KAMIND®

Cloud Solutions Advisors

An Introduction to the Cybersecurity Maturity Model Certification (CMMC)

Written By: KAMIND IT Inc.
Published: November 17th, 2020

Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Enterprise Mobility Management

KAMIND®
Cloud Solutions Advisors

Microsoft

Introduction to CMMC

As the United States federal government initiates more Cybersecurity programs and objectives, and even becomes a massive customer of security services and products itself. It is important that we stay on top of the latest events. The need to hire good quality contractors that can do the job is going to become of prime concern, not only for Federal government, but also to set a standard for all contractors that work with the Federal Government.. This is evident by the Department of Defense, as they are making one of the biggest pushes ever to help shore up the lines of defense of the United States both internally and externally. In 2019, the Department of Defense (DOD) created CMMC (Cybersecurity Model Framework certification) and will roll this framework out starting Nov 30, 2020.
This is the focal point of this whitepaper.

What Exactly Is The CMMC?

Background

According to a recent study that was conducted by Juniper Research, the overall amount of financial losses that the United States will experience by the year of 2024 is expected to far exceed $5 trillion (SOURCE: 1). This represents a Year Over Year (YoY) growth rate of nearly 11% until we hit that mark. One of the largest Cyber victims in all of this is what is known as the "Defense Industrial Base," also referred to as the "DIB" for short. The grouping of companies that are involved in this network is extensive.

For example, it represents more than 300,000 businesses across Corporate America, and even any subsidiaries or branch offices that have locations on a global platform. But this number grows even more when you include the nonprofit organizations and academic institutions that are tasked to do the following for our nations' military system:

- Research and engineering
- The development of new system designs
- The acquisition and procurement of the needed raw materials
- The final production and delivery of new products and services.

Introduction To FCI and CUI

The origin of CMMC was created in 2010, under executive order 13556. This established a program to standardize the collection of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI)._If any of the above CUI and FCI information have been compromised in any way, shape, or form, this would, of course, have massive and devastating consequences for the United States on a global level. This is especially true when it comes to the loss of both Intellectual Property (IP), Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The latter can be explicitly defined as follows:

"Federal Contract Information (FCI) is “Information not intended for public release. It is provided by or generated by the Government under a contract to develop or deliver a product or service to the Government. FCI does not include information provided by the Government to the public.

"Controlled Unclassified Information (CUI) is government-created, contractor-created (under a federal contract), or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies.

CUI is not classified information. It is information that was created by the federal government or created by a contractor for or included in requirements related to a government contract." (SOURCE: 2).

In other words, FCI and CUI is information that can be accessed to varying degrees by external third parties. However, it is not designed to be released to the public at large, because of some of the sensitivity that is involved with the datasets. As a result, there are fewer controls that are associated with FCI and CUI. Because of that, this presents a prime opportunity for the Cyberattacker to penetrate the system and gain access to the classified information covertly.

An Overview to The CMMC

To provide specific safeguards and controls to help further protect the FCI and CUI, the "Cybersecurity Maturity Model Certification," or the "CMMC" has been established.

This framework was launched by the Office of the Under Secretary of Defense for Acquisition and Sustainment, also explicitly known as the "OUSD (AS)" for short. Although one of the primary objectives of the CMMC is to protect FCI and CUI, one of the other main themes of it is to limit access to the external contractors that can gain access to it. Although these parties primarily reside in the United States, they could very well also have connections to associates in overseas offices, where both FCI and CUI could be released intentionally or non-intentionally to potential, malicious third parties.

These contractors form what is known as the "Defense Supply Chain (DSC)" for the Department of Defense (DoD). Along with the other entities described earlier in this whitepaper, this category also includes many small to medium-sized businesses. These organizations are the most prone to Cyberattacks, and according to the Verizon 2019 Data Breach Investigations Report, it is those entities that have up to 250 contractors (or more) that are at most risk for exposing FCI and CUI via Email, or any other electronic means. (SOURCE: 3).

One of the driving forces behind the CMMC is the list of best practices and standards that have been set forth by the National Institute of Standards and Technology, also known as "NIST." Before the adoption of the NIST framework, the guiding principles for implementing some controls for the FCI and CUI came from the "NIST SP 800-171", and the "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

In order to prove their level of trustworthiness when it comes to accessing FCI and CUI, these external contractors in the DSC (Defense Supply Chain) will have to be certified through the CMMC framework primarily through CMMC based Third Party Organizations also known as "C3PAOs" for short. This gets complicated because the third-party organization that performs the certification assessment cannot be the same organization that does the CMMC implementation. Certification is a requirement before any contract can be awarded (prior t0 2025), and after 2025, certification will be a requirement before any bidding on DoD contracts can take place. Accreditation must be awarded by the CMMC_AB (the not-for-profit CMMC Accreditation board). The CMMC accreditation level is stipulated in the I government Request For Proposals (RFPs).

