EXECUTIVE BRIEF

Cybersecurity Maturity Model Certification (CMMC)

AEROSPACE & DEFENSE

Beginning in Fall 2020, defense contractors face the very real threat of losing business if they are non-compliant with the newly released Cybersecurity Maturity Model Certification (CMMC) standard.

Under the current regulations — DFARS 252.204-7012 — contractors must implement security controls identified in NIST SP 800-171 that safeguard Controlled Unclassified Information (CUI). Contractors can self-attest to compliance after the contract is won, but security gaps may remain unidentified and unmitigated until a government DFARS audit is conducted.

With CMMC, self-attestation is out, and contractors must be audited and certified before they can bid on RFPs. The Department of Defense (DoD) is working with the CMMC Accreditation Body, an independent third party that will be responsible for operational aspects of the certification. These responsibilities include training third-party assessment organizations (C3PAOs) and licensing individual assessors.

What You Need to Know: Cybersecurity Maturity Model Certification (CMMC)

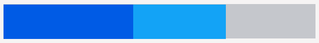
- First RFPs to contain CMMC requirements will appear in Fall 2020
- CMMC will apply to all subcontractors, regardless of their supply chain tier position
- Contractors must achieve 100% adherence BEFORE bidding on contracts
- Only certified assessors can provide CMMC validation
- Remediation plans or Plan of Action & Milestones (POA&M) are NOT allowed
- Certification is valid for 3 years
- CMMC will NOT be applied retroactively to existing contracts
- Certification costs are an allowable, reimbursable cost

The five Cybersecurity Maturity Model Certification (CMMC) Levels

The CMMC framework organizes cybersecurity processes, capabilities, and practices into a set of 17 capability domains mapped across five levels. These five levels represent a progression in cybersecurity capabilities, introducing and characterizing additional processes and practices required to achieve certification at each level.

Level 1 focuses on "basic cyber hygiene" practices such as regularly changing passwords and using anti-virus software. Level 2 is a transitional step to Level 3. Level 3 requires a significant increase from 72 to 130 practices, and the incorporation of organizational policy in order to protect CUI.

Levels 4 and 5 are intended for very critical technology companies working on the most sensitive programs. These levels require active cyber defense processes and practices against the tactics, techniques, and procedures used by Advanced Persistent Threats (APTs).

	Processes (# at each level)	Practices (# at each level)	Relationship to existing regulations
LEVEL 1	Performed (0) 	Basic Cyber Hygiene (17) 	• Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21
LEVEL 2	Documented (2) 	Intermediate Cyber Hygiene (72) 	• Comply with the FAR • Includes a select subset of 48 practices from the NIST SP 800-171 r1
LEVEL 3	Managed (3) 	Good Cyber Hygiene (130) 	• Comply with the FAR • Encompasses all practices from NIST SP 800-171 r1
LEVEL 4	Reviewed (4) 	Proactive (156) 	• Comply with the FAR • Encompasses all practices from NIST SP 800-171 r1 • Includes a select subset of 11 practices from Draft NIST SP 800-171B
LEVEL 5	Optimizing (5) 	Advanced / Progressive (171) 	• Comply with the FAR • Encompasses all practices from NIST SP 800-171 r1 • Includes a select subset of 4 practices from Draft NIST SP 800-171B

Frequently asked questions: CMMC Levels

Q: How do I know what certification level I need?

A: Each RFP will state the CMMC levels required for specific roles, which will likely be found in Sections L and M, as well as the Statement of Work. Subcontractors may require a lower maturity level than prime contractors, with final determinations based on contract negotiations and decisions on what information will be shared.

Q: Are my assessment results made public?

A: No, the results of a CMMC assessment will not be made public. The only information that will be publicly available is whether your organization is CMMC certified. The specific certification level will NOT be made public.

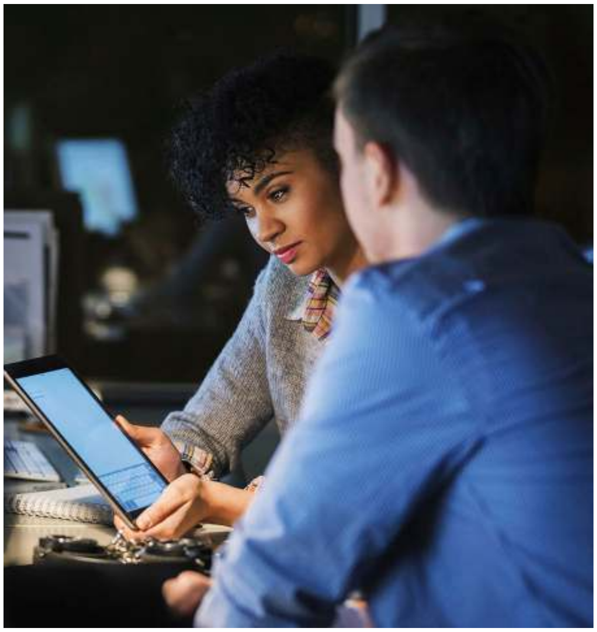
Q: I'm a subcontractor on a DoD contract. Do I need to be certified?

