KAMIND®
Cloud Solutions Advisors

The CMMC Enclave

A Publication by KAMIND IT

March 2025

The CMMC Enclave

In many of our blogs and white papers, we have examined in detail what the Cybersecurity Maturity Model Certification, or the CMMC is all about. On December 16, 2024 the CMMC ruling became law with the publication of 32 CFR (Code of Federal Register) part 170. Essentially, this is where all of the contractors and the subcontractors in the Defense Industrial Base (also known as the "DIB") need to come into compliance with 32 CFR to transact against any federal contract issued by the Department of Defense (DoD).

There are many different approaches to CMMC by an OSC (Organization Seeking Certification). The most common approach for an OSC that has both a commercial business and a government business is to build an enclave for Government Business. When a Defenses contractor files a SPRS (Supplier Performance Risk Score), they have two options, either an Enterprise (the entire Company) or an enclave (a smaller portion of the company). The advantage of an enclave is that you can reduce the scope of the Assessment to a smaller area, reducing cost and complexity. This is called the "CMMC Enclave" and will be further reviewed in this whitepaper.

What It Is An Enclave?

The first question that you are probably asking at this point is what exactly an enclave is. Well, as it relates to Cybersecurity and the needs of the DoD, it can be technically defined as the following:

"An enclave refers to a separate, secure area within a system or network that is used to process, store, or transmit Controlled Unclassified Information (CUI). This concept is often used to ensure that sensitive information is isolated and protected from unauthorized access or potential threats".

(SOURCE: 1).

In other words, for example, if you are using a Cloud based platform to conduct your work for the DoD, the Secure Enclave will let you carve out a very secure area of it and isolate it from the rest of the shared environment. One of the biggest advantages of taking this kind of approach is that your business is afforded some of the highest levels of protection that are possible, as it was alluded to in the above definition. OSCs like this approach because this has the potential to reduce the overall cost of a formal assessment.

As it relates to the CMMC, the Secure Enclave is primarily meant for the further protection of both the CUI and FCI datasets that your organization will be using, as supplied by the DoD. Although each Maturity Level specifies what controls are needed to safeguard these datasets, having a Secure Enclave in the Cloud, especially using the Microsoft Azure platform, will give you more ammunition to show to the DoD of your intentions of being compliant.

This point is further fortified by these following quotes, both from the DoD and NIST. First, is the quote from the former:

"When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s) depending upon where the information to be protected is handled and stored."

(SOURCE: 2).

Second, is the quote from the latter:

"Isolating CUI into its own security domain by applying architectural design concepts may be the most cost-effective and efficient approach for non-federal organizations to satisfy the security requirements and protect the confidentiality of CUI."

(SOURCE: 2).

So, even the DoD fully supports the use of some sort of Secure Enclave, and by doing so, you could quite possibly achieve compliance from Maturity Levels 1 – 3 in a very quick time period.

But before we go any further, it would be useful to provide a brief review of what CUI and FCI datasets actually are.

What FCI and CUI Are

The FCI

FCI stands for "Federal Contract Information". A technical definition of it is as follows:

"It is information not intended for public release. It is provided by or generated for 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."

(SOURCE: 3).

By the very nature of its name, the FCI has a much narrower scope than the CUI datasets (as just reviewed). In other words, these are the proprietary datasets that have been created and developed when the defense contractor and their third parties actually provide a tangible good to the Federal Government, under the terms of the contract that were awarded.

Examples of FCI datasets include the following:

- Any emails that are transmitted from the DoD to the defense contractor (and vice versa);
- Any other subcontracts and policies that are needed by the defense contractor;
- Any information that has been garnered as a result of instant messaging, video conferencing, etc.

The Levels At Which FCI Is Implemented

It should be noted that with regards to FCI, it impacts only the first two Maturity Levels which are as follows:

1) Level One:

   This is deemed to be the initial phase, where there is no formal structure yet in place in order to accomplish the work processes that are needed in order to deliver the goods or services to the Federal Government. Rather, the approach is Ad Hoc until it is all formalized. These typically can include the first round of meetings, information/data gathering, preliminary analysis requirements, etc.

