at this point.



WHO NEEDS TO BE INVOLVED?

All companies who contract or sub-contract on DoD contracts will be required to achieve CMMC certification. In addition, their third-party providers, such as managed service providers (MSPs) or cloud providers, who are involved in handling or hosting information management and technology may also need to be certified.

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 certify to the CMMC program.

An easy signifier of the need to certify to 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 certify to 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.

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 certify to the CMMC, either to replace NIST or in addition to compliance with it.

WHAT REQUIREMENTS ARE INCLUDED?

CMMC is divided into five levels of compliance. At the very least, DoD contractors and subcontractors whose contracts deal with Federal Contract Information (FCI) must meet the 17 controls of the first level (L1) and pass a one-day, on-site audit which will both check controls and ensure the company is US owned.

L1 involves basic cyber hygiene, and most companies will find that they already meet or almost meet L1 requirements.

Level 3 (CMMC L3) certification is required by companies handling FCI and CUI information. A big jump from L1, L3 includes 130 controls aimed at protecting CUI. Because of the large leap in requirements between L1 and L3, CMMC has included L2 as a benchmark for companies upgrading from L1 to L3 certification.

Levels 4 and 5, (L4 and L5) exist for a select and very small group of companies charged with handling sensitive and classified information that must be protected from Advanced Persistent Threats (APTs). Less than 1% of DoD contractors will need to meet these advanced certifications, and most are already well on their way to CMMC certification at their appropriate level.

WHEN DOES THIS TAKE EFFECT?

The DoD estimates that requirements will go in to effect on new and re-compete contracts issued beginning in January of 2021.

NOW WHAT?

Companies who need to certify to the CMMC are tasked with a hefty to-do list and 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 certification 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 LEVEL 1

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.

CMMC AC.1.001

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)."

CMMC AC.1.002

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."

CMMC AC.1.003

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."

CMMC AC.1.004

Limit who and where you share/post information

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

CMMC IA.1.076

Make accounts for each employee

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

CMMC IA.1.077

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."

CMMC MP.1.118

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."

CMMC PE.1.131

For your eyes only

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

CMMC PE.1.132

No unauthorized entry and supervise visitors

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

CMMC PE.1.133

Who accessed what information and when

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

CMMC PE.1.134

Know who has physical access, keep track

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

CMMC SC.1.175

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."

CMMC SC.1.176

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."

CMMC SI.1.210

Install updates and run patches

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

CMMC SI.1.211

Use antivirus systems appropriately

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

CMMC SI.1.212

Subscribe for threat protection

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

CMMC SI.1.213

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 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. Level 2 requires that organizations document certain **“intermediate cyber hygiene”** practices in order to protect CUI. The documentation of practices enables individuals to perform them in a repeatable manner.

You cannot certify to Level 2 but the requirements need to be met in CMMC Level 3 certification.

CMMC LEVEL 3

Practices found in CMMC Levels 1-3 (17 in Level 1, 55 in Level 2 and 58 in Level 3) include all 110 controls in NIST 800-171 plus an additional 20 requirements for a total of 130 practices. These practices are organized into 17 topics or “Domains.”

CMMC 17 CAPABILITY DOMAINS (v1.0)

The CMMC model has 17 domains, each of which includes a set of processes and capabilities that apply throughout the 5 maturity levels.

- | | | |
|------------------------------------|-------------------------|---------------------------------------|
| 1. Access Control | 7. Incident Response | 13. Risk Management |
| 2. Asset Management | 8. Maintenance | 14. Security Assessment |
| 3. Audit & Accountability | 9. Media Protection | 15. Situational Awareness |
| 4. Awareness & Training | 10. Personnel Security | 16. System & Communication Protection |
| 5. Configuration Management | 11. Physical Protection | 17. System & Information Integrity |
| 6. Identification & Authentication | 12. Recovery | |

