White Raven SECURITY

Understanding the Final CMMC Rule

Companies that support the U.S. Department of Defense should note how the various Cybersecurity Maturity Model Certification (CMMC) rules will affect their business. All companies within the Defense Industrial Base (DIB) will need to meet CMMC at various levels, beginning in 2025.

RECOMMENDATIONS FOR AEC

To prepare for compliance, begin by determining the CMMC level you can expect. If DFARS 252.204-7012 appears in your existing contracts, expect to focus on reaching CMMC Level 2. Clearly define where Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) reside within your systems to establish clear scope boundaries. Try to avoid handling CUI, if possible; otherwise, consider creating an enclave to store CUI. Review your supply chain to ensure that any subcontractors handling CUI adhere to the same requirements. Documentation is critical; assessors will prioritize it, so ensure that you have, and can follow, robust security policies and procedures.

UNDERSTANDING THE REGULATIONS

32 CFR Part 170

- Officially establishes and defines the CMMC Program
- Released October 15, 2024, effective December 16, 2024
- Outlines a phased implementation

48 CFR Parts 204, 212, 217, and 252

- DoD will assign a CMMC Level to each contract
- Closed to public comments on October 15, 2024
- Expected release by the end of Q2 2025 (3/1/2025)
- Kicks off the phased CMMC implementation

PHASED IMPLEMENTATION*

1
- Trigger: 48 CFR release
- Level 1 (self), Level 2 (self)

2
- One year following Phase 1
- Adds Level 2 (C3PAO)

3
- One year following Phase 2
- Adds Level 3 (DIBCAC)

4
- One year following Phase 3
- CMMC in every contract

** DoD has the discretion to add any CMMC level to any contract beginning in Phase 1*

CMMC LEVELS

Level 1 (Self) - Foundational

- All 15 requirements in FAR 52.204-21 are met
- Implemented during Phase 1
- Annual affirmation by a senior official
- No POA&Ms are permitted

Level 2 (Self) - Advanced

- All 110 controls in NIST SP 800-171 are met
- Implemented during Phase 1
- Self-assessment every three years
- Annual affirmation by a senior official
- POA&Ms permitted with a base score of 88, and 180 days to complete

Level 2 (C3PAO) - Advanced

- All 110 controls in NIST SP 800-171 are met
- Third-party assessment and certification
- Implemented during Phase 2
- Renew certification every three years
- Annual affirmation by senior official
- POA&Ms permitted with a base score of 88, and 180 days to complete

Level 3 (DIBCAC) - Expert

- Prerequisite: Meet Level 2 (C3PAO)
- All 24 controls in NIST SP 800-172 are met
- Assessment and certification by DIBCAC
- Renew certification every three years
- Annual affirmation by senior official

NEED SUPPORT?

980-277-1131

www.whiteravensecurity.com