2) Level Two:

   At this level, the respective workflows and processes needed to fulfill the terms of the DoD contract become more defined. In other words, the ability to track in more detail what is happening can now take place. This also involves the following activities:

   - The tracking of various costing schedules;
   - Workflow scheduling;
   - Defining the functionalities of the established workflows (in other words, defining in further detail the output that is expected, with an emphasis on the FCI related datasets that are to be created when developing the good or service to the Federal Government).

CUI

CUI stands for Controlled Unclassified Information. Simply put, these are the datasets that are owned by the Federal Government in which the defense contractor (and their affiliates) must have the minimum level of controls put into place in order to safeguard them.

This can be initially misleading, because of the term “Unclassified”. This means that these datasets can be shared with other entities that are CMMC Level 2 or Higher certified as determined by the contract, but they cannot be released to the public and need to be protected. The rules are simple, what processes, stores or transmits CUI must be secured under the NIST 800-171 specification.

Very often, the CUI is needed by the defense contractor in order to submit a comprehensive Request For Proposal (RFP) to the DoD, and to initiate the work that needs to be done.

Typical examples of CUI datasets include the following:

- Intellectual Property;
- Technical drawings;
- Blueprints;

- Other forms of related documentation, such as those for export control, Cyber vulnerability information, and other sorts of financial data.

Assets & Security Protection Assets

The next important component of the Secure Enclave are the Security Protection Assets. In the world of Cybersecurity, assets are often referred to as the "Digital Assets". These include other pieces of information and data, which are used in the normal, everyday usage of business transactions. Security Protection Assets are those assets that provide cyber security controls to manage the transmitting, processing or storage of CUI data.

The DoD would also like to see that your organization is taking proactive steps to safeguard the PII as well, by making use of the appropriate set controls and making sure that they are updated and patched on a regular cycle. In other words, it is not just enough to protect the FCI and CUI datasets. There is an inherent understanding that everything will be protected to the best of your ability, and that any remediations which are needed will be implemented quickly.

