32 CFR Part 170: CMMC Final Rule

Examining the Final CMMC Rule and its Impact on the A/E/C Industry

November 5, 2024, 3:00 p.m.

SBC
FEDERAL SMALL BUSINESS CONFERENCE
FOR THE A/E/C INDUSTRY

2024 FEDERAL SMALL BUSINESS CONFERENCE

STRENGTH in Partnership

SAME SAMESBC.ORG

MODERATOR

Laura Rodgers

NC State University

Director, Cybersecurity Practice

Fun Facts

- I climbed five 14,000+ foot mountains when I lived in Colorado. (We called them 14ers)
- I love whitewater rafting
- I started a book club via Zoom with my cousins during COVID.

HOUSEKEEPING ITEMS

Those connecting through a VPN will likely have difficulties. Please, ditch the VPN!

“Upvote” questions already asked that you want to hear the answer to as well!

Click on the “Handouts” tab to download a copy of the presentation slides.

This webinar is being recorded for future viewing.

What is your role in the defense ecosystem?

- Government
- Subject to CMMC certification
- Supporting the DIB

2024 FEDERAL SMALL BUSINESS CONFERENCE

STRENGTH in Partnership

SAMESBC.ORG

SPEAKER

Lori Jackson

White Raven Security

President

Fun Facts

- I use crocheting to reduce stress
- I've read 23 books so far this year
- SBC will be my first time visiting New Orleans!!

32 CFR Part 170 [Docket ID: DoD-2023-OS-0063]

- Published October 15, 2024
- Effective December 16, 2024
- Program implementation timing depends on Title 48 CFR
  - Parts 204, 212, 217, and 252 [Docket DARS-2020-0034]
- 470 Pages (double-spaced version)
  - Responses to Comments (p. 1)
  - Regulatory Details (p. 263)
  - Actual Rule (p. 384)

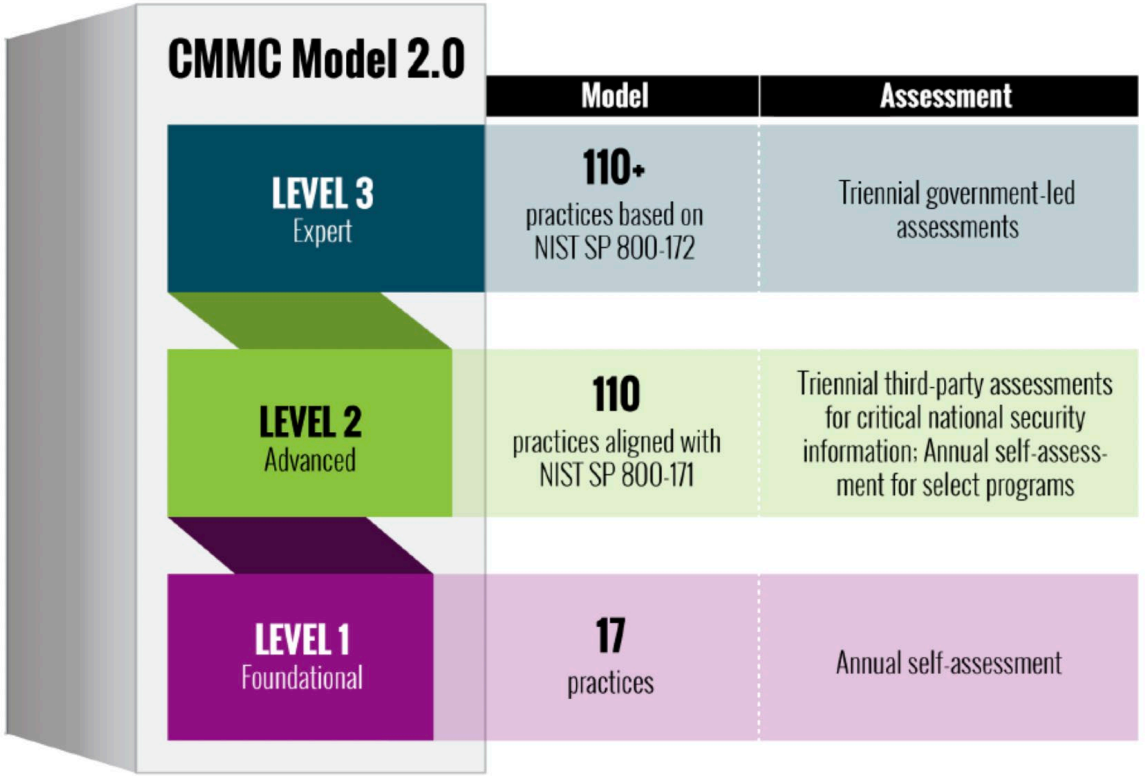
Final Rule: https://www.govinfo.gov/content/pkg/FR-2024-10-15/pdf/2024-22905.pdf
Double-spaced version: https://public-inspection.federalregister.gov/2024-22905.pdf

