Cybersecurity Maturity Model Certification

(CMMC) for Contractors

White Paper

Wayne Shaw



Wayne Shaw

Five 9s Consulting

[www.five9sconsulting.com](http://www.five9sconsulting.com)

www.five9sconsulting.com/CMMC

Contents

**CEO Introduction**

**Overview……………………………………………………………………………………………..1**

**Chapter 1 – The Information Is Key.…..…………………………………………………2**

**Chapter 2 – MSPs…………………………………………………………………………………3**

**Chapter 3 – COTS…………………………………………………………………………………3**

**Chapter 4 – Suppliers…………………………………………………………………………..4**

**Chapter 5 – Sub-Contractors………………………………………………………………..4**

**Conclusion…………………………………………………………………………………………..5**

CEO’s Introduction





**Owner – Five 9s Consulting**

All contractors who provide products and services to the DoD must obtain at least the Level 1 Maturity of the new CMMC program to verify they can adequately protect information throughout their supply chain. At Five 9s Consulting, we understand that CMMC can be overwhelming. For the last three years, we have focused on CMMC and have extensive expertise and experience to guide you through all CMMC compliance challenges and assistyou in reaching your required CMMC Level of Certification.

It will take time and effort, and you will most likely need to look at your company and IT differently. However, with CMMC certification, your company will be better positioned to receive the contracts you bid on, and you will be ahead of your competitors. In addition, you will not miss the opportunity to grow your company and be on the cutting edge to win RFPs.

Overview

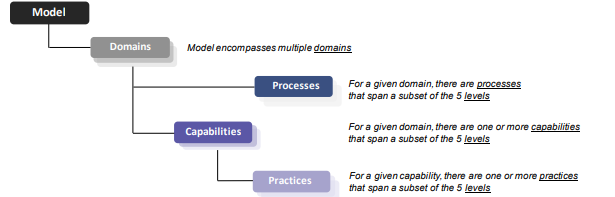
Malicious cyber activity threatens our economic and national security regularly and continues to target the Defense Industrial Base (DIB) sector and the supply chain of the Department of Defense (DoD).

The growing Cybercrime statistics are alarming:

* Every day 30,0000 websites are attacked.
* Nearly 80% of organizations have experienced a cyberattack within the last year.
* At least one-third of consumers were affected by data breaches this past year.
* It costs the global economy more than $10 trillion per year.

The Office of the Under Secretary of Defense for Acquisition and Sustainment recognized that security is foundational. Therefore, to combat these threats and enhance security and protect information within the DIB sector and DoD supply chain, they developed a new regulation: the Cybersecurity Maturity Model Certification (CMMC) model.

The CMMC model measures cybersecurity maturity and aligns processes and practices with the type of information that must be protected from threats. The CMMC requires a certification to verify processes and practices are followed and to increase assurance to the DoD and DIB contractor that they can adequately protect information throughout their supply chain.



Chapter 1 – The Information Is Key

One rule to keep in mind about the CMMC is it all revolves around the information that your company receives from the DoD and that you must protect.

There are three types of information:

1. **Commercial Off The Shelf (COTS)** - No CMMC is required for this type of information.
2. **Federal Contract Information (FCI)** is defined as information provided by or generated for the Government under contract not intended for public release.

To protect FCI, contractors must complete Level 1 CMMC and perform specified practices.

1. **Controlled Unclassified Information (CUI)** - It is sensitive information that the Government requires its handlers to adhere to strict rules to safeguard and keep it safe. There are strict rules concerning its dissemination and handling.

There are some unique requirements that you must meet in the CMMC:

1. If you are using a Managed Service Provider (MSP) with access to the CUI and FCI information from DoD, that MSP might be assessed in line with your scope of work.
2. Any of your suppliers you send CUI or FCI information to must be CMMC certified at the level of information they receive.
3. Any of the sub-contractors you use on DoD jobs must be CMMC certified at the level of CUI or FCI information they receive.
4. All CUI and FCI information must be securely transmitted that contains CUI and FCI.

Chapter 2 – MSPs

If your company uses the services of a Managed Service Provider (MSP), and the MSP has access to the CUI and/or FCI, then the MSP may be included in your company’s assessment scope. Your company is entrusted with protecting the information given to you. If you entrust the information to your MSP, then that MSP could fall under your assessment scope. If the MSP does fall under your scope, then all or part of the MSP’s company is subject to your assessment.

At Five 9s, we recommend you talk to your MSP to verify that they can pass an assessment because your assessment may depend on their adherence to the CMMC controls and their ability to pass a full or partial assessment.

Chapter 3 – COTS

If you are ordering an item that can be purchased at several places, and no modifications or changes are made to that item, then that item is considered as commercial off the shelf (COTS). No CMMC certification should be required for COTS. A good example would be a two-by-four board at your local lumber yard. You can buy them at several places, and they come in many standard lengths.

If the suppliers do not receive any FCI or CUI information about projects within your organization, there is no CMMC requirement. However, if you send a supplier’s blueprints for takeoffs, they have CUI and/or FCI information and require certification.

Chapter 4 – Suppliers

If you send information to a supplier for any reason, takeoffs, estimates, and is downloaded to their system, they will need to be certified. Likewise, if your suppliers get any information marked CUI or even suspect it to be CUI, they will need to be certified at Level Two.

Level Two focuses on cybersecurity practices and standards that protect CUI and mitigate threats throughout an organization. To summarize, Level Two is required of any contractor who handles and stores FCI and CUI or changes commercial off-the-shelf software (COTS). To comply, you must establish, maintain, and resource a plan that demonstrates the management of CMMC implementation activities.

If the information is FCI, then the supplier only needs to be CMMC certified at Level One. Level One requires contractors to follow basic cybersecurity standards and practices.

Chapter 5 –

Sub-Contractors

We want to keep as many of the sub-contractors at Level One as possible. To do this, we need to set up a system that allows you to keep the CUI and FCI information under your control.

By keeping the CUI and FCI information under your control, your sub-contractors are only required to be Level One certified.

This certification is far less complicated, time-consuming, and expensive than Level Three.

At Five 9s, we have developed a program to get your sub-contractors at Level One ready for your upcoming project start dates.

Conclusion

Non-compliant contractors will not qualify to bid on contracts and will not be able to retain DoD contracts unless they complete the required CMMC program. Achieving the necessary CMMC certification for contractors is not difficult. However, CMMC is not a simple call to a consultant to resolve and take care of all your requirements. The CMMC is an evidence-based certification encompassing your entire company. As a contractor, you will need to navigate the compliance challenges. Still, when you do, you will be far ahead of your competitors until they complete their certification if they even decide to get certified.

**Five 9s Consulting offers the following CMMC services:**

* **System Security Plan and Scoring**
* **Project Planning with Milestones**
* **CMMC Company Assessment**
* **Assessment Readiness Review**
* **Awareness and Training**

**Contact us to start your CMMC:**

**Website:** [www.five9sconsulting.com](http://www.five9sconsulting.com/)/cmmc

**e-mail**: [info@five9sconsulting.com](mailto:info@five9sconsulting.com)

**Phone:** 573-219-1948