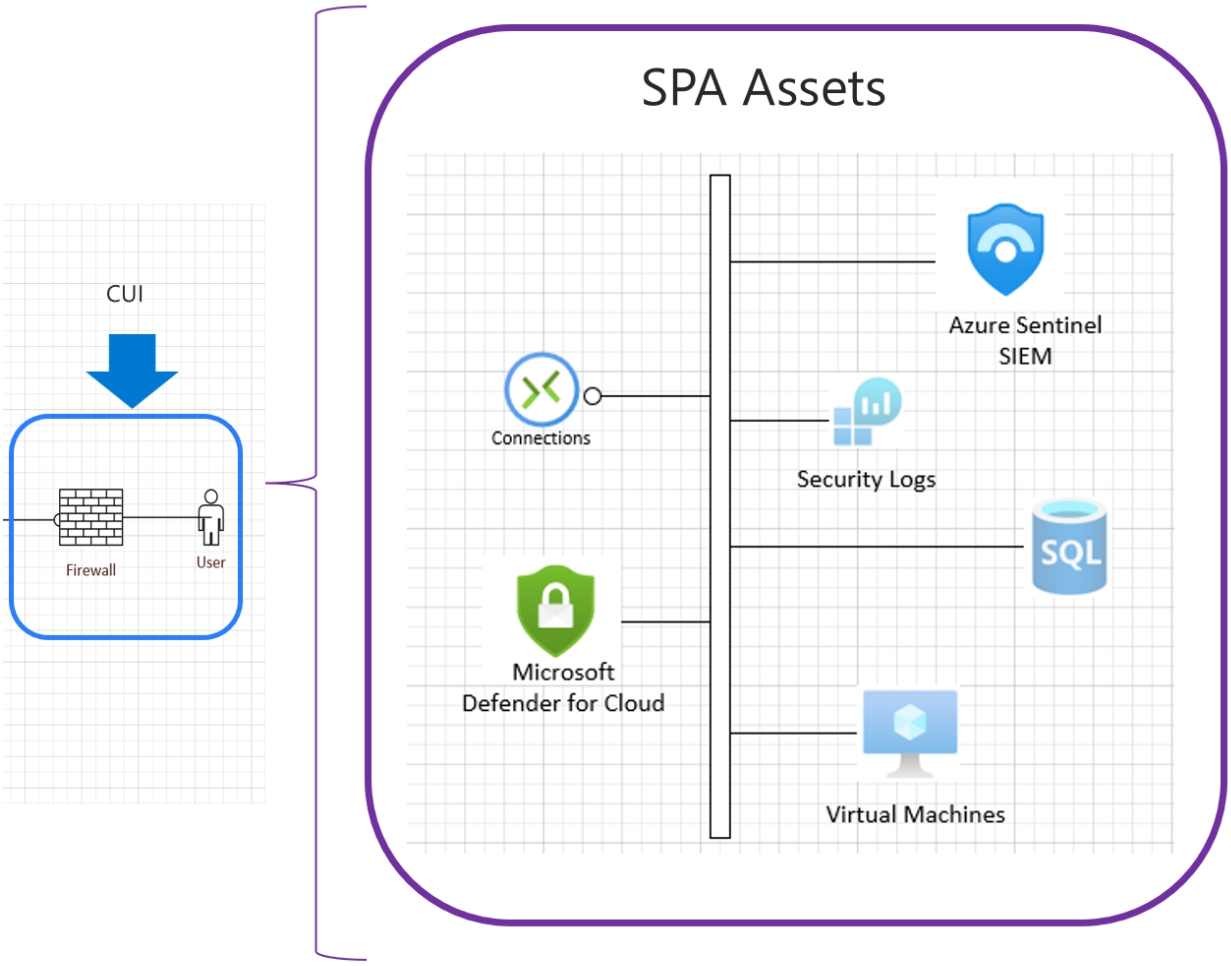
We can now extend this definition of Digital Assets and apply to what are known as "Security Protection Assets.", also known as "SPAs". According to the DoD, SPAs can be specifically defined as follows:

"These are the assets that perform a CMMC-required security function and are described in the system security plan in this regard."

In other words, any asset that is used from within your organization to protect any other asset that is deemed to be "in scope" (provide some level of functionality) with any of the other Maturity Levels of the CMMC is an SPA. A recent change in the December 16, 2024 law has defined the output of SPA as SPD (Security Protection Data).

(SOURCE: 4).

An example of an SPA is as follows:

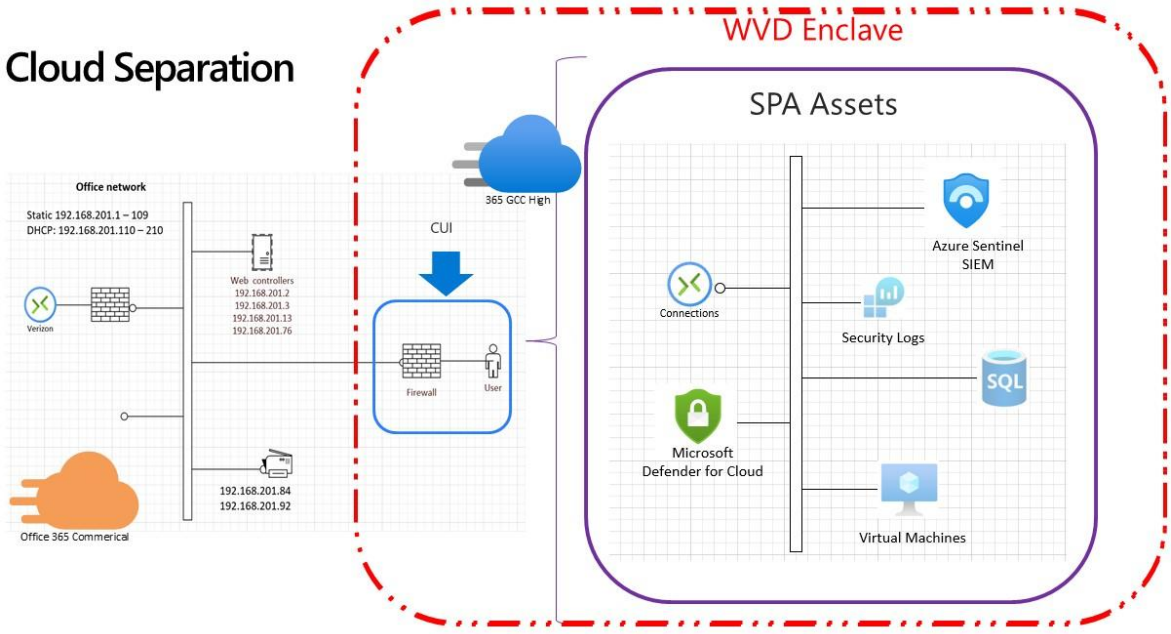


From this diagram, it is assumed that you are using Microsoft Azure for your CMMC deployments. It is evident that the Microsoft Defender for Cloud - at least on a theoretical basis - is providing a primary line of defense for the SPAs, which includes the following:

- Azure Sentinel SIEM;
- The Security Logs;
- The SQL database;
- The Virtual Machines.

What The Secure Enclave Consists Of

When it comes to using Microsoft Azure, the Secure Enclave is typically housed in what is known as an "Azure Virtual Desktop", also known as a "AVD" for short. It has now become easier to deploy Microsoft Cloud PC in Azure, instead of (or in in addition to) AVD. It consists of everything from the last figure, and also what is known as the "GCC High." This is illustrated in the diagram below also:



KAMIND IT Company Confidential

At this point, it is important to provide a review of what the AVD and GCC High are all about.

<u>What Exactly are Cloud PCs or Azure Virtual Desktop (AVD)?</u>

Cloud PCs and AVD are considered to be a set of tools, or technologies which are available in Microsoft Azure. They allow the IT department to almost instantaneously create a brand-new desktop computer which makes use of the Windows 11 OS. AVDs are built directly from Azure while Cloud PCs are purchased as a fixed price subscription product.

But instead of being physically deployed at your office, you can now access it with a few clicks of the mouse in just a matter of a few seconds.

But the nice thing about this is since it is all based in the Cloud, you do not have to worry about any licensing issues yourself directly or even deploying any software upgrades and patches. It is all handled for you by Azure.

This breakthrough was actually launched in 2019, but has not gained serious traction until now. It stems from the Remote Desktop Protocol (RDP), in which an end user could access a remote computer virtually and have a direct interface with the desktop.

Microsoft has introduced Cloud PCs, which are Windows 11 Pro devices managed like physical PCs. These virtual Cloud PCs can be effectively managed with Microsoft Intune and other Microsoft SPA services.

With the release of the CMMC law (32 CFR Part 170), the DOD has defined VDI (Virtual Device Interface). This describes what is in scope and out of scope for a CMMC assessment. You can deploy a cloud PC and

manage it via Intune where only the video, keyboard, and mouse are used. This is important because the host of the cloud PC (e.g., a laptop) would be considered an out-of-scope asset.

Here are some of the key benefits of using the Windows Virtual Desktop:

- It is much easier for all of your employees (if not most of them) to access a single instance of it. In other words, each individual does not need to have their own desktop. From one single Virtual Machine (aka VM), you can create one desktop, and from there, the employees can access it, depending upon the rights, privileges, and permissions that have been assigned to them.
- For security purposes, all of the user profiles that have been created are actually stored separately from the Windows Virtual Desktop environment, in separate Cloud Storage Containers.
- It offers a more secure way for employees to access the data. This was traditionally done by making use of the RDP, but with Azure, a separate Platform as a Service (aka PaaS) is offered so that it can automatically manage the login sessions on to the AVD.
- It supports the usage of all employees, not just a select few. For example, these are the kinds of workers that would make the most use of the AVD:

  *The Kiosk Workers: If you want your customers to access certain parts of your website that are designed specifically for them, such as a client login portal, you can now migrate this to the AVD environment, in a safe and secure manner. This transition actually decreases the security risks that are posed to your Web based application.

