guernsey

CMMC Readiness:

Considerations for preparation, assessment, and continued compliance

Laura Fawcett, CISM, CGEIT | Managing GRC Consultant

Contents

Introduction

Good Cybersecurity is critical for nearly all organizations, but for Federal contractors, especially those working with the Department of Defense (DoD), there are some specific cybersecurity requirements that must be understood and implemented to win and maintain contacts. Most contractors know these requirements are in their contracts and they've been hearing about the Cybersecurity Maturity Model Certification (CMMC) for years now, but may not understand what is really involved and how it could impact their future DoD contracts.

What is Required Today

There are currently multiple Cybersecurity related clauses in Federal and DoD contracts.

- **FAR 52.204-21:** The Government expects and requires contractors to protect their systems that handled federal contract information with 15 "basic" cybersecurity requirements – This "Basic Safeguarding of Covered Contractor Information Systems" clause is added to all Federal contracts [1].

- **DFARS 252.204-7012:** The DoD mandates that contractors protect systems that handle "Covered Defense Information" (also known as controlled unclassified infrmation – CUI) by following the requirements outlined in NIST 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" along with additional requirements for cloud systems and reporting cyber incidents [2]. Contractors have been expected to comply with NIST 800-171 since December 31, 2017. There is currently a proposed rule that would require compliance with 800-171 for ALL federal contracts. [3]

- **DFARS 252.204-7019/7020:** To understand how well contractors are complying with the requirements of the DFARS 7012 clause, the DoD added these clauses to contracts to define assessment critieria and establish requirements for contractors to self-report their compliance status and/or submit to a DoD assessment. [4][5]

DFARS 7019 & 7020 were part of DoD's interim rule that also included CMMC 1.0 (DFARS 252.204-7021). CMMC 1.0 included 5 levels and requirements above and beyond NIST 800-171. Because of the complexity and added requirements, it received significant push-back from industry. As a results DoD put the roll-out of CMMC on hold and later released CMMC 2.0.

CMMC 2.0 Overview

The initial draft of CMMC 2.0 was released in late 2021. The simplified 2.0 provided criteria for assessments at three levels rather than five, relying on security requirements from existing regulations and guidelines.

- **Level 1: Basic Safeguarding of FCI:** Requirements: Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21.
- **Level 2: Broad Protection of CUI:** Requirements: Assess compliance with the 110 security reqirements in NIST 800-171 Revision 2.
    - Either a self-assessment or a Certified Third Party Assessment Organization (C3PAO) assessment every three years, as specified in the solicitation. DoD notes that self-assessment vs. third party assessment is decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems and will be designated in the solicitation.
    - Annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2
- **Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats:** Requirements: After obtaining a Level 2 Certificate through a C3PAO asssesment
    - Undergo an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) to determine compliance with NIST 800-172.
    - Provide an annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172.

The DoD has published specific guidelines for determining what assets are in-scope at each level, and the specific assessment criteria. [6]