Where are you on your CMMC journey?

- We’re ready for a third-party assessment
- We've entered our score in the SPRS
- We’re just getting started
- What is CMMC again?

Cybersecurity Maturity Model Certification

- Three-level tier framework
  - Level 1 – Foundational
  - Level 2 – Advanced
  - Level 3 – Expert
- *Most* contractors will need to be certified by a third-party assessor in order to work on any DoD contract.



CMMC Level 1 Self-Assessment

- Federal Contract Information (FCI)
- FAR 52.204-21
- Timing:
  - Self-assessment annually
  - SPRS affirmation submitted annually
- Fully implement all 15 FAR requirements (17 security controls)
- No PoAMs are permitted – all controls must be MET in their entirety

CMMC Level 2 Self-Assessment

- Controlled Unclassified Information (CUI)
- DFARS 252.204-7012
- Timing:
  - Self-assessment every three years
  - SPRS affirmation submitted annually
- Fully implement 110 security controls (NIST SP 800-171)
- PoAMs allowed (next slide)

Plan of Action and Milestones (PoA&M)

- PoAMs are allowed if:
  - Total score of at least 88 (80% implementation)
- No security controls valued higher than 1 point (exception: SC.L2-3.13.11)
- These security controls must be MET:
  - AC.L2-3.1.20 - External Connections (CUI Data)
  - AC.L2-3.1.22 - Control Public Information (CUI Data)
  - CA.L2-3.12.4 - System Security Plan
  - PE.L2-3.10.3 - Escort Visitors (CUI Data)
  - PE.L2-3.10.4 - Physical Access Logs (CUI Data)
  - PE.L2-3.10.5 - Manage Physical Access (CUI Data)
- Open PoAMs must be closed within 180 days

CMMC Level 2 Certification Assessment

- Controlled Unclassified Information (CUI)
- DFARS 252.204-7012
- Timing:
  - Third-party assessment every three years
  - SPRS affirmation submitted annually
- Fully implement 110 security controls (NIST SP 800-171)
- Third-party assessment by a C3PAO
- Allowed PoAMs following the same parameters as Level 2 (self), but must be confirmed completed by C3PAO

CMMC Level 3 Certification Assessment

- Controlled Unclassified Information (CUI)
- Timing:
  - Third-party assessment every three years
  - DIBCAC assessment every three years
  - Level 2 and Level 3 affirmations annually
- CMMC Level 2 Certification Assessment (C3PAO)
- CMMC Level 3 Certification Assessment (DIBCAC)
  - 24 additional security controls (NIST SP 800-172)
- PoAMs allowed (next slide), but must be confirmed completed by DIBCAC

PoA&Ms at Level 3

- PoAMs are allowed if:
  - Total score (Level 3) demonstrating 80% implementation
- These security controls must be MET:
  - IR.L3-3.6.1e Security Operations Center
  - IR.L3-3.6.2e Cyber Incident Response Team
  - RA.L3-3.11.1e Threat-Informed Risk Assessment
  - RA.L3-3.11.6e Supply Chain Risk Response
  - RA.L3-3.11.7e Supply Chain Risk Plan
  - RA.L3-3.11.4e Security Solution Rationale
  - SI.L3-3.14.3e Specialized Asset Security
- Open PoAMs must be closed within 180 days