  *The Administrative Workers: These employees are typically the executive administrative assistants, secretaries, and other essential support personnel that are required to keep your business running seamlessly on a daily basis.

  *The Knowledge Workers: These are those kinds of employees that are always on the go, and need constant, remote access to company resources. Typically, this group includes the outdoor account managers, members of the C-Suite, etc.

  *The Power Users: This is the classification that is most often given to those employees that use computing processing powers to its maximum availability. These are the software developers that are creating new applications for your company to offer to customers and prospects, and even graphic designers that make use of video production in order to advertise/showcase your products and services. In the past, these employees would very often require having their own dedicated servers and workstations in order to serve these high intense CPU and memory needs. But, this can now all be offered through the AVD.

The GCC High

The DoD requires a special type of Cloud environment in order to secure its most sensitive dataset. This comes down to what needs to be protected based on CUI. Anything that stores, processes or transmits

CUI needs to be protected. In order to satisfy this need, Microsoft devised a new kind of Cloud Platform called the "Government Community Cloud", or the "GCC and GCCH" for short, in order to meet its compliance standards.

There are two versions of GCC, one in the commercial cloud and the other in the Sovereign data center, called Azure Government. The main differences between the two are the support structure and FedRAMP compliance. GCC operates in the public cloud and is supported globally by Microsoft. In contrast, GCCH resides in the Government Cloud and is considered a sovereign data center.

Apart from the CMMC, this is also available to those entities that are involved with the following:

- FedRAMP High;
- DFARS 7012;
- The International Traffic in Arms Regulations (ITAR);
- The Criminal Justice Information Services Policies.

What Are The Differences Of GCC High With The Commercial M365 (aka GCC)?

It differs in four key areas, which are as follows:

1) Storage:

   Microsoft Azure has datacenters located throughout the world, and the end user typically has a choice as to which one of them they would like to deploy their Cloud environment in. But with the GCC High, this is not the case. All data that is stored, processed, and archived are stored in US based datacenters only. Further, access to this is severely restricted, as individuals must be employees of Microsoft, and have to also be thoroughly screened and background checked. Also, access to the DoD datasets is only allowed on a request only basis.

2) Access to M365 applications:

   When a business establishes their Azure account along with M365, all applications from within them are available instantaneously. This is not the case with GCC High. Applications are much slower to roll out, given all of the security checks that must be conducted first.

3) Licensing:

   While the licensing for the commercial versions of M365 and Azure can be purchased from just about any Cloud Services Provider (CSP), licensing for the GCC High Cloud can only be purchased from a limited number of Microsoft AOSG Partners, such as KAMIND.

4) The sharing of information:

   The data that is stored and processed in the GCC High Cloud cannot be shared at all with other commercial Cloud Platforms that use Azure. It can only be shared from within other GCCH environments.