It is crucial to keep in mind that merely achieving CMMC certification does not guarantee that the third-party contractors will gain immediate and automatic access to the CUI datasets. Instead, the DoD will have final oversight as to the types of CUI that will be disseminated. The first version of the CMMC (Version 1.0) was released in 2020. DOD will stipulate at least 15 contracts that require CMMC accreditation, after Nov 30, 2020. The Goal of the DOD is to have the DSC (Defenses Supply Chain), fully accredited by October 30, 2025.

The Structure Of The CMMC Model

CMMC is composed of 17 Technology domains and 5 processes and is designed based on 5 levels. The CMMC has 17 specific domains, which are referred to as CMMC practices, and are as follows:

- Access Control (AC).
- Asset Management (AM).
- Audit and Accountability (AU).
- Awareness and Training (AT).
- Configuration Management (CM).
- Identification and Authentication (IA).
- Incident Response (IR).
- Maintenance (MA).
- Media Protection (MP).
- Personnel Security (PS).
- Physical Protection (PE).
- Recovery (RE).
- Risk Management (RM).
- Security Assessment (CA).
- Situational Awareness (SA).
- System and Communication Protection (SC).
- System and Information Integrity (SI).

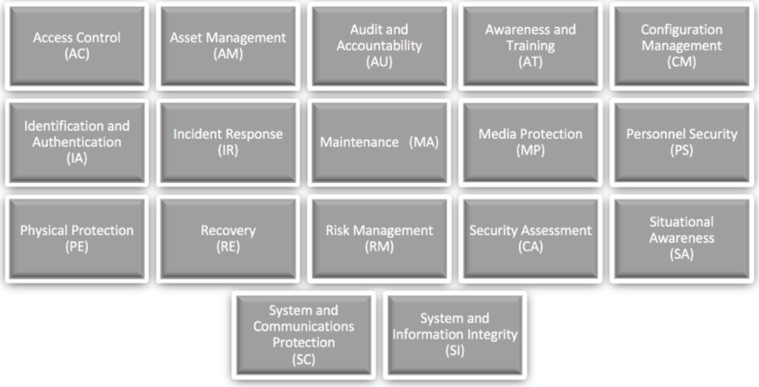

Access Control (AC)
Asset Management (AM)
Audit and Accountability (AU)
Awareness and Training (AT)
Configuration Management (CM)
Identification and Authentication (IA)
Incident Response (IR)
Maintenance (MA)
Media Protection (MP)
Personnel Security (PS)
Physical Protection (PE)
Recovery (RE)
Risk Management (RM)
Security Assessment (CA)
Situational Awareness (SA)
System and Communications Protection (SC)
System and Information Integrity (SI)

Figure 1. CMMC Domains.

Each of these practices' domains have five maturity levels of certification (designated as ML1, ML2, ML3, ML4, ML5). Each Practice domain has additional process models that define how the cyber maturity levels are implemented in the organization. Before any external third-party contractor can gain access to any FCI or CUI, they must have achieved at least the appropriate level of certification. As an example, CUI information requires a L3 level of certification. These domains have had their originations from the following sets of publications:

- ➢ The Federal Information Processing Standards (FIPS) Publication 200.
- ➢ The NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Also, these 17 domains have a grand total of over 171 technical areas.

<u>The Maturity Levels Of Certification</u>

The five distinct Maturity Levels are designated as ML1, ML2, ML3, ML4, and ML5. Maturity levels are used because DoD expects the organization to achieve the maturity level processes and practices a good year before they bid on the federal contract. As an example, if an organization wishes to achieve certification, the assessor will expect the Maturity level implementation a good year before the assessment is performed. This means that if the DoD timetable is October 30, 2025, the DIB will need to implement the ML process and practices by October 30, 2024. Furthermore, any business that does any bidding or work for the DoD, the company that employs the outside contractors must achieve the required Maturity Level as well as the ones that are below that. For example, if the business is required to be at ML3 for a specific contract, they must also show a deep level of expertise at ML1 and ML2, with object evidence and processes fully documented and implemented.

