Note: CMMC is still going through the rule-making process and certain aspects and requirements may change. Refer to the *Resources Guide* provided in this training for the most updated information.

Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Supply Chain Cyber Training

Cyber/Cybersecurity Maturity Model Certification (CMMC) v2.0

CMMC Proposed Rule 32 CFR 170 Supplemental Slides

CyberAssist

Initial Summary of CMMC Proposed Rule 32 CFR 170

CMMC Program Rule Focus/Purpose: Formally establishing DCMA DIBCAC Role/Responsibilities and Cyber AB Ecosystem with High-Level Planning

- Comments were due 26 Feb 2024 (Public Inspection 22 Dec, Officially in Federal Register 26 Dec 2023)

32 CFR 170 Defense Contracting | Title: Cybersecurity Maturity Model Certification (CMMC) Program

- 230+ pages, 70+ regulatory language (*initial summary on regulatory language only; does not include supplement/discussion*)
- 4 Subparts: i) General Info, ii) Govt Roles & Responsibilities, iii) CMMC Ecosystem, & iv) CMMC Key Elements
- 24 Subordinate Parts designated as 32 CFR 170.01 – 170.24 and Appendix A with URLs for Assessment and Scoping Guides
- **Not DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements or DFARS implementation**

- Describes the DoD CMMC Program and establishes **policy for FCI and CUI safeguarding & compliance**
  - Standards as set forth in FAR 52.204-21 and NIST 800-171 Rev 2, and for CMMC Level 3 only select requirements from NIST 800-172/ODPs
  - Establishes Requirements for CMMC Self Assessments/Certifications for Organizations w/Company Affirmation & Scoping Criteria
    - Information on Scoring, POA&M Conditions, & Subcontractor Compliance
    - Of interest includes Joint Surveillance limited acceptance & process for FedRAMP Moderate Equivalency

Source: Cybersecurity Maturity Model Certification Model Certification Program, A Proposed Rule by Department of Defense | December 26, 2023, https://www.federalregister.gov/d/2023-27280

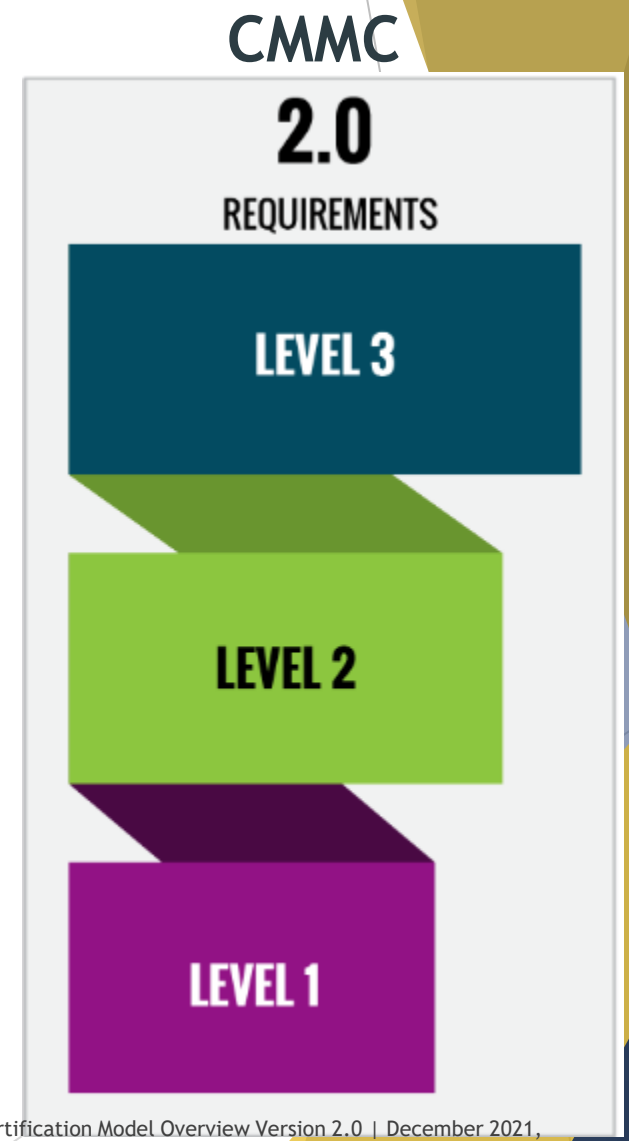
Initial Summary of CMMC Proposed Rule 32 CFR 170

CMMC Level 1 New or Partially New Requirements

- Self-assessment using NIST SP 800-171A against "basic safeguarding" requirements of FAR clause 52.204-21 (15 FAR / 17 NIST SP 800-171 requirements) annually (Partially New)
- Report implementation status in the DoD's Supplier Performance Risk System (SPRS) (New)
- Affirmation by organization senior official of continuing compliance with the security requirements annually (New)

CMMC Level 2 New or Partially New Requirements

- Requires affirmation after every assessment, including POAM closeout (New)
- Requires affirmation annually by senior organization official (New)
  - Affirming official: OSA senior official who is responsible for ensuring OSA compliance with CMMC Program requirements
- POAMs are allowed for selected requirements but must be closed out and verified (by 3rd party) within 180 days (New)
- Has scoping specifics for different asset types (New)



