CMMC 2.0

New Hampshire
PROCUREMENT TECHNICAL ASSISTANCE CENTER

Cybersecurity Maturity Model Certification Version 2.0

The Way Forward in 2022 and Beyond

March 3, 2022

Background on CMMC

- 2013 NDAA led to development of **DFARS 252.204-7012** Safeguarding Covered Defense Information and Cyber Incident Reporting. It is a rule. It applies only to defense contracts
- DFARS 252.204-7012 sparked the creation of **NIST 800-171** – the core "standard" that tells us what we have to do to comply with the rule.
- Compliance was required by 12/31/2017. There was no enforcement or meaningful support. Consequently, compliance has been insufficient.
- DoD changed its approach from voluntary compliance to mandatory certification, leading to the development of **CMMC**.
  - Based on NIST 800-171, **CMMC** is a multi-level, formal certification administered by 3rd parties (not the government). It is modeled after the ISO certifications.
  - Subsequent DFARS rules require concrete steps to be taken **now.** Certification will be required by 2025, **but in some cases is required today.**

Background on CMMC

- FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems – This contract clause probably slipped into your federal contracts and subcontracts – almost all of them, not just DoD.
- It requires you to certify that you have certain cybersecurity measures in place.
- FAR 52.204-21 is virtually identical to CMMC Level 1.
- As a result, CMMC Level 1 is becoming the basic cybersecurity benchmark for essentially all businesses.

What is CMMC 2.0

Source: Federal Register 11/17/2021

- *In March 2021, the Department (DOD) initiated an internal assessment of CMMC 1.0 implementation that was informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment of CMMC engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation. This review resulted in "CMMC 2.0," which updates the program structure and the requirements to streamline and improve implementation of the CMMC program.*

Key Modifications to CMMC (Feb 2022)

- *Eliminating levels 2 and 4, and renaming the remaining three levels in CMMC 2.0 as follows:*
- *○ Level 1 (Foundational) will remain the same as CMMC 1.0 Level 1;*
- *○ Level 2 (Advanced) will be similar to CMMC 1.0 Level 3;*
- *○ Level 3 (Expert) will be similar to CMMC 1.0 Level 5.*
- *Removing CMMC-unique practices and all maturity processes from all level*
- *For CMMC Level 1 (Foundational), allowing annual self-assessments with an annual affirmation by DIB company leadership;*

Source: Federal Register 11/17/2021

Key Modifications to CMMC (Feb 2022)

- *Bifurcating CMMC Level 2 (Advanced) assessment requirements:*
  - *Prioritized acquisitions involving CUI will require an independent third-party assessment;*
  - *Non-prioritized acquisitions involving CUI will require an annual self-assessment and annual company affirmation;*

Source: Federal Register 11/17/2021

Late News Feb 10 2022 Federal News Network:

When the Pentagon initially announced the "CMMC 2.0", DoD planned on "bifurcating" requirements for the approximately 80,000 contractors that handle controlled unclassified information (CUI).

At the time, officials said only half of those 80,000 manage CUI that is truly sensitive if it were to fall into the hands of U.S. adversaries. While those contractors would still be required to get a third-party assessment, officials anticipated the other 40,000 managing less risky data would only need to submit a self-assessment.

But during a Feb. 10 town hall, Deputy DoD CIO David McKeown said further analysis has shown all 80,000 will require third-party assessments.

Key Modifications to CMMC (FEB 2022)

- *For CMMC Level 3 (Expert), requiring Government-led assessments.*
- *Developing a time-bound and enforceable Plan of Action and Milestone process; and,*
- *Developing a selective, time-bound waiver process, if needed and approved.*

Source: Federal Register 11/17/2021

Way Forward Outline

- *The title 32 CFR rulemaking for CMMC 2.0 will be followed by additional title 48 CFR rulemaking, as needed, to implement any needed changes to the CMMC program content in 48 CFR.* ***DoD will work through the rulemaking processes as expeditiously as possible.***
- *Until the CMMC 2.0 changes become effective through both the title 32 CFR and title 48 CFR rulemaking processes,* ***the Department will suspend the CMMC Piloting efforts and will not approve inclusion of a CMMC requirement in DoD solicitations. The CMMC 2.0 program requirements will not be mandatory until the title 32 CFR rulemaking is complete****, and the CMMC program requirements have been implemented as needed into acquisition regulation through title 48 rulemaking.*

Source: Federal Register 11/17/2021

DFARS 252.204-7012 Catch!

- **DFARS 252.204-7012**. Safeguarding Covered Defense Information and Cyband is er Incident Reporting
  - https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.#DFARS-252.204-7012
- This DFAR contract clause is likely included in most/all federal defense contracts and subcontracts
- Covered Defense Information is Controlled Unclassified Information (CUI) as described in the CUI Registry marked (CUI) or otherwise available in support of the performance of a contract.
  - http://www.archives.gov/cui/registry/category-list.html

Notes

- CMMC 2.0 Level 1 remains focused on access to Federal Contracting Information (FCI) – that is information that the government does NOT intend to release to the public.
- CMMC 2.0 Level 2 covers CUI – Controlled Unclassified Information. CUI is NOT "Classified" information but is information that must be controlled
- Cybersecurity compliance requirements apply to government contractors & subcontractors at all tiers.
- There are exemptions for:
  - Micro-purchases – Purchase Card buys under $10,000
  - COTS contracts – contracts for commercial, off-the-shelf items
- If your contracting business with the government involves contracting both above and below micro-purchase and/or for COTs and non-COTS, CMMC compliance will be required.

DFARS 252.204-7012 Catch!

Key CUI Security Requirements

- ***Adequate security*** for your (contractor) information system - defined as "an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information."
- Requirements for "adequate security" refer to the security requirements in the **NIST Special Publication 800-171** (now Revision 2), "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations".
  - SP 800-171 Rev. 2, Protecting CUI in Nonfederal Systems and Organizations | CSRC (nist.gov)
- Note: This requirement is stated to be implemented not later that December 31, 2017.

DFARS 252.204-7012 Catch!

Key CUI Security Requirements

- ***Cyber incident reporting requirement*** *in the event of discovery of a cyber incident that affects a covered contractor information system or the covered defense information residing on contractors system*
- ***Malicious software –*** *handling of malicious software in connection with a reported cyber incident*
- *Additional media preservation, access, damage assessment activities and related safeguarding of related contractor information*
- ***Requirements for Flow-down Adequate security requirements noted above to Subcontractors which will include covered defense information***

DFAR 252.204-7012 Catch!

- **DFARS 252.204-7012**. Safeguarding Covered Defense Information and Cyber Incident Reporting
- This DFAR contract clause is most likely included in many (most) federal contracts and subcontracts – almost all of them, not just DoD.
- 15 Key Safeguarding Requirements - cybersecurity requirements which are virtually identical to CMMC Level 1 (1.0 and now 2.0)
- Applies flow-down requirements from Prime to Subcontractors
- As a result, CMMC Level 1 (same in CMMC 2.0 as in 1.0) is becoming the initial cybersecurity benchmark for essentially all businesses.
- Level 1, now titled "Foundational" requires you to certify that you have the 17 specific cybersecurity measures in place.
- 5230.24

Our Advice

Work on completing Self Assessment of CMMC 2.0 Level 1 Foundational requirements (see list on following pages). If you have completed a CMMC 1.0 Level 1 self assessment, you will want to start an annual process of review.

If you are a defense contractor, subcontractor or supplier, you may have DFARS 252.204-7019 in your contract. If so, you must upload your score into a DoD database called the Supplier Performance Risk System (SPRS).

SPRS is accessed through the Procurement Integrated Enterprise Environment (PIEE). If you sell to DoD, you are probably already familiar with PIEE as the home of Wide Area Workflow (WAWF), DoD's online invoicing tool.

NH PTAC can help you understand what you need to do and how to submit your score through these systems

Self-Assessment guidance and tools are readily available including the vast sources related to NIST 800-171 Rev 2.

Level 1 Foundational Requirements -17

- **Access Control (AC)**

1.001: Limit information system access to authorized users, process acting on behalf of authorized users, or devices (including other information systems)

1.002 Limit information system access to the types of transactions and functions that authorized uses are permitted to execute

1.003 Verify and control/limit connections to and use of external information systems

1.004 Control information posted or processed on publicly accessible information systems

- **Identification and Authentication (IA)**

1.076 Identify information system users, processes acting on behalf of users, or devices

1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems

Level 1 Foundational Requirements -17

- **Media Protection (MP)**

1.118 Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse

- **Physical Protection (PP)**

1.131 Limit physical access to organization information systems, equipment, and the respective operating environments to authorized individuals

1.132 Escort visitors and monitor visitor activity

1.133 Maintain audit logs of physical access devices

1.134 Control and manage physical access devices

- **System and Communications Protection (SC)**

1.175 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems

1.176 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

Level 1 Foundational Requirements -17

- **System and Information Integrity (SI)**

1.210 Identify, report, and correct information and information system flaws in a timely manner

1.211 Provide protection from malicious code at appropriate locations within organizational information systems

1.212 Update malicious code protection mechanisms when new releases are available

1.213 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Cost to Be Cyber Secure?

How badly do you want to be in business? The vast majority of businesses across all sectors are at risk of harm as a result of just being "on the web".

1. Costs will vary greatly, depending on the size and complexity of your business, and the degree of your reliance on IT.
2. There are four categories of cost to understand:
   - Initial cost to get into compliance
   - Costs to get assessed/certified (if required)
   - Ongoing costs to maintain secure systems
   - Future Update/upgrade costs driven by
     - Business growth/change
     - Technology changes

Conclusions

Good Cybersecurity is certainly a common necessity going forward

- At present time, you only will need to be "certified" if you are a DoD contractor or subcontractor – this due to FAR and DFAR clauses already in force.
- It will take time and effort for Level 2 – and probably require outside assistance and third party certification
- Management buy-in is critical, and compliance at all electronic connections within an organization must be assured.
- Your IT staff will be responsible for many of the details, but they should not lead your program. Management must take the lead.

Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward

A Proposed Rule by the Defense Acquisition Regulations System on 11/17/2021

PUBLISHED DOCUMENT

Start Printed Page 64100

AGENCY:

Office of the Under Secretary of Defense for Acquisition and Sustainment, Department of Defense (DoD).

ACTION:

Advanced notice of proposed rulemaking.

SUMMARY:

This document provides updated information on DoD's way forward for the approved Cybersecurity Maturity Model Certification (CMMC) program changes, designated as "CMMC 2.0." CMMC 2.0 builds upon the initial CMMC framework to dynamically enhance Defense Industrial Base (DIB) cybersecurity against evolving threats. The CMMC framework is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors and provide assurance that Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) will be protected at a level commensurate with the risk from cybersecurity threats, including Advanced Persistent Threats. Under the CMMC program, DIB contractors will be required to implement certain cybersecurity protection standards, and, as required,

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
11/17/2021

Agencies:
Office of the Secretary
Defense Acquisition Regulations System

Dates:
November 17, 2021.

Document Type:
Proposed Rule

Document Citation:
86 FR 64100

Page:
64100 (1 page)

CFR:
32 CFR chapter undef
48 CFR chapter II

Document Number:
2021-24880

DOCUMENT DETAILS

Key Resources

- Federal Register
- NIST 800-171

  Includes further links to POAM Template, SSP Template

- OUSD A&S - Cybersecurity Maturity Model Certification (CMMC) (osd.mil)

  A new DOD website with significant content and guidelines

- CMMC Accreditation Body

Thank you!

New Hampshire Procurement Technical Assistance Center
Division of Economic Development
Department of Business and Economic Affairs
100 North Main Street, Suite 100
Concord, NH 03301
603-568-8485
nheconomy.com/sell-to-the-government
Email: govcontracting@livefree.nh.gov

Deborah Avery Danielle Bishop Jane Brezosky Larry Findeiss Dave Pease