More detail on these Maturity Levels is as follows:

1) **<u>Maturity Level 1</u>:**
   This signifies the basic "Cyber Hygiene" and represents only those minimal controls that are needed for the protection of the FCI, as it is stipulated in the document "Basic Safeguarding of Covered Contractor Information Systems," also known as the "48 CFR 52.204-21". At this level, the business must implement and enforce these minimal controls but has no process requirements. This is called Ad Hoc processes. There are 17 practices required for ML1

2) **<u>Maturity Level 2</u>:**
   This level is the stepping-stone for achieving a baseline of cybersecurity for the CUI, as it is stipulated in NIST SP 800-171. At this point, the business is required to document how they will establish the need for a particular domain, as illustrated previously. ML2 requires 72 practices, and 1 process implementation.

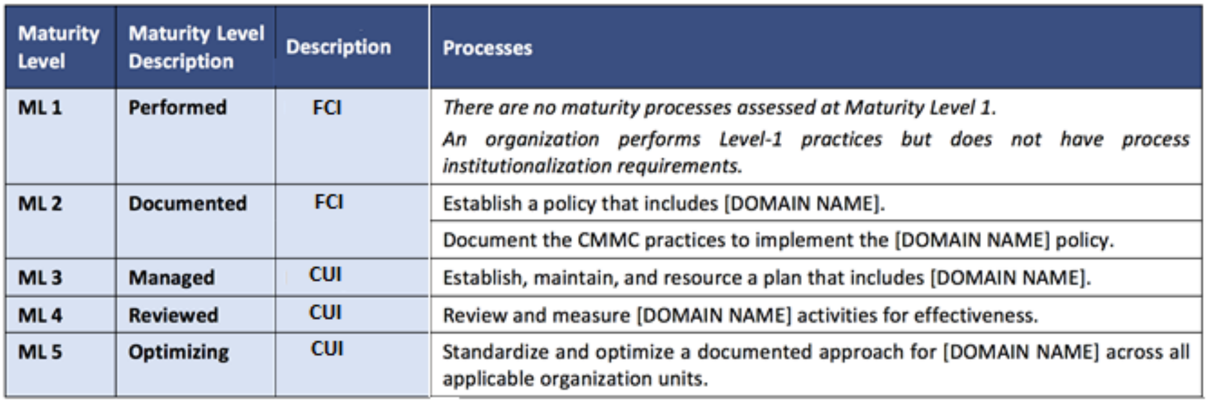
3) **<u>Maturity Level 3</u>:**
   This level emphasizes the full protection of the CUI, as also spelled out in NIST SP 800-171. At this stage, the business is required to create, deploy, and maintain a specific plan of action for managing their activities in a particular domain. ML2 brings in the concept of training, not only for the end user, but also for the security personnel. As this evolves, Cyber Ranges will become more common to train the security team. ML3 requires 130 practices and 3 process implementations.

4) **Maturity Level 4:**
This level embraces the full, proactive mindset and techniques that are needed to protect the CUI from the standpoint of cybersecurity. It is designed to focus upon the two types of actor vector categories:
   - Tactics, Techniques, and Procedures (also known as "TTPs").
   - Advanced Persistent Threats (also known as "ATPs").

   At this point, the business is required to establish key metrics to gauge the effectiveness of the cybersecurity controls that have been deployed, including the training of the Cyber Security personnel. This training is expected to include a Cyber Range model to meet the simulation environment. ML4 requires 156 practices and 4 process implementations.

5) **Maturity Level 5:**
This level is devoted to the full protection of the CUI from the ATPs. At this stage, the business is required to further streamline, as well as optimize, the Cybersecurity controls that have been implemented. ML4 requires 171 practices and 5 process implementations.

All of this can be seen in the illustration below:



Maturity Level	Maturity Level Description	Description	Processes
ML 1	Performed	FCI	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level-1 practices but does not have process institutionalization requirements.*
ML 2	Documented	FCI	Establish a policy that includes [DOMAIN NAME]. Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	Managed	CUI	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	Reviewed	CUI	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	Optimizing	CUI	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Figure 2. CMMC Processes.

(SOURCE: 4).

How Does The CMMC Compare to NIST 800-171?

As mentioned previously, it is the NIST 800-171 that serves as one of the major backbones for the CMMC. However, there are key differences between the two, and they are as follows:

1) **CMMC requires certification to be conducted by third-party assessors:**

   Previously under NIST, the third-party defense contractors could self-certify. Meaning, they could state that they are currently compliant or have full intentions to do it, and no further documentation was required. But with the CMMC, this is no longer the case. They now have to be fully certified by an outside agency that is qualified to gauge if they are truly in compliance with the mandates that have been set forth by the DoD. These agencies are known as "Assessors." However, it is essential to keep in mind that even Assessors themselves must be fully certified as well. This is done by the CMMC Accreditation Body, which is a nonprofit organization that was set up in January 2020. Their goal is to train and certify up to 10,000 Assessors by the end of 2020. Also, they will need to undergo and pass a comprehensive background check as well.

