UNANET WHITE PAPER

A DOD Contractor's Guide to CMMC

Strategic insight on the Department of Defense's Cybersecurity Maturity Model Certification and how it will impact your government contracting business .

OVERVIEW

If you're a government contractor (GovCon), you can't underestimate your need to establish solid cybersecurity principles. Beyond the general importance of safeguarding your data, people, and systems, there are also strict government mandates designed to ensure GovCons are maintaining proper cybersecurity protocols.

While these mandates help keep GovCons honest in terms of maintaining a satisfactory cybersecurity posture, achieving compliance can be a tough ask in practice. The U.S. Department of Defense (DOD)'s Cybersecurity Maturity Model Certification (CMMC) is a perfect example of regulatory guidance that can be challenging for GovCons supporting DOD. These requirements will likely be leveraged by other government agencies in the future as well.

CMMC can be a complicated topic to discuss, but this guide will prepare your GovCon to achieve compliance AND become more secure as an organization.

Let's dive into...

- **What CMMC is and why it exists**
- **Where it stands today and updated rollout timeline.**
- **The implications for you as a DOD GovCon**
- **The problems facing DOD cybersecurity experts as they try to protect our data**
- **How you can company can get the CMMC compliance support it needs**

THE ORIGINS OF CMMC

Over the past decade, DOD has become increasingly concerned about cybersecurity. This has led to the department prioritizing the protection of government institutions and the DOD supply chain from cyberattacks. The agency believes the traditional measures of GovCon performance – cost, schedule, and quality – are only effective and applicable in a secure environment. Through the CMMC framework, the DOD tells defense contractors they must meet certain cybersecurity standards to work for the DOD in the future.

The first attempt to address cybersecurity issues was an informal request by the government that all GovCons comply with National Institute of Standards and Technology (NIST) Special Publication 800-171 requirements. After that, the first Cybersecurity Maturity Model Certification – CMMC 1.0 – was unveiled by the DOD in 2019. This proposed guidance provided a new cybersecurity compliance framework for DOD contracts and the data associated with them. It introduced a DOD certification process that measured a company's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

CMMC combines various cybersecurity standards and maps these best practices and processes to three security levels. CMMC 1.0 would have required a third-party assessment for all contractors at all levels. The total number was estimated at more than 300,000, including both prime contractors and subcontractors. After much debate, CMMC 1.0 was rejected because it would be too expensive and burdensome for contractors and government agencies.

In November 2021, DOD released CMMC 2.0. The model described there was similar to management maturity models used by other entities inside and outside the government. CMMC 2.0 contains progressive levels that describe a GovCon's cybersecurity practices and processes from basic cyber hygiene to highly advanced practices.

Finally, in October of 2024, the CMMC rule was finalized and will be implemented in December of 2024. After this, a timeline starts where Level 2 Assessments must be in place for contracts starting in the middle of 2025 - pending any waivers or extensions that will be decided for individual contracts and awards. Full rollout of all 3 levels will continue until the end of 2026.

WHY NOW?

After nearly seven years of debate and lots of iteration. CMMC is finally coming to fruition. The public comment period ended on February 26th, 2024, and the final revision of the rule is expected to be in place by the end of 2024 – potentially earlier. This then starts a clock for certification with a three-year rollout plan.

So, what can GovCons expect from the new requirements?

- For the first sixth months, Level 1 or 2 self-assessments will be a requirement for award
- The next 12 months, Level 2 assessments will be required for new contracts
- The year after that, when applicable, Level 3 assessments will be required

Finally, these requirements will flow down to subcontractors. If you are a sub on a contract that requires level 2 or 3 third-party assessment, you will require the same.

For some GovCons, this may seem simple enough. Others may find themselves asking the differences between each level. Here's what you need to know about them and what you'll need to comply at each stage.

A BREAKDOWN OF CMMC LEVELS

One major difference in CMMC 2.0 is that it focuses on the most critical requirements and streamlines the previous version of the model ***from five compliance levels down to three.*** It removes 20 additional practices and three processes originally in Level 3 to make the standard identical to NIST 800-171 Rev2. Here's what the government expects from your organization at each level.

Level 1: Foundational cyber hygiene practice

This level requires basic cybersecurity protocols deployed by most companies. To reach Level 1, firms need to implement 17 NIST SP 800-171 Rev2 controls. All GovCons will be able to self-certify for Level 1.

Level 2: Advanced cyber hygiene practice

This level requires all NIST 800-171 controls to achieve Level 2 certification and nearly all companies requiring Level 2 will require assessment by a CMMC Third-Party Assessment Organization (C3PAO).

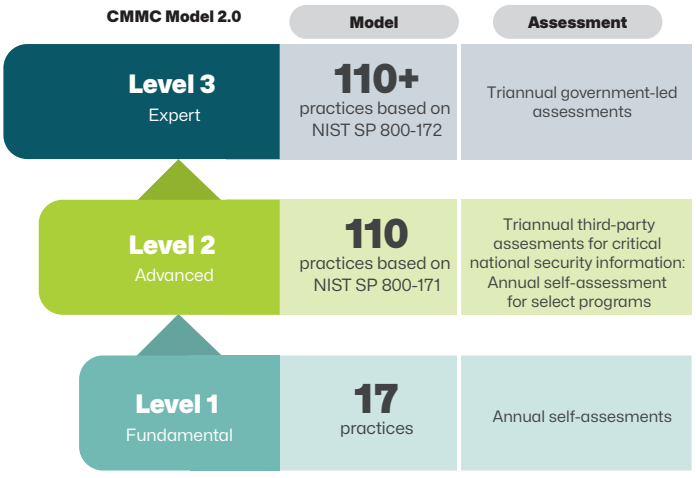
DOD also estimates that approximately 80,000 contractors will fall into this category, 4,000 of which will be able to self-assess. However, a trend appears to be developing among primes to require all subcontractors to be certified at Level 2.

This may increase the number even beyond DOD's estimate. While the number of GovCons that require third-party certification is less than under CMMC 1.0, it is still an exceptionally large number.

Level 3: Expert practice

This level includes advanced cybersecurity processes implemented, reviewed, and updated across the enterprise. Companies at Level 3 will have to implement all NIST 800-171 controls plus an additional subset of NIST 800-172 controls. This aligns with the widely accepted cybersecurity standards set forth by NIST.

CMMC 2.0 Processes



WHAT CMMC MEANS FOR DOD GOVCONS

CMMC implementation is expected to impact a broad range of entities that do business with the DOD. There are six areas in which those entities are likely to be affected by the new policy:

1. All government contractors working with the DOD, except those who provide only Commercial Off-the-Shelf (COTS) items, will need to become CMMC. This is by either a self-assessment and self-certification (for Level 1) or by passing an independent CMMC audit by a C3PAO (for Levels 2 and 3). This is in order to verify that GovCons have met the CMMC requirements for their business. The CMMC level required will be specified for each procurement in its solicitation.

2. The government contractor may not be required to meet the specified certification level at the time of contract award for the next year or so, but may be permitted to submit a binding Plan of Action and Milestones (POA&M) for achieving certification. Acceptance of a POA&M in lieu of certification is at the discretion of the contracting officer and is dependent on the deficiencies identified in the preliminary assessment. This is something of a loophole since there are some realistic concerns about the bandwidth for C3PAOs to assess all 77,000+ companies in less than 18 months.

3. Prime contractors must flow down the appropriate CMMC requirement to the subcontractors they intend to use for a specific contract. Verification of the subcontractors' status will also be the Prime's responsibility.

4. The DOD contracting officer will determine the appropriate CMMC level for the contracts they award and administer. Not all contracts will require the highest level of security and the level required for a particular contract will be specified in the solicitation and in the resulting contract. During the CMMC Pilot Program, the inclusion of a CMMC requirement in any solicitation will require the approval of the Office of the Undersecretary of Defense (OUSD) for Acquisition and Sustainment.

5. The cost of preparing for a CMMC audit and becoming certified will be an "allowable cost" to government contracts. While DCAA has not issued specific guidance yet, it is the opinion of many experts in GovCon accounting and compliance that the cost will almost certainly be an indirect cost – most likely as a general and administrative (G&A) expense.

