CHECKLIST · UPDATED OCTOBER 2026

CMMC 2.0 readiness checklist

Jay Nichols
jaynichols.net · jay@jaynichols.net

Update. Status check (October 2026): on July 13, 2026 the Department of War suspended CMMC Phase 2, which had been scheduled for November 10, 2026, and started a review of the program. Phase 1 self-assessment requirements remain in place, solicitations may currently require only Level 1 (Self) or Level 2 (Self), and DFARS 252.204-7012 still applies.

1 · Applicability and level

- [ ] **Confirm what information you handle**
  Federal Contract Information (FCI) points to Level 1; Controlled Unclassified Information (CUI) points to Level 2 or higher. Check contract documents and markings, and the CUI Registry for categories. [1] [2]

- [ ] **Find the CMMC clause and required status**
  Look for DFARS 252.204-7021 in solicitations and contracts and note the CMMC status it requires: Level 1 (Self), Level 2 (Self), Level 2 (C3PAO) or Level 3 (DIBCAC). [3] [4]

- [ ] **Track the current implementation phase**
  Phase 1 began November 10, 2025. Phase 2 (planned for November 10, 2026) is suspended pending a DoW review, so check the DoW CIO page before planning around C3PAO dates. [5] [1]

- [ ] **Map your flow-down obligations**
  Primes must flow the CMMC requirement to subcontractors that will process, store or transmit FCI or CUI, at the level appropriate to the information flowed down. [3]

2 · Scope

- [ ] **Inventory assets by CMMC category**
  Classify assets as CUI assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets or Out-of-Scope assets. Specialized Assets explicitly include OT, IoT/IIoT, government property, restricted information systems and test equipment. [6]

- [ ] **Draw the boundary (consider an enclave)**
  Document where CUI flows and consider isolating it into an enclave to shrink the assessment scope. Keep a current network diagram. [6] [7]

- [ ] **List external and cloud service providers**
  Identify every ESP and CSP that touches CUI or security functions. Cloud services that store, process or transmit CUI must meet the FedRAMP Moderate baseline or equivalent. [8] [1] [9]

3 · Implement and document

- [ ] **Level 1: the 15 basic safeguarding requirements**
  Implement the requirements in FAR 52.204-21 for systems that hold FCI. POA&Ms are not permitted at Level 1. [10] [11]

- [ ] **Level 2: the 110 NIST SP 800-171 Rev 2 requirements**
  CMMC Level 2 is aligned to NIST SP 800-171 Rev 2. Rev 3 (97 requirements) is published, but DoD Class Deviation 2024-O0013 keeps DFARS 252.204-7012 contractors on Rev 2 for now. [12] [13] [14]
- [ ] **Write and maintain the System Security Plan**
  The SSP describes the boundary, environment and how each requirement is met. It is one of the requirements that can never be placed on a POA&M. [12] [11]
- [ ] **Self-check against the assessment objectives**
  Use NIST SP 800-171A objectives and the DoW CMMC assessment guide to test each requirement the way an assessor would, and keep the evidence. [15] [7]
- [ ] **Level 3 only: plan for SP 800-172**
  Level 3 adds 24 enhanced requirements from NIST SP 800-172 and requires a Final Level 2 (C3PAO) status first. [16] [1]

4 · Score, affirm and report

- [ ] **Score with the CMMC methodology**
  Requirements are weighted 1, 3 or 5 points; a perfect Level 2 score is 110. [17]
- [ ] **Know the conditional-status rules**
  A Conditional Level 2 status needs a score of at least 80% (88 of 110), only 1-point items on the POA&M (with a narrow FIPS-encryption exception), none of the excluded requirements, and closeout within 180 days. [11]
- [ ] **Enter results in SPRS**
  Post assessment results in the Supplier Performance Risk System. DFARS 252.204-7019/7020 separately require a current NIST SP 800-171 DoD Assessment score in SPRS. [18] [19]
- [ ] **Affirm, then affirm annually**
  A senior Affirming Official must affirm compliance after each assessment and annually; status lapses if annual affirmation is missed. [20] [5]

5 · Operate

- [ ] **Be ready to report incidents in 72 hours**
  DFARS 252.204-7012 requires reporting cyber incidents to DoD via DIBNet within 72 hours of discovery (a DoD-approved medium assurance certificate is needed) and preserving images and relevant data for at least 90 days. [8] [21]
- [ ] **Re-assess on schedule**
  Level 2 self-assessments are repeated every three years; Level 1 annually. Changes to the boundary or environment should trigger an SSP update. [5] [1]
- [ ] **Do not forget the OT**
  If production lines, test benches or building systems touch CUI, they are Specialized Assets: document them in the inventory, SSP and diagrams, and protect them with OT-appropriate controls (see NIST SP 800-82r3). [6] [22]

Sources

1. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program (eCFR)
   https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
2. DoD CUI Registry
   https://www.dodcui.mil/
3. DFARS 252.204-7021, Contractor Compliance with the CMMC Level Requirements
   https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements.
4. DFARS CMMC final rule (DFARS Case 2019-D041), Federal Register, Sep 10, 2025
   https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
5. DoW CIO, About CMMC (Phase 2 suspension notice, Jul 13, 2026)
   https://dodcio.defense.gov/cmmc/About/
6. 32 CFR 170.19, CMMC scoping (eCFR)
   https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.19
7. DoW CIO, CMMC Resources & Documentation (assessment and scoping guides)
   https://dodcio.defense.gov/cmmc/Resources-Documentation/
8. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
   https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
9. FedRAMP Marketplace
   https://marketplace.fedramp.gov/
10. FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
    https://www.acquisition.gov/far/52.204-21
11. 32 CFR 170.21, Plan of Action and Milestones requirements (eCFR)
    https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.21
12. NIST SP 800-171 Rev. 2, Protecting CUI in Nonfederal Systems
    https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
13. NIST SP 800-171 Rev. 3 (May 2024)
    https://csrc.nist.gov/pubs/sp/800/171/r3/final
14. DFARS Class Deviation 2024-O0013, Revision 1 (NIST SP 800-171 Rev 2 for DFARS 252.204-7012)
    https://www.acq.osd.mil/dpap/policy/policyvault/USA001074-24-DPC.pdf
15. NIST SP 800-171A, Assessing Security Requirements for CUI
    https://csrc.nist.gov/pubs/sp/800/171/a/final
16. NIST SP 800-172, Enhanced Security Requirements for Protecting CUI
    https://csrc.nist.gov/pubs/sp/800/172/final
17. 32 CFR 170.24, CMMC scoring methodology (eCFR)
    https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.24
18. Supplier Performance Risk System (SPRS)
    https://www.sprs.csd.disa.mil/
19. DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
    https://www.acquisition.gov/dfars/252.204-7019-notice-nist-sp-800-171-dod-assessment-requirements.
20. 32 CFR 170.22, Affirmation (eCFR)
    https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.22
21. DIBNet, DoD cyber incident reporting portal
    https://dibnet.dod.mil/
22. NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (Sep 2023)
    https://csrc.nist.gov/pubs/sp/800/82/r3/final

Educational summary, not legal advice. Confirm requirements against the current regulation and your contract. Online version with live links: www.jaynichols.net/resources/cmmc-readiness-checklist/