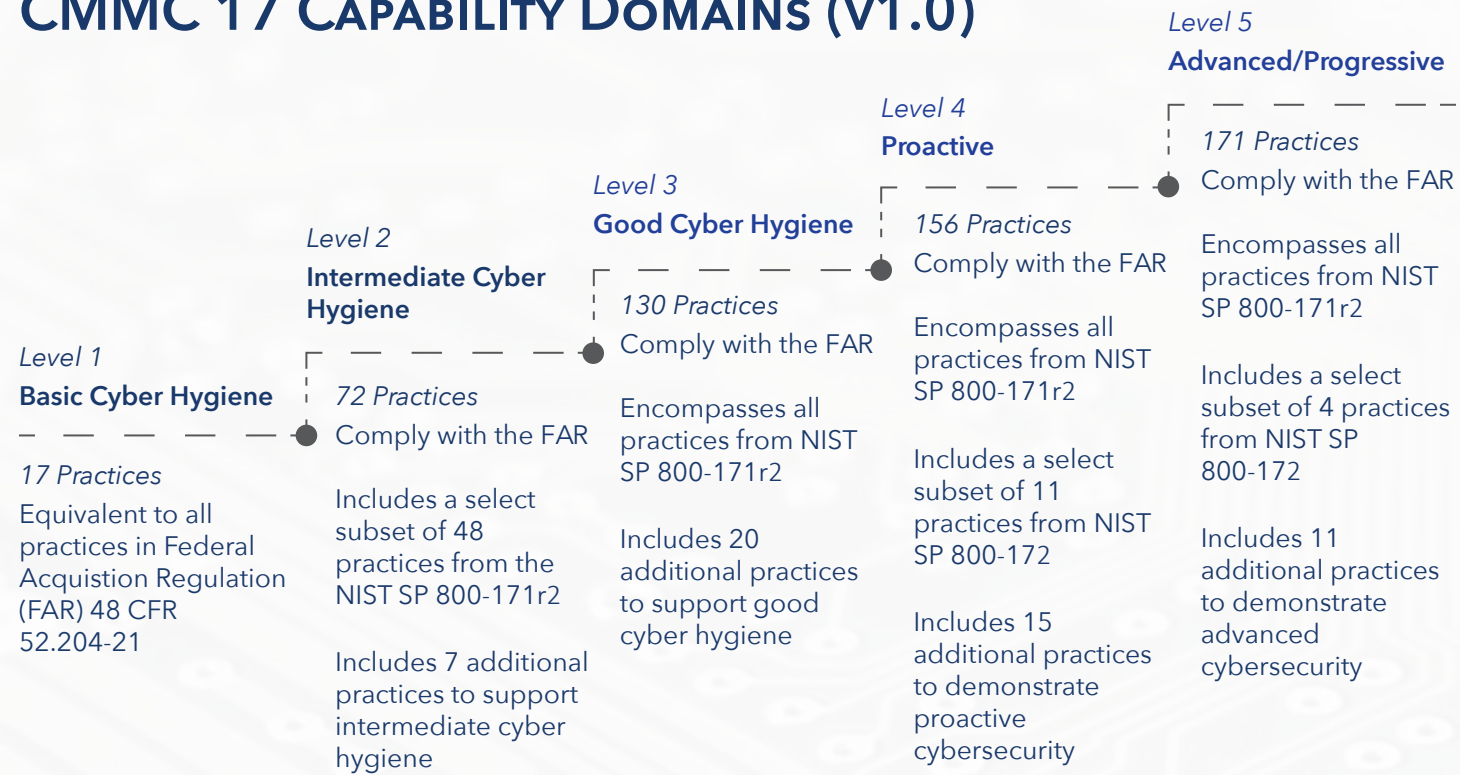
To pass a Level 3 audit, companies will be assessed on their ability to meet and demonstrate all 130 practices to address Levels 1, 2, and 3. This will include technical architecture and solutions, along with written policies.

Organizations that are in the Defense Industrial Base and handle CUI, must comply with at least CMMC Level 3.

CMMC Levels 4 and 5 are for organizations that handle more confidential information, and need a very high level of security. Most companies that need certification will fall into either Level 1 or Level 3.



CMMC 17 CAPABILITY DOMAINS (v1.0)



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.
- Certification requires a third-party auditor.
- Cost of certification may be considered reimbursable as an allowable expense.
- 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 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 SSP and POAM** and **lay out a roadmap and budget** for successful implementation and remediation - all in preparation for your **third-party certification audit**.

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 certification,
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