INTELLIGENT TECHNICAL SOLUTIONS

EVERYTHING YOU NEED TO KNOW ABOUT CMMC [UPDATED]

A Quick Guide to the Updated Cybersecurity Maturity Model Certification

TABLE OF CONTENTS

Introduction

What is CMMC?

Who needs to get CMMC accreditation?

What are the levels of accreditation for CMMC?

What are the four phases of CMMC implementation?

How much does it cost to get CMMC?

How do I get CMMC accreditation?

I. INTRODUCTION

Are you struggling to understand the intricacies of CMMC and how it impacts you?

You're not alone.

The complexities of Cybersecurity Maturity Model Certification (CMMC), in its recently finalized capacity, can be daunting for compliance officers, Department of Defense (DoD) contractors, and anyone involved in the Defense Industrial Base (DIB) ecosystem.

This eBook explores **the essential elements of CMMC, unpacking its framework and highlighting the final requirements you need to follow.**

With Intelligent Technical Solutions' (ITS) expertise in guiding organizations through the maze of CMMC regulatory controls, we'll provide insights and strategies necessary for a smooth transition to compliance.

Expect to discover actionable steps, key considerations, and expert advice to prepare your company for the challenges and opportunities that CMMC brings.

II. WHAT IS CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is the final version of the original CMMC framework developed by the U.S. Department of Defense (DoD). Its goal is to enhance the cybersecurity standards within the Defense Industrial Base (DIB) and its supply chains.

CMMC serves as a method to evaluate an organization's cybersecurity standards periodically. It introduces a unified cybersecurity framework for all entities within the DIB, ensuring a standard of data security and compliance across all DIB primes contractors and their subcontractor supply chain.

This framework is the result of extensive collaboration between government and industry experts. It aims to establish a flexible method for assessing cybersecurity capabilities and bolstering national security.

It is structured around three levels of cybersecurity maturity:

- Level 1: Basic Safeguarding of FCI
- Level 2: Broad Protection of CUI
- Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats

Each level outlines specific criteria that organizations must fulfill to obtain certification. Further discussion about these levels is in *Chapter 4: What are the Levels of CMMC Accreditation?* of this eBook

HISTORY OF CMMC

Although officially introduced in 2019, CMMC's origins can be traced back to the Federal Information Security Management Act of 2002. This act mandated federal agencies in the U.S. to secure their information and systems.

Over time, with contributions from the National Institute of Standards and Technology (NIST), the government standardized cybersecurity guidelines. In 2019, the DoD rolled out CMMC to assess whether government contractors and suppliers were adhering to NIST's Cybersecurity Framework.

RELATED: *What is the Difference Between CMMC and NIST 800-171?*

In response to feedback from its initial implementation, the DoD adjusted the CMMC framework. **These modifications led to the development of CMMC 2.0,** a more streamlined version of the certification process **focusing on efficiency and accessibility** for all stakeholders.

In December 2023, the DoD issued another call for feedback, which ended in February 2024. **CMMC guidelines were finalized on October 15, 2024**, with a mandatory four-phase compliance process to begin on December 14, 2024, for those covered by this policy.

The full breakdown of the compliance process deadlines is explained in *Chapter 5: What are the Four Phases of CMMC Implementation?*

III. WHO NEEDS TO GET CMMC ACCREDITATION?

The DoD **requires all companies in its supply chain to comply with CMMC regulations. Phase 1 implementation is set to begin on December 14, 2024.**

Sean Harris, ITS Senior VP for Cybersecurity, said, “Any organization that wants to do work with the Department of Defense or any vendor that's doing work for the Department of Defense is going to be subject to CMMC. So, at the very least, they’ll be subject to identifying and scoping if their data is subject to it.”

So, if you are:

- A business interacting with the DoD (whether as a contractor or subcontractor),
- Have access to Federal Contract Information (FCI) or Controlled Unclassified Information (CUI),
- Want to work with the DoD in the future,

... then you will need CMMC accreditation.

INTELLIGENT TECHNICAL SOLUTIONS

IV. WHAT ARE THE LEVELS OF ACCREDITATION FOR CMMC?

The final CMMC regulations are only three levels. Each level has its own method of accreditation, security requirements, and access to government contracts.

LEVEL 1
Basic Safeguarding of FCI

The first level is for companies handling only Federal Contract Information (FCI). It requires an annual self-assessment of CMMC controls.

All companies that need this level of certification must follow FAR 52.204-21 and focus on the protection of FCI.

LEVEL 2
Broad Protection of CUI

The second level is for companies working with FCI and Controlled Unclassified Information (CUI). It requires either a tri-annual self-assessment or a tri-annual assessment by a C3PAO (CMMC Third-Party Assessment Organization) for critical national security information. After assessment, contractors will have to reaffirm their compliance annually.

Companies handling CUI must follow the NIST Special Publication (SP) 800-171 (Revision 2) for Protecting CUI. The DoD Assessment Requirements push DoD contractors to follow Revision 2 and currently make no mention of following NIST SP 800-171 Revision 3.

LEVEL 3
Higher-level Protection of CUI Against Advanced Persistent Threats

The third level is for companies working on the highest priority programs and handling both CUI and FCI. The government will conduct tri-annual assessments called the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Annual reaffirmations are another requirement of Level 3 CMMC accreditation.

They must also follow NIST Special Publication (SP) 800-171 (Revision 2) and 24 selected rules from NIST SP 800-172.

WHAT LEVEL OF CMMC DO YOU NEED?

The CMMC level you require entirely depends on the kind of contracts you want and the corresponding data involved.