The Disadvantages Of The GCCH

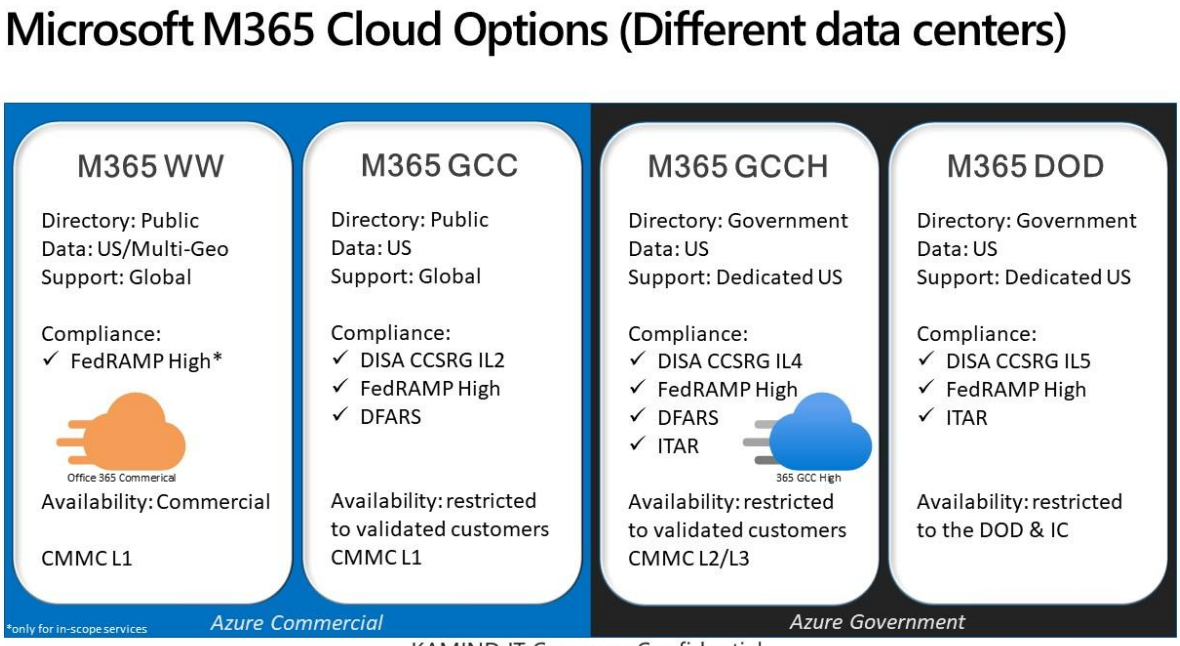
While the primary advantage of the GCCH is that it offers a very secure and robust environment for the DoD datasets, because of that it also has a number of limitations as well:

- The ability to share and collaborate outside the sovereign data centers is significantly restricted. Microsoft has also implemented additional controls to limit the IP address ranges that can access the sovereign data centers, as well as to restrict data transfers outside of the Sovereign Cloud.

- The Sovereign Cloud is a separate data center, located and operated differently from the commercial cloud. It has additional security requirements to ensure the hosted data's safety.

- Given the tightness of the environment, many other features of it are still quite limited, and there is virtually no interaction allowed with 3rd party applications.
- It can be more expensive than a commercial data center

It is important to note at this point there are different versions of M365 that you could possibly use for your company, and these can be seen in the diagram below:



KAMIND IT Company Confidential

Typically, you will need an M365 G5 or a (MS365 G3 + G5 security) for your Security Enclave these licenses are typically required at Maturity Level 2 or higher, if GCC High is going to be deployed into it.

Conclusions

Overall, some of the strategic benefits of using a Secure Enclave are as follows:

- The costs of CMMC Compliance are lower, as well as maintaining your certification for the long term;
- It can help with the reduction of any training requirements that are needed for others that will have access to your Secure Enclave;
- It will support the concept of Least Privilege (this is where you are giving only the authorized personnel access to the Secure Enclave to do only what they need to do, and nothing more);
- It will help to reduce the total amount of SPAs that are needed to conduct and transact CMMC functionalities.

Keep in mind that the Secure Enclave is still very new, but at KAMIND IT, we are keeping up to date with all of the latest developments. Contact us if you would like more information, or have questions about it.

Sources

1) https://csrc.nist.gov/pubs/sp/800/171/r3/final
2) https://www.cmmcaudit.org/what-is-fci-in-cmmc/
3) https://www.cmmcaudit.org/cmmc-scope-are-you-ready-for-an-assessment/#:~:text=Security%20Protection%20Assets%20(SPA),security%20plan%20in%20this%20regard.