What Defense Contractors need to know about the US Government's CMMC requirements

Cocoon Data

What Defense Contractors need to know about the US Government's CMMC requirements

Just like any other organization, the cybersecurity of the US Department Of Defense (DOD) is only as strong as its weakest link – all DIB organizations are required to be compliant with NIST 800-171, and if ITAR data is involved they are also required to comply with DFARS 7012. Failure to comply already has serious consequences. These smaller companies are often targets for cyber-attacks because they don't have the same levels of cybersecurity that larger organizations have; therefore, they can serve as an entry point for attackers to move up the DoD supply chain.

Because of the alarming increase and continual threat of supply chain attacks from both nation states and cybercriminals alike and the high cost of government data loss from even its smallest contractor, the US Government has decided to implement a Cybersecurity Maturity Model Certification (CMMC) to its entire Defense Industrial Base (DIB) supply chain of contractors and subcontractors.

If you are one of the 300,000-500,000 businesses or organizations either contracted directly to the United States DOD, or working as a subcontractor, you form part of their DIB supply chain. The DOD and CMMC-AB recommend that you, if you haven't already started, begin implementing cybersecurity controls in alignment with NIST 800-171.

What is CMMC?

The CMMC framework implements cybersecurity best practices by standardizing existing data protections and practices for DoD DIB, but in the future this may extend across multiple US departments and agencies. These new unified cybersecurity standards ensure the security of government data on its DIB networks.

There are two main types of unclassified informa-tion DIB contractors and subcontractors handle – Federal Contract Information (FCI) and the more stringently regulated Controlled Unclassified Information (CUI). CMMC ML1 controls are specifically designed to protect FCI, and CMMC ML 2 controls are for CUI protection.

Although CUI is not classified information it still requires some level of protection from unauthorized access and release due to its sensitive nature. Unauthorized disclosure of CUI can severely negatively impact the defense posture of the United States and its allies.

How will CMMC 2.0 impact your organization?

With the updated CMMC 2.0 framework there is a significant realignment to NIST 800-171 controls. However, the new changes focus on accountability and increased scrutiny for the most sensitive data. The DoD has stressed they are not bifurcating CUI into two different classifications, but they are putting a greater emphasis on more sensitive projects.

Given there are still 110 controls for maturity level 2, that is not much time for small teams to implement these often costly and time-consuming controls and the security technology that enables those capabili-ties. Many organizations will now be allowed to self-attest. This does not necessarily mean it will be easier. One mistake could cost your organization dearly, and Cocoon Data has solutions that can reduce these burdens.

What is the difference between CMMC and DFARS?

The Defense Federal Acquisition Regulation Supplement (DFARS) was implemented by the US DoD in 2016 to protect sensitive government data from cybersecurity attacks. Since DFARS has been in place for years already, there is a tight deadline for the implementation of CMMC 2.0.

However, as the US Government comes under increasing threat of cyberattack, it decided to launch the CMMC framework to enhance its cybersecurity defense along its supply chain.

CMMC and DFARS have a lot of similarities, and they both target how your DIB organization uses security controls to protect CUI, but the biggest difference between the two is CMMC’s maturity levels. If there’s an update to either CMMC or DFARs, you’ll need to adhere to both.

Lets take a closer look at the CMMC Model Framework:

Model		Assessment	CMMC Model 1.0
171 Practices	5 Processes	Third Party	LEVEL 5 Advanced
156 Practices	4 Processes	None	LEVEL 4 Proactive
130 Practices	3 Processes	Third Party	LEVEL 3 Good
72 Practices	2 Processes	None	LEVEL 2 Intermediate
17 Practices		Third Party	LEVEL 1 Basic

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ Practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 Practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information: Annual self-assessment for selected programs
LEVEL 1 Foundational	17 Practices	Annual self-assessment

How is the CMMC 2.0 Model; Framework structured?

The CMMC 2.0 Model Framework consists of three levels:

◦Level 1 (Foundational): For companies with FCI only. Information requires protection but is not critical to national security. This level will require DIB company self-assessment. Reports must be submitted to the SPRS.

◦Level 2 (Advanced): For companies with CUI. This level may require third-party or self- assessments, depending on the criticality of information handled.

-For prioritized acquisitions, third-party assessments will be required. Companies will need to undergo an assessment and certifications as a condition of contract award.

-For non-prioritized acquisitions, self-assessments will be required. Companies will complete and report a CMMC Level 2 self-assessment and submit their senior official affirmations. Reports must be submitted to the SPRS.

◦Level 3 (Expert): For the highest-priority programs with CUI. This level will be assessed by government officials.

These requirements will mirror NIST SP 800-171 and NIST SP 800-172. Level 2 aligns with NIST SP 800-171 and Level 3 uses a subset of NIST SP 800-172 requirements.

How flexible are these requirements?

CMMC 2.0 does allow limited use of plan of action and milestones (POA&Ms) and waivers.

Use of POA&Ms will be:

•Very limited. Companies may not use POA&Ms for their highest-weighted requirements. They must meet a minimum score requirement to support certification with POA&Ms.

•Time-bound. Contracting officers can use contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline, which is expected to be 180 days. Use of waivers will be very limited and must be accompanied by strategies for mitigating CUI risk.

Waivers will be:

•Limited to mission-critical instances.

•Strictly time-bound, with timing determined on a case-by-case basis.

•Subject to senior DoD approval to minimize potential misuse.

What actions should your DIB organization take now?

If you're a DoD contractor or subcontractor, having a full understanding of the CMMC's technical requirements will prepare your DIB organization for the quick evolution of the DoD's new cyber security requirements, as well as cement your own cybersecurity capability.

If you start now to evaluate your cybersecurity hygiene practices and procedures, when the details are finalized you will be well-positioned to navigate the process and meet the mandatory CMMC contract requirements for your upcoming projects.

At Cocoon Data we work with DIB organizations worldwide to navigate government compliance regulations, and we know how challenging it can be for defense contractors to keep up with these regularly evolving compliance requirements. We are fully certified to ISO 27001 and undertake regular external audits to ensure we meet strict, documented standards.

$25

USD

Per user*
Per month
USA Hosted

Start sharing securely today

Our simple subscription package is designed for immediate deployment with no lock-in contracts. With a choice of data sovereignty, you choose where your data is hosted.

It's your business; keep it that way.

*Minimum 10 users per month

Contact us to find out how using our file sharing platform can assist in obtaining your Cybersecurity Maturity Model Certification (CMMC).

Cocoon Data

Contact

+1 303 536 1115
Washington

info@cocoondata.com

Cocoondata.com