10 FAQs About CMMC Compliance

If a DoD contractor handles CUI, does every employee in the company need to be part of the security boundary?

The documentation for the CMMC model v1.02 states that: "when implementing CMMC, a DIB contractor can **achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s)**, depending upon where the information to be protected is handled and stored."

So, the "enclave model" for protecting CUI is supported by CMMC policies and the security boundary can include only those employees that handle CUI.

Can I continue to use Commercial O365 or Gmail if I need to be CMMC compliant?

You can continue to use platforms like Commercial O365 and Gmail but they must be separated from your compliance boundary and not handle CUI.

What is my responsibility for protecting CUI I receive from my contractors as well as CUI I need to share with my own suppliers?

If you receive CUI from your prime, it should already be marked as such. You will need to handle the CUI according to the policies and procedures laid out in your System Security Plan (SSP).

If you share CUI with your own suppliers, you'll want to make sure they have a compliant environment for storing and handling CUI. You also want to make sure you share CUI with the proper encryption according to the procedures stated in your SSP.

If I have a DFARS 7012 clause in my contract, what is my responsibility to my suppliers and subcontractors. What are the key responsibilities of my Cloud Service Provider (CSP)?

My responsibility to my suppliers is that I must comply with the 110 NIST 800-171 controls and be prepared to support the 130 CMMC practices when contracts begin to include CMMC.

My responsibility to my subcontractors is to flow down the DFARS 7012 requirement to them and ensure they meet the 110 NIST 800-171 controls and 130 CMMC practices when they appear in contracts.

The responsibility of my CSP is to ensure we can meet the requirements for cyber incident reporting detailed in DFARS 7012 paragraphs c-g. Additionally, the CSP must also have achieved FedRAMP moderate equivalency.

As a DoD contractor, do I have to comply with FedRAMP standards?

FedRAMP standards require that any cloud services provider (CSP) storing CUI must address FedRAMP Moderate controls. Most defense contractors are not CSPs themselves, instead they store federal data with a CSP. So, the defense contractor does not need to be FedRAMP compliant but the CSPs they work with do need to meet this level of compliance. Make sure that the CSP you are planning to work with is storing data in a sovereign Continental US "FedRAMP Authorized" cloud.

Do I need to rip out my existing email and file sharing systems and replace them in order to become CMMC level 3 compliant?

One option is to replace your existing technologies to support CMMC level 3 compliance. However, an alternative is to maintain your existing systems for non-CUI management and deploy an enclave for CUI so that the information is protected per the requirements detailed in the NIST 800-171 and CMMC controls.

I don't have inhouse experience with CMMC compliance. Who can help me?

Many small and large defense companies don't have the inhouse expertise and knowledge required to put their company onto a CMMC compliance path. For these organizations, there are a number of qualified MSPs, MSSPs or consulting organizations who can help.

PreVeil can help connect you with a qualified partner that has been trained by the CMMC-AB.

If I currently have FOUO (For Official Use Only – a type of CUI) information or CUI, do I have to find it all and migrate it over to a secure Drive? Or since I received it before the DFARS Interim Rule, does that content not apply to CMMC controls?

If you currently have FOUO, you must treat it as CUI and migrate it to a NIST 800-171 and CMMC compliant environment. It cannot remain in noncompliant systems.

What do I need to do if someone emails us CUI outside our secure network?

The company should have a policy in their SSP for handling CUI outside of the compliant network intended for CUI. The policy should include instructions for promptly moving the CUI to the compliant network and sanitizing the CUI from the non-compliant network.

There is some confusion that this event should be reported as an incident to DIBnet per DFARS clause 252.204-7012 but DOD policy states that a cyber incident is defined as a "compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. Assuming the CUI is promptly moved off the non-compliant network it would likely not be considered an incident.

I have heard that CMMC is based on maturity. How do I demonstrate maturity when preparing for an assessment?

Maturity can be demonstrated to assessors or auditors by showing appropriate and complete documentation for the NIST 800-171 or CMMC controls as well as evidence and artifacts that the controls have been in use over a period of at least 3-6 months.