PAUL HASTINGS

Stay Current

October 2024

Follow @Paul_Hastings

U.S. Department of Defense Set to Implement Its Cybersecurity Maturity Model Certification Program With Publication of New Rule

By Aaron Charfoos, Scott M. Flicker, Michelle A. Reed, Keith Feigenbaum & Hunter Nagai

I. Introduction

On October 15, 2024, the Department of Defense ("DoD") published the final version of its rule implementing the Cybersecurity Maturity Model Certification ("CMMC") Program under Title 32 of the Code of Federal Regulations (the "Title 32 Rule").[1] The Title 32 Rule updates DoD's national security regulations, while a parallel, proposed ruling under Title 48 aims to update the Federal Acquisition Regulation ("FAR") and Defense Federal Acquisition Regulation Supplement ("DFARS") (the "Title 48 Rule") to impose cybersecurity requirements for nearly all DoD contractors later this year.[2] As these long-awaited rules come to fruition, Defense Industrial Base ("DIB") contractors of all sizes and at all levels (i.e., prime contractor or subcontractor) should assess their current cybersecurity compliance level and consider what will be required to compete for future DoD contracts.

II. Background

DoD initially proposed the Title 32 Rule on December 26, 2023, followed by the proposed Title 48 Rule on August 15, 2024. DoD's finalization of the Title 32 Rule formally establishes the CMMC Program and outlines the security controls based on the CMMC 2.0 framework. The CMMC 2.0 framework, introduced in November 2021, is designed to enhance cybersecurity across the DIB by requiring contractors to meet specific security standards based on the sensitivity of the information they manage. Under the Title 32 Rule, contractors must comply with the requirements for their respective security level and undergo assessments to confirm compliance.[3] The Title 32 Rule also establishes processes and procedures for the assessment and certification of CMMC compliance, and institutes the roles and responsibilities of the federal government, contractors, and third parties involved in the assessment and certification process.[4]

The Title 32 Rule is set to come into effect on December 16, 2024. Since the rule is considered a major rule, it will be subject to a Congressional review period of up to 60 days prior to becoming finalized into law. Prior to the rule's implementation, the Title 48 Rule will need to be finalized[5] and the Cyber AB[6]—the CMMC accreditation body—is expected to release its Compliance Assessment Guidelines for CMMC assessors.

III. Overview of the Title 32 Rule

The Title 32 Rule largely maintains the CMMC Program's original structure but includes several important clarifications regarding its applicability, as well as an adjusted timeline for implementation. A table outlining the three-level CMMC 2.0 framework for assessment has now been codified in the Rule's Preamble[7]:

TABLE 1—CMMC LEVEL AND ASSESSMENT REQUIREMENTS

CMMC status	Source & number of security reqts.	Assessment reqts.	Plan of action & milestones (POA&M) reqts.	Affirmation reqts.
Level 1 (Self) ...	• 15 required by FAR clause 52.204–21.	• Conducted by Organization Seeking Assessment (OSA) annually. • Results entered into SPRS (or its successor capability).	• Not permitted	• After each assessment. • Entered into SPRS.
Level 2 (Self) ...	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by OSA every 3 years ..... • Results entered into SPRS (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).
Level 2 (C3PAO).	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by C3PAO every 3 years ..... • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).
Level 3 (DIBCAC).	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012. • 24 selected from NIST SP 800–172 Feb2021, as detailed in table 1 to § 170.14(c)(4).	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment. • Conducted by Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every 3 years. • Results entered into CMMC eMASS (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Level 2 (C3PAO) affirmation must also continue to be completed annually. • Entered into SPRS (or its successor capability).

A. APPLICABILITY

CMMC certification is a condition of contract award for all applicable DoD contractors and applies equally to both U.S. and non-U.S. contractors.[8] In addition to the requirements outlined in the table above, the Title 32 Rule provides a number of key clarifications as to the applicability of these requirements:

- **Annual Affirmations**. Contractors at all levels will be required to file annual affirmations from an "Affirming Official" of their continued compliance with CMMC requirements.[9] The Title 32 Rule adds a definition for "Affirming Official" to clarify that the individual is a senior-level representative "responsible for ensuring the [company's] compliance with the CMMC Program requirements and has the authority to affirm the [company's] continuing compliance with the specified security requirements for their respective organizations."[10]

- **Subcontractor Flow-Down**. CMMC certification requirements will flow down at all levels to subcontractors who process, store, or transmit federal contract information ("FCI") or controlled unclassified information ("CUI").[11] The Title 32 Rule clarifies that subcontractors who only process, store, or transmit FCI (and not CUI) have Level 1 status, even if the prime contractor has a higher status.[12] Furthermore, when a prime contractor has Level 3 status, its subcontractors who process, store, or transmit CUI are subject to Level 2 (C3PAO) assessment.[13]