6. Audits will be performed by an independent C3PAO that has been accredited by "The Cyber AB" (formerly known as the CMMC Accreditation Body). As of April 2023, there were 38 C3PAOs. The Cyber AB is an independent not-for-profit organization that is responsible for training and certifying independent C3PAO auditors. *See a full list of the current C3PAOs at The Cyber AB website.*

DEFINITION AND TREATMENT OF CUI

A key part of CMMC is Controlled Unclassified Information (CUI) – also known as Covered Defense Information (CDI).

CUI Definition

Controlled Unclassified Information is unclassified information the United States Government creates or possesses that requires safeguarding or dissemination controls limiting its distribution to those with a "lawful government purpose." CUI may not be released to the public without further review. There are different types of CUI and different distribution levels. Defined CUI markings alert recipients that special handling may be required to comply with law, regulation, or Government-wide policy. All CUI data must be either marked by the government or in some cases marked by the contractor. Contractors and government officials must undergo annual CUI training.

For contractors, it is their responsibility to handle CUI effectively, and CUI is one of the main triggers for requiring Level 2 CMMC in a contract.

CUI, CSP, and FedRAMP Moderate Equivalency

Authorized or provide evidence of Equivalency – meaning demonstrating they can fully fulfill the requirements of FedRAMP Moderate Authorization. It is the contractor's duty to verify any cloud software they use meets these requirements.

Sources of Confusion

The DoD has stated it anticipates CMMC costing a contractor about $100K and 6+ months to achieve Level 2. Also, DoD estimates there are 80,000 organizations that it says will require Level 2. To date there are only ~55 Certified Third Party Assessors (C3PAO) that MUST perform L2 certifications and they have completed...154 pre-assessments (JSVA). This will be an issue for a long time unless many more C3PAO will be added very quickly.

What is CUI? It should always be marked by the government. However, CUI is up to the discretion of a Contracting Officer (KO). Not all KOs are equal, and they tend to err on the side of caution when it comes to applying clauses and requirements to contracts. This also extends to how they label CUI. They have been doing this for a few years now as part of existing DFARS requirements, and it has been somewhat contentious.

THE CMMC MILESTONE TIMELINE

If you want to stay cyber safe and keep the federal government happy from a CMMC standpoint, you'll want to know about any upcoming deadlines you'll need to comply with. Here's a look at notable dates and expected timing for implementing and complying with CMMC:

- Publication of a Final Rule is expected by the end of 2024.
- Within 60 days of publishing that rule, companies will need to start getting certified to win DOD contracts.
- The phase-in plan for CMMC is a five-year period over which successively more and more solicitations would contain the requirement.

The problem the DOD faces is one of contractor certification. After more than three years of training and testing, there are only 242 authorized C3PAOs today (and counting). With 80,000 companies to certify, this implies that each C3APO must conduct around 300 assessments. Estimating each C3PAO's capacity to conduct 100 assessments annually results in a three-year period to complete all mandatory assessments.

Nonetheless, Murphy's Law still holds. If there is only one DOD solicitation that gets the clause this year, it will be the one your business development team has been tracking. And, if it isn't true in 2025, it will be in 2026.

SUPPORT FOR GOVCONS WITH CMMC COMPLIANCE NEEDS

Individual GovCons are facing a new regulatory reality where they will be evaluated for CMMC compliance by an independent, sanctioned third-party auditor. But maintaining awareness is only the first step. You'll want to have easy-to-use software solutions in place to ensure you stay CMMC compliant while also making it easier for your people to get their work done.

One example of a solution that can help you stay CMMC compliant is Unanet's purpose-built business software. Unanet's platform supports relevant technical requirements within its new model related to multifactor authentication, identification and access controls, and data encryption.

The Unanet Cloud Operations team has been diligent about staying aligned with new DOD policies and has taken the necessary steps to ensure that its processes and procedures are also aligned with CMMC and NIST 800-171 standards.

For information on how Unanet can support and simplify your organization's CMMC compliance, visit us at unanet.com.

Unanet

Where Information Means Insight

Unanet is a leading provider of project-based ERP and CRM solutions purpose-built for Government Contractors, AEC, and Professional Services. More than 4,100 project-driven organizations depend on Unanet to turn their information into actionable insights, drive better decision-making, and accelerate business growth. All backed by a people-centered team invested in the success of your projects, people, and financials

ADDRESS
22970 Indian Creek Drive
Suite 200
Dulles, VA 20166

ONLINE
Email: info@unanet.com
Web: unanet.com