Source: Cybersecurity Maturity Model Certification Model Certification Program, A Proposed Rule by Department of Defense | December 26, 2023, https://www.federalregister.gov/d/2023-27280

Image source: Cybersecurity Maturity Model Certification Model Overview Version 2.0 | December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

CyberAssist

CMMC Proposed Rule Summary

	Self-Assessment		Certification Assessment	
	Level 1	**Level 2**	**Level 2**	**Level 3***
Requirements	15 Requirements in FAR clause 52.204-21	110 Requirement in NIST SP 800-171 rev 2	110 Requirement in NIST SP 800-171 rev 2	24 tailored requirements from NIST SP 800-172
Scoring[1]	All requirements must be fully implemented	"Fully implemented" requirements worth either 5, 3 or 1 point	"Fully implemented" requirements worth either 5, 3 or 1 point	"Fully implemented" requirements worth 1 point
Procedure	Verify 59 objectives via NIST SP 800-171A. Fully implemented: All objectives MET. No Open Items. "Final Self Assessment.	Verify 320 objectives via SP 800-171A. Fully Implemented: All objectives MET[2] No open items result in: "Final Self-Assessment"	Verify 320 objectives via SP 800-171A. Fully Implemented: All objectives MET[2] No open items result in: "Final Certification Assessment"	Verify 103 objectives via SP 800-172A. Fully Implemented: All objectives MET[2] No open items result in: "Final Certification Assessment"
POAMs	No POAMs allowed	Permissible open items[3] "Conditional Self-Assessment" 180 days to close via self-assessment	Permissible open items[3] "Conditional Certification Assessment" 180 days to close via C3PAO	Permissible open items[3] "Conditional Certification Assessment" 180 days to close via DIBCAC
Assessment	Annual Results submitted to SPRS	Triennial (every 3 years) Results submitted to SPRS	Triennial (every 3 years) via C3PAO Results submitted to eMASS	Triennial (every 3 years) via DIBCAC Results submitted to eMASS
Affirmation	At each assessment and annually via senior company official	At each assessment and annually via senior company official	At each assessment and annually via senior company official	At each assessment and annually via senior company official
Scoping[4]	Set boundary but "consider" External Service Providers (ESP) during assessment	Set boundary. ESPs must have L2 Final Cert. CUI Assets and Security Assets must meet all requirements. Risk Managed, Specialized assets in diagrams, SSP, and inventory. Out of Scope assets have no requirements but must be proven.	Set boundary. ESPs must have L2 Final Cert. CUI Assets and Security Assets must meet all requirements. Risk Managed (may be assessed), Specialized assets in diagrams, SSP, and inventory. Out of Scope assets have no requirements but must be proven.	Set boundary. ESPs must have L2 Final Cert. All Assets in scope. Out of Scope assets have no requirements but must be proven.

*Prerequisite: CMMC L2 Final Certification
1) See 170.24 for scoring details
2) See 170.16-170.18 for criteria
3) See 170.21 for restrictions
4) See 170.19

Source: Cybersecurity Maturity Model Certification Model Certification Program, A Proposed Rule by Department of Defense | December 26, 2023, https://www.federalregister.gov/d/2023-27280

Proposed Timelines and Phases (170.3)

- DoD "intends to include CMMC requirements for Levels 1, 2, and 3 in all solicitations issued on or after October 1, 2026, when warranted by any FCI or CUI information protection requirements"
  - Before Oct 1, 2026, DoD Program Managers will have discretion to include CMMC requirements
- Phase 1
  - Immediately upon "the effective date of the DFARS rule that will implement CMMC Requirements"
  - Self-assessment only "when warranted by the FCI and CUI categories associated with the planned effort"
- Phase 2
  - Six (6) months after start of Phase 1
  - In addition to Phase 1 requirements, DoD intends to include the CMMC Level 2 Certification Assessment requirement in all applicable DoD solicitations and contracts **as a condition of contract award**
- Phase 3
  - One (1) Calendar Year after start of Phase 2
  - In addition to Phase 1 and 2 requirements, DoD intends to include the CMMC Level 2 Certification Assessment requirement in all applicable DoD solicitations and contracts **as a condition of contract award and as a condition to exercise an option period** on a contract awarded prior to the effective date
  - DoD intends to include the CMMC Level 3 Certification Assessment requirement in all **applicable** DoD solicitations and contracts as a condition of contract award
- Phase 4
  - One (1) Calendar Year after start of Phase 2
  - All solicitations include CMMC requirements

Source: Cybersecurity Maturity Model Certification Model Certification Program, A Proposed Rule by Department of Defense | December 26, 2023, https://www.federalregister.gov/d/2023-27280

CMMC Proposed Rule 32 CFR 170 Resources

- CMMC 32CFR Proposed Rule
  - Overview page: https://www.federalregister.gov/d/2023-27280
  - PDF: https://public-inspection.federalregister.gov/2023-27280.pdf
- CMMC Guidance docs
  - Overview page: https://www.federalregister.gov/d/2023-27281
  - PDF: https://public-inspection.federalregister.gov/2023-27281.pdf
- Department of Defense CMMC Proposed Rule Informational Video, February 2024, https://www.defense.gov/News/News-Stories/Article/Article/3678476/defense-department-releases-companion-video-for-cmmc-public-comment-period/