2) **Full compliance is needed to start bidding after October 30, 2025:**
Before any third-party defense contractor can even submit documents for Requests For Information (RFIs) and Requests For Proposals (RFPs), they must be fully certified by the requirements that are set forth for every DoD project that requires these two documents. Prior to Nov 1, 2025, the defense contractor must have already achieved the ML specified in the contract when it is awarded.

3) **Other entities may have to be certified as well:**
If any contract is awarded to the third-party defense contractor, and if they have to outsource some of that work to other subcontractors, then these subcontractors also have to be CMMC certified.

4) **Smaller sized contractors will have lesser requirements:**
One of the primary intentions of the DoD is to help smaller contractors to further beef up their cybersecurity Maturity Levels (MLs) that are based upon the NIST 800-171 requirements. For example, these smaller sized contractors will only have to reach up to Maturity Level 1. Those third-party defense contractors that are only at ML1 will be required to come into compliance with 17 of the 171 total controls that are specified in the CMMC if they have FCI (Federal Contract information). **Larger sized contractors will have more requirements to be met:**

Those third-party defense contractors that are up to ML5 in the CMMC framework will need to also come into full compliance with the NIST 800-171 requirements. But for those entities that are up to ML4 and ML5 will have further requirements that they will have to meet, and they are outlined in the following:

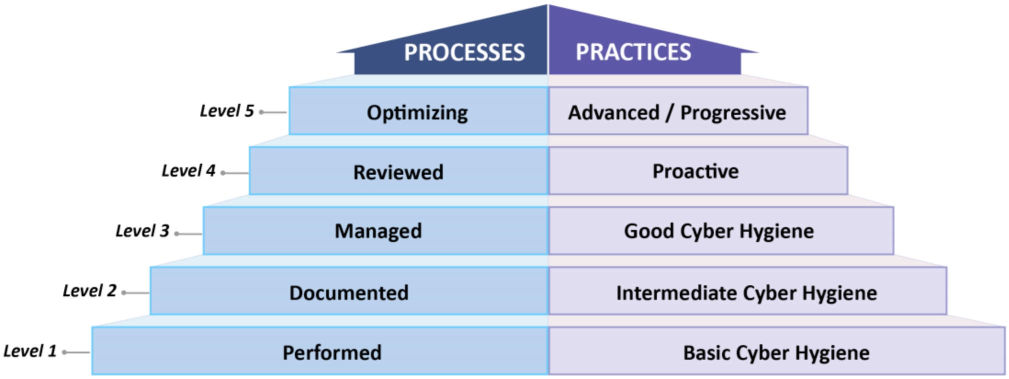
- The FAR Clause 52.204-21.
- The NIST 800-172.
- The CERT Resilience Management Model (also known as the "CERT-RMM");
- The NIST Cybersecurity Framework (also known as the "CSF").

5) **More domains will be added:**

At present, the NIST 800-172 has only 14 domains. But with the advent of the CMMC, this now comes to up a total of 17 new domains. The new domains are as follows:

- Asset Management.
- Recovery.
- Situational Awareness.

6) **More Maturity Processes are added:**
The NIST 800-172 is focused primarily upon the implementations of controls. But with the CMMC, the emphasis is not only on this but also on practice and process requirements. This is illustrated below:



CMMC Levels, Processes and Practices

(SOURCE: 5).

7) **Cybersecurity is embraced:**
While the NIST 800-172 focuses upon the traditional mechanisms of the following:
   - Access control.
   - Audits.
   - Configuration management.
   - Portable media devices.
   - Personnel Security.

   The CMMC also includes a special emphasis on cybersecurity. These can be broken down as follows:

   - Levels 2 and 3 focus upon Cyber Threat Intelligence.
   - Levels 4 and 5 focus upon the advanced topologies of Cyber Threat Intelligence, which are:
     *Incidents of Compromise (IOC).
     *Threat Hunting.
     *Sharing the specific sources of Cyber Threat Intelligence.