A: Yes, your organization is required to have its own certification at the required CMMC level. Subcontractors are NOT covered by the CMMC certification of their prime contractor.

Five steps to CMMC Success

Contractors should begin preparing now for self-assessment and third-party certification. Successfully meeting CMMC level requirements may include investment in additional IT staff, migrating IT infrastructure, and evaluating different back office business systems, network solutions, or end user devices and software. In addition to additional resources, organizations will also need to produce and maintain extensive documentation of organizational standards, policies, and procedures as evidence of compliance.

Here are five steps you can take now to position yourself for success.



Step 1: Identify your target maturity level

An organization's target maturity level depends on current contracts and programs you'd like to bid on in the future. Both current contractors and those new to DoD programs should review the RFIs and RFPs expected in Fall 2020 to understand what maturity levels are being required for typical program roles.

> Work on projects requiring ITAR compliance? You need to achieve CMMC Level 3 certification, at a minimum.

Step 2: Determine whether external security or compliance services are needed.

Contractors need to consider the overall business impact and cost when deciding whether to pursue CMMC certification entirely in-house or to engage external expertise and services. The quickest way to achieving CMMC certification may be to outsource some security and compliance activities to consultants or third-party IT solution vendors. The tools and skills required to achieve CMMC certification can mean a significant change in operating expenses, personnel, and administrative overhead.

> Organizations that find themselves facing one or more of the following circumstances should work with qualified third-party advisors:
>
> - May require Level 3 or above
> - Are facing NIST SP 800-171 for the first time
> - Have no dedicated security personnel

Step 3: Conduct a self-assessment and update security documentation.

This step should help make the actual certification process go as efficiently as possible, providing contractors with a clear look at what security controls they need to implement, what processes they need to improve and what documentation they need to have in place to achieve certification. The self-assessment asks about security control implementation and evaluates whether the security controls are sufficiently documented, captured in policy, managed, and reviewed per each of the CMMC level requirements.

> Reference the NIST Handbook 162, a self-assessment handbook for NIST SP 800-171 that uncovers baseline readiness to identify all gaps and inform development of a preliminary remediation plan for each. These plans need to be documented within a Plan of Action & Milestones (POA&M).

Step 4: Remediate gaps

The POA&M created in Step 3 serves as a to-do list to better organize, prioritize, and track the completion of all gap closure activities. Actions in the POA&M may require development of new organizational standards, policies, and procedures. Larger gaps may mean modifying the architecture of an organization’s IT infrastructure and procurement of new software and IT security solutions.

> Consider reaching out to cloud-based software providers to see how they can help. Their products may already have the security protocols in place to satisfy CMMC requirements.

Step 5: Conduct CMMC readiness assessment

After completing the previous steps, organizations are ready to repeat their CMMC self-assessment as a final readiness check before the actual C3PAO audit. Organizations that have not used external services yet may consider doing so now to raise their level of confidence. This can also serve as a practice run for the actual audit.

> “
> Repeat the self-assessment until all gaps and POA&M items have been addressed.

While the timeline for CMMC is evolving, here are some estimated dates to track (as of May 2020):

May 2020
CMMC AB Marketplace

June 2020
Initial RFIs with CMMC Requirement

July 2020
Initiate CMMC AB training for assessors and Defense Acquisition University training for acquisition officials for Levels 1-3

Sept 2020
Complete DFARS Rulemaking Process

September 2020
Initiate CMMC AB training for assessors and Defense Acquisition University training for acquisition officials for Levels 4-5

October 2020
Initial RFPs with CMMC Requirement (dependent on final Rulemaking)

Beyond meeting federal regulations, contractors who prioritize rigorous cybersecurity best practices now will substantially differentiate themselves from competitors. Companies that delay certification may get caught in a backlog of assessments that cause business opportunities to pass them by. Prime contractors will be looking for certified subcontractors that enable them to confidently incorporate suppliers and partners into their supply chains. Getting ahead of CMMC mitigates the risk of cyberattacks not only on CUI, but also on company intellectual property.

Read the Cybersecurity Maturity Model Certification (CMMC) Best Practices Guide for more information on the CMMC and how it can help your organization accomplish your cybersecurity mission.

DOWNLOAD NOW →

infor Gold Channel Partner

GODLAN

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

641 Avenue of the Americas, New York, NY 10011

INFDTP2345357-en-US-0620-1

Godlan, Inc.
15399 Canal Road
Clinton Township, MI 48038
586-464-4400
info@godlan.com
www.Godlan.com