- **External Service Providers ("ESPs")**. Title 32 Rule clarifies that CMMC certification is no longer required for ESPs and are instead included within the contractor's assessment scope.[14] Thus, contractors must identify the information systems, including systems or services provided by ESPs that process, store, or transmit FCI (for Level 1 status) or CUI (for all other levels).[15] Additionally, ESPs that are not Cloud Service Providers are no longer required to meet CMMC requirements.[16]

B. ADJUSTED IMPLEMENTATION TIMELINE

Another important aspect of the Title 32 Rule is the adjusted timeline for CMMC implementation. Particularly, Phase 1 of the CMMC's implementation has been extended by six months, while the rollout of each subsequent phase remains consistent with the rule's proposed version.[17] The updated timeline is as follows:

- **Phase 1** begins the effective date of the Title 48 Rule, requiring Level 1 or Level 2 (self-assessment) for contract awards.[18] Under this phase, DoD may impose Level 1 or 2 self-assessment criteria as a condition for exercising an option period on a contract awarded prior to the effective date of the CMMC Program.[19] Moreover, DoD has discretion in Phase 1 to impose Level 2 C3PAO requirements on applicable solicitations and contracts.[20]

- **Phase 2** begins one year after the start of Phase 1 and introduces Level 2 (C3PAO) assessment requirements for new contracts.[21]

- **Phase 3** begins one year after the start of Phase 2 and requires Level 2 (C3PAO) assessment for option year awards and contract renewals, as well as Level 3 (DIBCAC) assessment for new contracts.[22]

- **Phase 4** begins one year after the start of Phase 3 and implements CMMC Program requirements for all new contracts and option year awards.[23]

IV. Conclusion

With the Title 32 Rule in place, DoD contractors should begin preparing for the phased rollout, which will commence upon entry into effect of the Title 48 Rule. Mapping controls and collecting documentation with respect to FCI and CUI, as well as identifying and addressing any compliance gaps internally and across the supply chain, will require considerable time and resources. DoD contractors should review their current contracts to ensure continued compliance with cybersecurity requirements and prepare for CMMC requirements that will be incorporated into option periods, contract extensions, and new contracts.

Our Data Privacy and Cybersecurity practice regularly advises on compliance with CMMC and other cybersecurity regulations. If you have any questions concerning how these requirements may affect your organization, please do not hesitate to contact the members of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Dallas

Michelle A. Reed
1.972.936.7475
michellereed@paulhastings.com

Washington D.C.

Scott M. Flicker
1.202.551.1726
scottflicker@paulhastings.com

Hunter Nagai
1.202.551.1968
hunternagai@paulhastings.com

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Keith Feigenbaum
1.202.551.1929
keithfeigenbaum@paulhastings.com

---

[1] Cybersecurity Maturity Model Certification (CMMC) Program, 32 C.F.R. pt. 170 (2024), available at https://www.govinfo.gov/content/pkg/FR-2024-10-15/pdf/2024-22905.pdf.

[2] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), Docket DARS-2020-0034 (proposed Aug.15, 2024) (to be codified at 48 CFR Parts 204, 212, 217, and 252), available at https://www.govinfo.gov/content/pkg/FR-2024-08-15/pdf/2024-18110.pdf.

[3] *See* 32 C.F.R. § 170.14.

[4] *See generally*, 32 C.F.R. Part 170 (2024).

[5] Among other things, the proposed Title 48 Rule includes a new DFARS provision, 252.204-7YYY, "Notice of Cybersecurity Maturity Model Certification Level Requirements." This provision requires notice to contractors of the CMMC level required by the solicitation and of the proof of compliance required to be submitted in the Supplier Performance Risk System ("SPRS"). The provision requires: (1) offerors to post CMMC Level 1 and 2 self-assessments in SPRS, (2) third-party assessment organizations to post Level 2 certificate assessments in SPRS, and (3) the DoD assessor to post the Level 3 certificate in SPRS.

[6] Cyber AB, https://cyberab.org/About-Us/Overview.

[7] 32 C.F.R. Part 170.

[8] *Id.*

[9] 32 C.F.R. § 170.22(a)(2)(ii).

[10] 32 C.F.R. § 170.4(b).

[11] 32 C.F.R. § 170.23

[12] *Id.*

[13] *Id.*

[14] *See* 32 C.F.R. § 170.16(c)(2) and (3); 32 C.F.R. § 170.17(c)(5) and (6); 32 C.F.R. § 170.18(c)(5) and (6).

[15] 32 C.F.R. § 170.19.

[16] *See* 32 C.F.R. § 170.16(c)(2) and (3); 32 C.F.R. § 170.17(c)(5) and (6); 32 C.F.R. § 170.18(c)(5) and (6).

[17] 32 C.F.R. § 170.3(e).

[18] 32 C.F.R. § 170.3(e)(1).

[19] *Id.*

[20] *Id.*

[21] 32 C.F.R. § 170.3(e)(2).

[22] 32 C.F.R. § 170.3(e)(3).

[23] 32 C.F.R. § 170.3(e)(4).