The Timeline For The CMMC

It is important to note that the CMMC is still a work in process, so the complete timetable for implementing it and getting certified is still somewhat tentative. But here are some key dates to keep in mind, generally speaking:

1) **The attainment of New Contracts and their Renewals:**
Any new projects to be awarded by the DoD under the CMMC framework will be on an ongoing basis until at least Oct 31, 2025, if not longer. Thus, the DoD will specify the CMMC requirements for any new contracts, their renewals, and the RFIs and the RFPs that come out in this time period.

   Once we reach Nov 31, 2025, contractors will need to have their accreditation in place.

2) **The training of Auditors**:
It is the specific duty of the CMMC Auditor to make sure that the third-party defense contractors continue to meet the stringent compliance requirements after they have been certified. Training has already started, and 70 auditors are being trained as provisional assessors to access the first 15 contracts and the 1500 subcontractors in 2021. Keep in mind, if you hire an assessor (form a C3PAO), they cannot offer you advice on how you should do the implementation. Therefore, the CMMC-AB created a second group of Assessor organizations, known as an RPO (Registered Practitioner Organization). An RPO (such as KAMIND IT) can implement CMMC for an organization (that is, help develop processes and SOPs, and help collect the Object Evidence for the assessment), and work with the C3PAO assessor and guide you through an assessment process.

   The RPO, C3PAOs are listed in the CMMC-AB marketplace at www.cmmcab.org

3) **The Requests For Information (RFIs) and Requests For Proposals (RFPs)**:
According to Under Secretary of Defense for Acquisition and Sustainment, Ellen Lord, the DoD will start to issue new 15 RFIs with the new CMMC requirements starting in November 2020, and thereafter monthly. Any new contracts awarded after this timeframe will require the third-party defense contractors to produce their CMMC certification upon demand. There is a total of 15 contracts that DoD has identified that will have CMMC requirements in them for 2021.

4) **Certification and Post Certification steps**:
It is highly recommended that the third-party defense contractors start the process of certification and achieving it ***right now***. CMMC is a maturity level model, which requires a culture and process change in the defense contractor on handling not only CUI, but the FCI information. After you have achieved the level of certification that you are required to get, it will then last for a period of three years. During the period of certification, you are required to maintain the cyber security deployments and processes. At the end of the 3-year period, you will need to recertify with the then current CMMC Model. The best approach is to work with an RPO on a certification and deployment methodology that incorporate changes as they occur. CMMC is a living practice that addresses the fact that security is a process, not a point in time.

   Keep in mind, if you are required to achieve a higher level of Maturity Level certification (than what is awarded), you will have to go through yet another audit, but which is only applicable to that higher level that you need to achieve to bid for a DoD contract. As of 2020, the highest level of CMMC certification one can obtain is at Maturity Level 3.

What Are The Ramifications For Being Noncompliant?

The DOD will issue the new guidelines on Nov 30, 2020. At this time, the new federal contracts now come under the Fair-Claims Act. This means that if an organization falsifies information to the assessor, or an organization decides not to follow through with the practices or processes after the assessment, then the DOJ can enforce legal proceeding on this. The Fair Claims Act also includes a finder's fee of 15 – 30% of the sanctions against the company for the reporting individual who turns in the violation to the DOJ. The fair claims act also includes criminal enforcement if warranted.

If an organization is certified, and the organization has been impacted by a Cyberattack or other type of security breach, they may not necessarily lose their CMMC certification. However, they will have to go through another audit to determine exactly what happened and what steps are being taken to remedy the situation and come back into compliance with the CMMC.

Conclusions

Overall, this whitepaper has provided an overview of what the CMMC is all about, and some important deadlines you will need to keep in mind. Remember, it is still a work in process, and so the process of getting certified to whatever Maturity Level you need to be at can be quite a daunting process. It's always best to work with an RPO that has assessors on staff and can work with you on the CMMC processes and practices. In this regard, KAMIND IT is an RPO and can help you. Contact us today to see how we can help you to achieve your CMMC certification.

More answers to questions can also be found at this link.

Sources

1) https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches
2) https://www.dcsa.mil/mc/ctp/cui/
3) https://enterprise.verizon.com/en-gb/resources/reports/dbir/
4) https://insights.sei.cmu.edu/sei_blog/2020/03/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc.html
5) https://aws.amazon.com/blogs/publicsector/how-plan-cybersecurity-maturity-model-certification-cmmc/
6) https://csrc.nist.gov/publications/detail/fips/200/final
7) https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
8) https://breakingdefense.com/2020/02/cmmc-1-0-vs-nist-800-171-eight-essential-differences/
9) https://www.cmmcaudit.org/how-to-become-a-cmmc-auditor-or-certifier/
10) https://www.mossadams.com/articles/2020/03/cmmc-timeline