Here's a table explaining the level of CMMC accreditation you need:

REQUIRED DATA HANDLED (BY CONTRACTOR)	LEVEL OF CMMC ACCREDITATION NEEDED
• Federal Contract Information (FCI)	Level 1 (Self-assessment)
• Federal Contract Information (FCI) AND • Controlled Unclassified Information (CUI)	Level 2 (Self-assessment OR C3PAO assessment)
• Federal Contract Information (FCI) • AND Controlled Unclassified Information (CUI) • AND DoD High-Priority Programs	Level 3 (C3PAO & DIBCAC)

V. WHAT ARE THE FOUR PHASES OF CMMC IMPLEMENTATION?

To ease companies into full CMMC implementation, the DoD has broken down the rollout of CMMC into four different phases:

INTELLIGENT TECHNICAL SOLUTIONS

Phase 1

Phase 1 is set to begin on December 14, 2024. Currently, the DoD requires CMMC Level 1 (Self) or Level 2 (Self) for DoD solicitations and contracts as a condition for contract award.

Additionally, DoD may apply these requirements to option periods on pre-existing contracts and, if needed, substitute Level 2 (C3PAO) in place of Level 2 (Self).

Phase 2

This phase starts one year after Phase 1. DoD will add the requirement for CMMC Level 2 (C3PAO) certification as a condition for contract awards. They may defer this requirement to an option period and optionally add Level 3 (DIBCAC) requirements for certain contracts.

Phase 3

Phase 3 begins one year after Phase 2. The requirements from Phases 1 and 2 continue, with Level 2 (C3PAO) required for all contract awards and option periods on post-effective contracts. CMMC Level 3 (DIBCAC) will be required for applicable contracts as a condition of award, though DoD may defer this to an option period.

Phase 4 (Full Implementation)

This phase commences one year after Phase 3, marking the full integration of CMMC requirements into all relevant DoD solicitations and contracts, including option periods for contracts awarded before Phase 4.

VI. HOW MUCH DOES IT COST TO ACHIEVE CMMC?

Unfortunately, there's no set price for achieving CMMC accreditation.

The cost of CMMC accreditation will vary depending on several factors, such as the **size and complexity of your organization, the level of certification you are seeking, and the C3PAO (CMMC Third-Party Assessor Organization) you work with.**

It's challenging to provide an exact cost without knowing your organization's specific setup and desired goals. **The best way to estimate the costs of getting CMMC is to have an accredited third-party IT provider evaluate your current IT environment.**

This is because the CMMC process generally involves several steps, including:

- A self-assessment,
- An on-site assessment by a C3PAO, and
- Any necessary remediation of any gaps or weaknesses in your cybersecurity practices.

Each of these steps has associated costs, such as fees for the C3PAO's services, the cost of implementing new cybersecurity measures, and any other expenses related to the certification process.

VII. HOW DO I ACHIEVE CMMC ACCREDITATION?

The time required to complete CMMC accreditation depends on the size and complexity of your organization. The process may take a while, but it is a continuous assessment of your compliance efforts rather than a one-time review.

To achieve CMMC accreditation, you'll need to:

1. Get the right people onboard.
2. Assess your current IT setup.
3. Evaluate the payoff for complying with CMMC guidelines.
4. Commit to a plan of action.
5. Coordinate with an accredited C3PAO.

1. Get the right people onboard.

You'll need all hands on deck for CMMC accreditation: your business owners, technology leaders, and department heads. Each person will help hold the organization to CMMC standards.

2. Assess your current IT setup.

Compare your network to the CMMC guidelines with a thorough network assessment. You can self-audit or hire a third party to work with your team.

3. Evaluate the payoff for complying with CMMC guidelines.

After assessing your current IT setup, you can see the gap between where you are and where you need to be for CMMC accreditation. Conduct a quick cost-benefit analysis: getting CMMC certified can be expensive, so is it worth it?

4. Commit to a plan of action.

If you plan to move forward, decide what gaps to fill first, review the specific guidelines for the level of accreditation you desire, and then build a Plan of Action and Milestones (POA&M) with your IT department or third-party IT partner. Your POA&M should explain the gaps in your requirements and the steps you'll take to cover those gaps.

You'll also need to create a System Security Plan (SSP), which details every control and what you have in place to meet it.

Lastly, you'll need to have a Customer Responsibility Matrix (CRM), which specifically details the responsibility for protecting the CUI/FCI in relation to outside vendors and the OSR.

It's a lot of necessary work before the C3PAO arrives to conduct the official assessment.

5. Coordinate with an accredited C3PAO.

After setting up your IT environment to follow CMMC guidelines and creating the necessary documents and plans depending on your target level of accreditation, you must work with a CMMC-accredited C3PAO.

The C3PAO will assess your organization's cybersecurity practices and determine whether you meet the requirements for certification.
If you are compliant, you will be granted CMMC accreditation.

VIII. READY TO START YOUR CMMC JOURNEY?

At the end of the day, CMMC is an essential step toward establishing a cybersecurity program in any organization with DoD partnerships.

To get your company CMMC accredited, you need IT experts to guide you through the process. As a managed security services provider (MSSP) with experience handling clients juggling multiple government regulations, we're offering a way for you to get a head start on the process: a free cybersecurity assessment.

However, if you'd rather continue looking for more information about implementing cybersecurity regulations for your organization, check out our Learning Center.

Meeting the requirements of CMMC requires integrating multiple solutions. Depending on the extent of your security defense infrastructure, CMMC compliance may be a significant undertaking and expense to consider.

KEEP YOUR DOD CONTRACTS. PAINLESSLY.

Schedule a Meeting with us.

INTELLIGENT TECHNICAL SOLUTIONS

3330 W Desert Inn, Suite B,
Las Vegas, NV 89102
Phone: (702) 605-6670
www.itsasap.com