EXECUTIVE BRIEF

# Updated Cybersecurity Maturity Model Certification (CMMC)

Aerospace & Defense

Defense contractors face the very real threat of losing business if they are noncompliant with the Cybersecurity Maturity Model Certification (CMMC) standard.

The CMMC is a new cybersecurity framework by the US Department of Defense (DoD) for the DoD supply chain and its contractors. The goal of the CMMC compliance requirement is to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

This new umbrella standard includes requirements from National Institute of Standards and Technology (NIST) SP 800-171, Federal Acquisition Requirements (FAR) document 52.204-21, and beyond. In the latest iteration, CMMC 2.0 (announced November 4, 2021), there are three levels of CMMC compliance. Each level requires more practices and controls than the previous. Most organizations will have to comply with either Level 1 or Level 2.

With CMMC, self-attestation is out, and contractors must be audited and certified before they can receive new contract awards. The DoD is working with the CMMC Accreditation Body, an independent third party that's responsible for operational aspects of the certification.

These responsibilities include training third-party assessment organizations (C3PAOs) and licensing individual assessors.

To spur CMMC compliance, the final rule in 2020 added a new requirement that defense contractors must submit a NIST SP 800-171 self-assessment into the Supplier Performance Risk System (SPRS). While the numeric score, with a maximum of 110 possible points, is not used to evaluate suppliers, the self-assessment must be submitted before contract award. While NIST SP 800-171 compliance has been a requirement since December 2017, this is an opportunity for companies to reevaluate their security posture in preparation for CMMC.

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. Prime contractors are sending out supplier surveys that are very similar to the SPRS request, asking for attestations of compliance or timelines for anticipated completion of all the security controls. Companies without a strategy in place risk losing their preferred supplier status.

Getting ahead of CMMC mitigates the risk of cyberattacks not only on CUI, but also on company intellectual property.

## The three CMMC levels

The CMMC 2.0 model has been streamlined from five to three levels

- Eliminates CMMC 1.0 Levels 2 and Levels 4; these levels were originally intended as transition levels and not meant to be assessed requirements
- Eliminates all CMMC unique practices and maturity processes; works with NIST to address identified gaps in NIST SP 800-171
- Establishes three levels, each one more advanced than the last, and based on the specific type of information
  - Level 1 (Foundational)—For companies with FCI only; the information must be protected but isn't critical to national security
  - Level 2 (Advanced)—For companies with CUI
  - Level 3 (Expert)—This applies to the top-priority programs with CUI requirements; it mirrors NIST SP 800-171 and NIST SP 800-172
- Level 1 addresses "basic cyber hygiene" practices, like regularly changing passwords and using anti-virus software
- Level 2 is a transitional step to Level 3; aligns Level 2 with NIST SP 800-171
- Level 3 uses a subset of NIST SP 800-172 requirements; Level 3 requires a significant increase from 72 to 130 practices, and includes organizational policy to protect CUI

## What's changed under CMMC 2.0?

To simplify compliance with DoD cybersecurity standards, the CMMC 2.0 framework implements a new tier system for the sensitivity of DoD information. The five-tier security system introduced in the original CMMC framework is now revised down to three. Originally, any external firm doing business with the DoD was required to meet one of five CMMC levels: basic cyber hygiene, intermediate cyber hygiene, good cyber hygiene, proactive, or advanced.

Under the original CMMC framework, contractors were required to undergo a third-party security assessment. This has been relaxed in CMMC 2.0. Now, only those contractors handling sensitive data are required to meet these qualifications, while contractors handling less critical data can perform self-assessments.

| CMMC Model 1.0 | | | | CMMC Model 2.0 | | |
|---|---|---|---|---|---|---|
| Model | | Assessment | | | Model | Assessment |
| **171** practices | **5** processes | Third-party | **LEVEL 5** Advanced CUI, critical programs | **LEVEL 3** Expert | **110+** practices based on NIST SP 800-172 | Triennial government-led assessments |
| **156** practices | **4** processes | None | **LEVEL 4** Proactive Transition level | | | |
| **130** practices | **3** processes | Third-party | **LEVEL 3** Good CUI | **LEVEL 2** Advanced | **110** practices aligned with NIST SP 800-171 | Triennial third-party assessments for critical national security information: annual self-assessment for select Programs |
| **72** practices | **2** processes | None | **LEVEL 2** Intermediate Transition level | | | |
| **17** practices | | Third-party | **LEVEL 1** Basic FCI only | **LEVEL 1** Foundational | **17** practices | Annual self-assessment |

**Level 1 (Foundational)** applies to contractors that neither receive, process, or create controlled CUI, nor handle high value assets (HVA). At this level, companies must perform self-assessments of their security protocols, as well as have them monitored and confirmed by company leadership. This must happen annually and is aligned with the existing FAR 52.204-21 standard.

**Level 2 (Advanced)** applies to contractors who receive, process, or create CUI, but not HVA. There are two subsections, depending on whether a company handles CUI that's classified as Critical National Security Information. Those that don't, can perform an annual self-assessment. Those that do require a third-party assessment, will be required to do so once every three years, which can be conducted by C3PAOs. This is aligned with the existing NIST SP 800-171 standard.

**Level 3 (Expert)** applies to any contractor that handles HVA. Assessments at this level must be completed by the government, rather than a C3PAO. This is aligned with the existing NIST SP 800-172 standard.

As the revised CMMC reduces the number of contractors that need a third-party security assessment, the DoD anticipates a faster rollout and implementation. The original CMMC standards were intended to be adopted over a five-year period. This lengthy process was criticized by those who advocated for stricter measures to be applied immediately. The DoD took this feedback seriously and emphasized the importance of speeding up progress and streamlining cybersecurity protocols as the driving factor behind its release of CMMC 2.0.

CMMC 2.0 also allows for "Plan of Action and Milestone" reports, otherwise known as PoAMs. These can be used by contractors that currently don't meet the security requirements. This allows them to continue to bid on DoD contracts, provided they also submit an outline of how they will implement security procedures in the future.

## What you need to know: Cybersecurity Maturity Model Certification (CMMC)

- CMMC applies to all subcontractors, regardless of their supply chain tier position
- Contractors must achieve 100% adherence ***before*** they can receive new contract awards
- Only certified assessors can provide CMMC validation
- Remediation plans or Plan of Action & Milestones (POA&M) are ***not*** allowed
- Certification is valid for three years
- CMMC will ***not*** be applied retroactively to existing contracts
- Certification costs are an allowable, reimbursable cost

## How should DoD contractors prepare for CMMC 2.0?

Although CMMC 2.0 reduces the burden of cybersecurity audits and other requirements for many DoD contractors compared to the original proposals, contractors shouldn't become complacent.

To prepare for CMMC 2.0, the first step is to determine which level of compliance applies to your business. This will depend on whether you handle CUI or HVA.

LEARN MORE

Follow us:

Infor is a global leader in business cloud software specialized by industry. Over 65,000 organizations in more than 175 countries rely on Infor's 17,000 employees to help achieve their business goals. Visit www.infor.com.

Copyright© 2022 Infor. All rights reserved. The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All other trademarks listed herein are the property of their respective owners. www.infor.com.

641 Avenue of the Americas, New York, NY 10011

INF-2642255-en-US-0222-1