guernsey
ENGINEERS
ARCHITECTS
CONSULTANTS

CMMC 2.0 in Action

What You Need to Know, Do, and Avoid

MATT WATSON CISSP, CCA

CYBERSECURITY CONSULTANT

ROAD TO CMMC

- DFARS 252.204-7012:
  - Requirement to implement NIST 800-171
  - Security requirements for cloud services storing CUI
  - Cyber incident reporting requirements
- DFARS 252.204-7019 & 7020:
  - Self-assess compliance with 800-171
  - Submit assessment score to SPRS (update within 3 years)
  - You must have a plan and timeline to become compliant
  - Defines assessment types – Low (self), Medium, & High
  - DoD Authority to assess company for Med/High assessments
- DFARS 252.204-7021 (PENDING FINAL RULE):
  - DoD will specify the required CMMC Level in each solicitations and the resulting contract.
  - Many prime contractors are requesting their subs work toward Level 2 Certification.
  - Final contact language pending, expected in October

ONE PROGRAM – TWO RULES

32 CFR Rule – Details of CMMC Program

- Became Effective 12/16/2024
- C3PAO Assessments began 01/02/2025
- Self-Assessments in SPRS began 02/28/2025
- Recent DoD counts on program activity:
  - ~ 3800 Level 1 Self-Assessments
  - ~ 850 Level 2 Self-Assessments
  - ~ 260 Level 2 C3PAO Assessments Completed

ONE PROGRAM – TWO RULES

48 CFR Rule – Details for DFARS Clause

- Draft published on 8/15/2024
- Now in final step of rulemaking
- Likely to be published in 60-90 days.
- DoD estimates the rule to be effective in December 2025 (if not sooner).

CMMC PROGRAM ROLL-OUT

DoD has defined a four-phase rollout

- Phase 1 – Begins on the effective date of the CMMC revision to DFARS 252.204-7021 (48 CFR rule)
- Estimated late Q4 2025
- Intend to include CMMC Level 1 or Level 2 Self-Assessment for all applicable DoD solicitations and contracts as a condition of award.
- *At DoD discretion, can include Self-Assessments as a condition to exercise an option period and/or can also choose to include Level 2 Certification in place of Self-Assessment.

CMMC PROGRAM ROLL-OUT

DoD has defined a four-phase rollout

- Phase 2 – Begins 1 year after the start of phase 1
- Estimated Q4 2026
- In addition to phase 1 requirements, Intend to include CMMC Level 2 Certification Assessment for all applicable DoD solicitations and contracts as a condition of award.
- *At DoD discretion, can delay the inclusion of Level 2 Certification Assessment to an option period instead of as a condition of award. Can also include Level 3 Certification Assessment for applicable solicitations and contracts.

CMMC PROGRAM ROLL-OUT

DoD has defined a four-phase rollout

- Phase 3 – Begins one year after the start of phase 2
- Estimated Q4 2027
- In addition to phase 1 & 2 requirements, intend to include CMMC Level 2 Certification Assessment for all applicable DoD solicitations, contracts, and to exercise an option period as a condition of award. Also intend to include Level 3 Certification Assessment for all applicable solicitations and contracts.
- *At DoD discretion, can delay the inclusion of Level 3 Certification Assessment to an option period instead of as a condition of award.

CMMC PROGRAM ROLL-OUT

DoD has defined a four-phase rollout

- Phase 4 – Begins one year after the start of phase 3
- Estimated Q4 2028
- Full Implementation
- DoD will include CMMC Program requirements in all applicable solicitations and contracts, including option periods on contracts awarded prior to phase 4.

DoD ASSESSMENT ESTIMATES BY YEAR

All Entities

Year	Triennial Level 1 Self Assessment	Triennial Level 2 Self Assessment	Triennial Level 2 3rd Party Assessment	Triennial Level 3 Assessment
1	945	27	517	4
2	4,720	136	2,599	50
3	15,748	453	8,666	169
4	30,184	894	17,127	327
5	30,179	1,003	19,205	373
6	30,179	1,320	25,272	492
7	27,246	1,677	32,121	622

KEY POINTS

- Level 2 Self-Assessments must follow the same CMMC program rules as a C3PAO assessment.
- Many primes are already asking and encouraging subs to be Level 2 compliant.
- Any cloud solution used to handle CUI must be FedRAMP authorized at a moderate level or equivalent.
- There is no technical solution that will meet 100% of CMMC requirements for you.
- Outsourced IT/Security resources will need to involved in your assessment.

Matt Watson, CISSP, CCA

5555 North Grand Boulevard
Oklahoma City, OK 73112-5507
405.416.8185
matthew.watson@guernsey.us
cybersecurity@guernsey.us
guernsey.us

guernsey

REALIZE THE DIFFERENCE