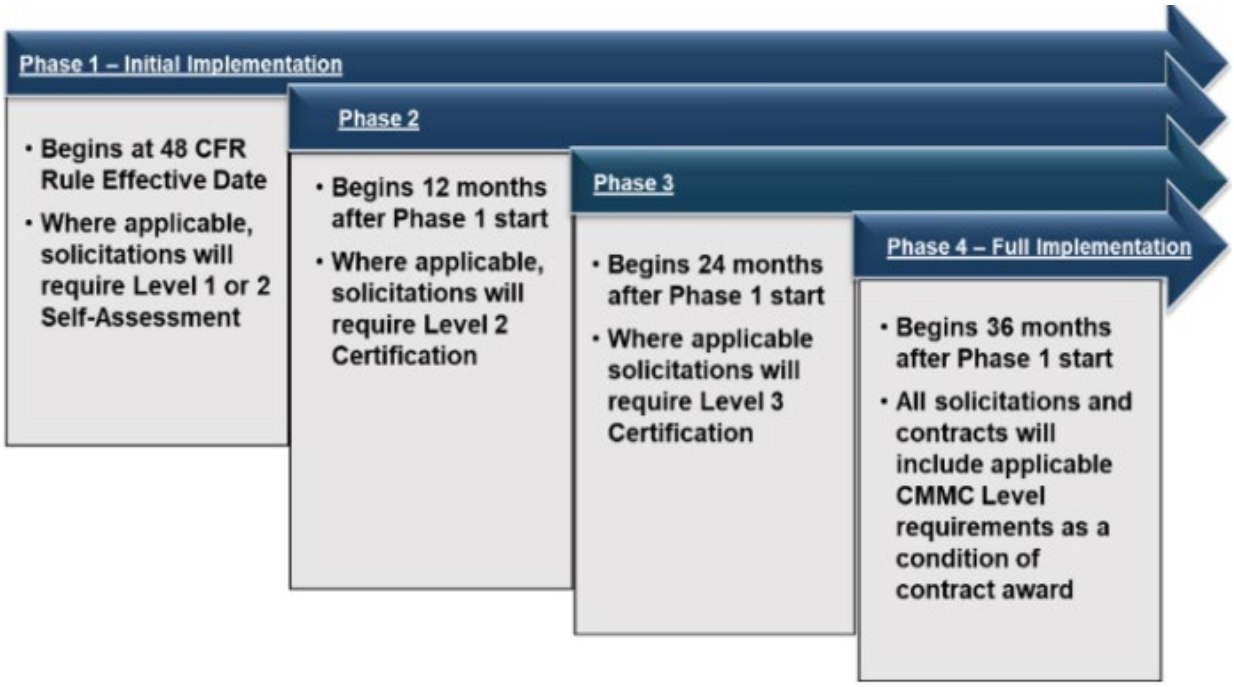
CMMC Timeline

The idea of CMMC has been around for over five years with many fits and starts, and general confusion and frustration for many. With the most recent final rule, the program is here to stay, and it is time for companies have not already prepared, to get ready.

The full CMMC program will be driven by two Federal Rules. The first is 32 CFR Part 170.[7] This rule defines the full program along with a timeline for implementation. The second is a Title 48 CFR acquisition rule [8], which will define the CMMC contract language that will be included in DoD contracts. Below is an overview of the status of both rules.

- August 15, 2024 – Draft 48 CFR (Acquisition rule) published for public review and comment. The final version could be effective before the end of 2025.
- December 16, 2024 – 32 CFR Part 170 becomes effective – Meaning CMMC C3PAO assessment can begin once the ecosystem is ready (estimated to be 1/2/2025).

As stated in the CMMC Rule and described on the DoD's CMMC Page [9], the Phased rollout will begin 60 days after the publication of the final Title 48 CFR CMMC acquisition rule. Current this is estimated to be spring of 2025.



If the 48 CFR CMMC Rule is finalized in late 2025, the phases will begin as follows:
Phase 1 – Begin Q4 2025
Phase 2 – Begin Q4 2026
Phase 3 – Begin Q4 2027
Phase 4 - Begin Q4 2028

Conclusion

Most companies may not see a CMMC Level 2 certification requirement in solicitations until later in 2026, however they may require Level 2 self-assessments - which still requires compliance with most of the NIST 800-171 requirements. Companies should also remember that while CMMC is not currently required in their contracts, the cybersecuity requirements on which CMMC is based are required. These are measures all organizations should have, or should be put in place now. It is also possible that large prime contractors will start requiring CMMC compliance prior to the requirements appearing in solicitations

and contracts. They will want to ensure their supply chain in ready so they can confidently bid any project that may have CMMC requirements.

The other thing to remember is that cybersecurity measures, including CMMC, are not a "one and done" type effort. To achieve and maintain CMMC compliance, organizations need to actively manage and monitor the cybersecurity practices that have been implemented. Even with a third-party assessments only being required every three years, every year organizational leadership must ensure their program has been reviewed and validated, and they must attest to the compliance.

There is currently a limited number of C3PAOs and certified assessors in the ecosystem, so if you are considering scheduling an assessment soon, you should be starting to meet with these companies and getting on their assessment schedule. Guernsey is available to discuss your business model and assessment needs to help you determine the best timing for your organization to kick-off an official certification assessment.

As a C3PAO and DoD contractor Guernsey has a deep understanding of the program, how it impacts organizations, and how organzations can best prepare for an assessment. For organizations not yet ready for a third-party assessment Guernsey can provide readiness assessments and/or support to get you where you need to be.

Citations

[1] FAR 52.204-21 “Basic Safeguarding” - https://www.acquisition.gov/far/52.204-21
[2] NIST SP 800-171 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
[3] DFAR 252.204-7012 “Safeguarding Covered Defense Information” - https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting
[4] DFAR 252.204-7019 “Notice of DoD Assessment Requirements” https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.
[5] DFAR 252.204-7020 “DoD Assessment Requirements” https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.
[6] Resources – “Overview, Scoping Guides, Assessment Guides” - https://dodcio.defense.gov/CMMC/Resources-Documentation/
[7] 32 CFR Part 170 “CMMC RULE” https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program
[8] 48 CFR “Proposed Acquisition Rule” https://www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
[9] “Depatment of Defense Office of CIO CMMC Overview” https://dodcio.defense.gov/cmmc/About/