Key Takeaways – Timeline

- Effective Date: 16 December 2024
  - C3PAOs may begin conducting third-party assessments
- Effective with 48 CFR (~March 1, 2025)
  - Phase 1 – Level 1 (Self), Level 2 (Self)
  - Phase 2 – Adds Level 2 (C3PAO)
  - Phase 3 – Adds Level 3 (DIBCAC)
  - Phase 4 – Full Implementation

Key Takeaways – Scoping

- Contractor Risk Managed Assets (CRMA) *should be prepared to be assessed* against CMMC security requirements at Level 2, and included in the SSP, asset inventory, and network diagrams.
  - If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies.
- Out-of-Scope Assets cannot process, store, or transmit CUI; and *do not provide security protections for CUI Assets.*
  - Prepare to justify the inability of an Out-of-Scope Asset to process, store, or transmit CUI.

Key Takeaways – External Service Providers

- If an OSA utilizes an ESP, including a Cloud Service Provider (CSP), that does not process, store, or transmit CUI, the ESP does not require its own CMMC assessment. The services provided by the ESP are assessed as part of the OSC's assessment as Security Protection Assets.
- ESP services and responsibilities need to be documented in the OSA's SSP, service descriptions, and customer responsibility matrix (CRM).
- Any CSP used by the contractor to handle CUI must meet Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline or the equivalent requirements defined in DoD Policy.

Recommendations for AEC

- Determine the approximate level you can expect. Look for DFARS 252.204-7012 in your existing contracts or subcontract agreements.
- Avoid CUI, if possible. Otherwise, consider an enclave (narrow the scope).
- Thoroughly define the scope of where FCI/CUI resides within the system.
- Examine your supply chain – if subconsultants will handle CUI, a flow-down is necessary. They must meet the same CMMC-level contract requirement as the Prime.
- Determine *all* the devices that are connected to your network/enclave, as well as software installed. Remember that any device that you don't control should not contain company or government data, especially CUI (this includes personal devices).
- Documentation is the first thing an assessor will ask for. Be sure you can follow your own documentation. Make employees aware of the documents/rules that pertain to them (they will be interviewed).

Resources

- 32 CFR CMMC Rule: https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program
- 48 CFR Proposed Rule: https://www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
- CMMC Resources: https://dodcio.defense.gov/cmmc/Resources-Documentation/
- Controlled Unclassified Information (CUI): https://www.dodcui.mil/

Lori Jackson, CISSP, CCA
lori@whiteravensecurity.com
704-806-8089

Terminology (CMMC-custom terms)

- *CMMC Third-Party Assessment Organization (C3PAO)* - organizations that are responsible for conducting Level 2 certification assessments and issuing Certificates of CMMC Status to OSCs based on the results.
- *Organization Seeking Assessment (OSA)* - the entity seeking to undergo a self-assessment or certification assessment for a given information system for the purposes of achieving and maintaining any CMMC Status. The term OSA includes all Organizations Seeking Certification (OSCs).
- *Organization Seeking Certification (OSC)* - the entity seeking to undergo a certification assessment for a given information system for the purposes of achieving and maintaining the CMMC Status of Level 2 (C3PAO) or Level 3 (DIBCAC). An OSC is also an OSA.

Terminology (cont'd)

- *Contractor Risk Managed Assets (CRMA)* – Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place. Assets are not required to be physically or logically separated from CUI assets.
- *Supplier Performance Risk System (SPRS)* – CMMC assessment results and contractor affirmations of compliance will be posted in SPRS, DoD's authoritative source for supplier and product performance information.
- *Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)* – a part of DCMA, DIBCAC assesses DIB companies to ensure they are meeting contractually required cybersecurity standards and to ensure contractors have the ability to protect CUI for government contracts they are awarded.

Terminology (cont'd)

- *External Service Provider (ESP)* - external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (*e.g.*, log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.
- *Cloud Service Provider (CSP)* - an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Terminology (cont'd)

- *Affirming Official* – the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations.