

CMMC Fundamentals

Understanding the Requirements and Getting Started



Why does CMMC Exist?



Program created by the DoW / DoD to protect CUI and FCI across the DIB.



FCI & CUI = sensitive data that if compromised, can harm national security.



Goal: verify you have implemented contractually obligated cyber requirements in NIST 800-171

- **FCI - Federal Contact Information:**

- Information **not meant** for public release
- Provided by / created for the government in performance of a contract.

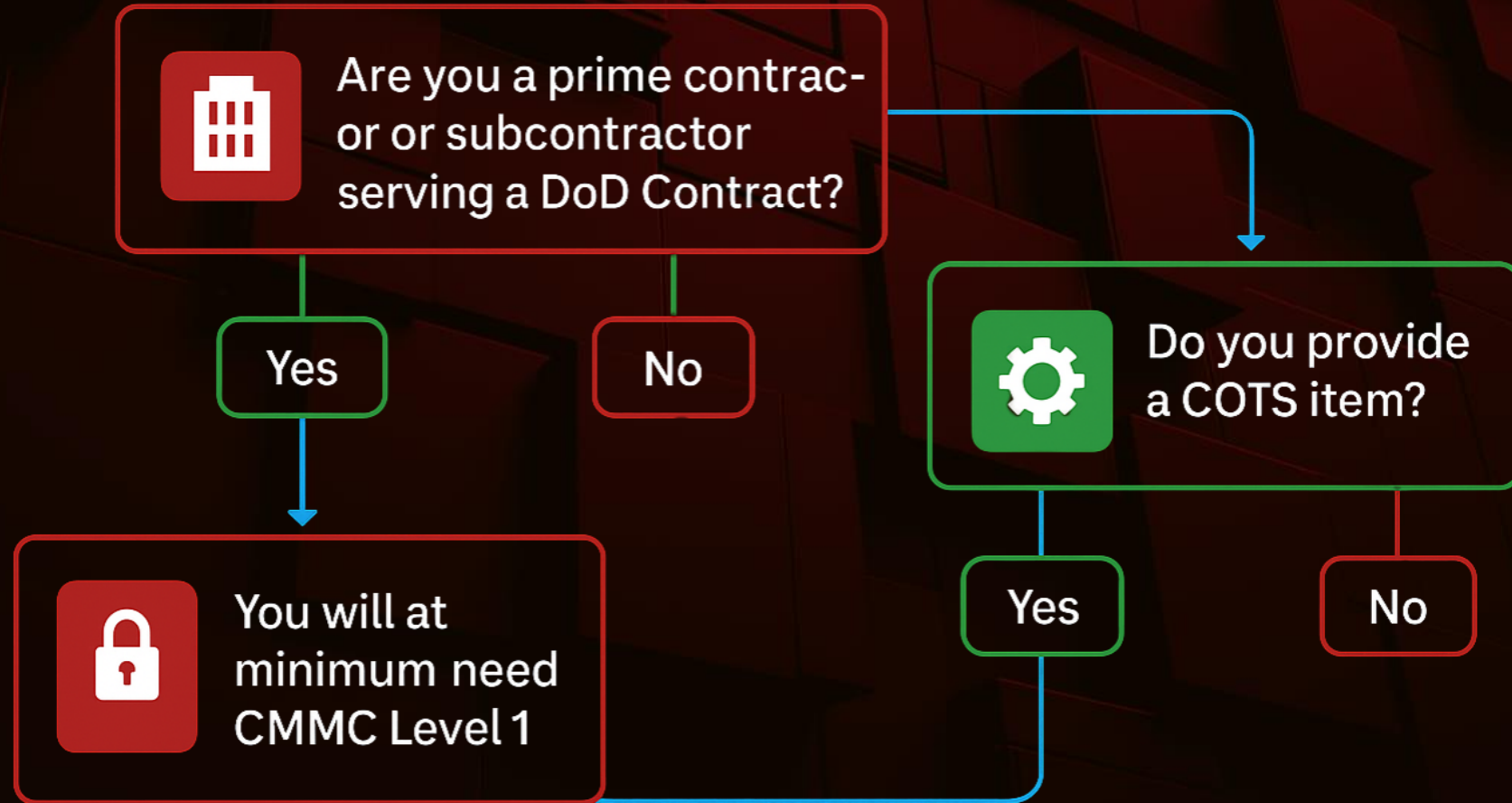
- **CUI - Controlled Unclassified Information:**

- Federal, non-classified information considered critical to national security.
- Provided by / created for the Government in performance of a contract.
- Requires safeguarding & dissemination controls.
- Control marking, not a classification marking.

CMMC Players

- **OSC**: Organization Seeking Certification
- **RPO**: Registered Practitioner Organization
 - **RP**: Registered Practitioner
- **C3PAO**: Certified Third-Party Assessor Organization
 - **CCP**: Certified CMMC Professional
 - **CCA**: Certified CMMC Assessor
- **MSP**: Managed Service Provider
 - **MSSP**: Managed Security Services Provider
 - **CSP**: Cloud Service Provider (FedRAMP Authorized or Equivalent)

CMMC Starting Point



CMMC Levels

LEVEL 1 – Foundational

15 Practices aligned with FAR 52.204-21

- FCI
- Annual self-assessment

LEVEL 2 - Advanced

110 Practices Aligned with NIST SP 800-171 r2

- CUI
- C3PAO assessment every 3 years
- **OR** Self-assessment every 3 years for select programs
- Annual Affirmation

LEVEL 3 - Expert

134 Practices Including:
110 from NIST SP 800-171 r2
+ 24 from 800-172

- DIBCAC assessment every 3 years
- Annual Affirmation
- Select programs handling critical CUI

Where we are today

- Phase 1 begins 11/10/2025, 48 CFR released
- Self-assessments required
- Small number will qualify for S/A only
- Majority of level 2 will need C3PAO
- Warm up for Phase 2

Phase 1

11/10/2025

L1 & L2 Self-Assessment required

May include C3PAO for L2

Phase 2

11/9/2026

L2 3rd Party (C3PAO) certifications required

Phase 3

11/9/2027

L3 Certifications (DIBCAC)

Phase 4

11/9/2028

CMMC Fully Implemented. Required in **all** DoD solicitation and contracts

Clauses in your contract that will trigger CMMC:

- DFARS 252.204-7012: Requires NIST SP 800-171 compliance for protecting CUI.
- DFARS 252.204-7019 / 7020: Requires posting self-assessment scores in SPRS and allows DoD to request evidence.
- DFARS 252.204-7021 / 7025: Requires contractors maintain appropriate CMMC Level, flowdown.

Roles & Responsibilities

Leadership/Executives

- Own compliance, allocate resources, set accountability.
- CMMC is a business obligation, not just an IT job.

IT/Security Teams

- Can help with guiderails, and controls.
- Implement and maintain technical controls, log management, access restrictions, and incident response.

ESP/MSPs

- Provide infrastructure and tooling, but you still retain compliance responsibility (shared responsibility model).

Impact

- Forces coordination across departments, contracts, HR, IT, leadership.

How to Prepare

What Needs to be Included in CUI Boundary

- Determine where CUI lives, how it enters your system and who has access to it.
- Supporting services that may have access.
- Systems, users, data flow, networks, physical locations.

Key Documents

- Key Artifacts:
 - SSP (System Security Plan)
 - P&P (at least one for each control family)
 - Asset Inventory
 - Network Diagram

Total Cost of Compliance

- Readiness
- Assessment
- Continuous monitoring

How do I know I am ready?

- Go through a **Mock Assessment** yourself
 - Answer all **320 objectives**
 - Find / collect your **evidence** and **document** along the way
 - Calculate your **SPRS Score**
 - Each of the 110 NIST 800-171 security controls is assigned a weight of either 1, 3 or 5 points.
 - Scoring starts at the highest possible score of 110.
 - Points are deducted for each control not satisfied, all the way down to -203.
 - Document **deficiencies**
- Have a 3rd party **validate** (C3PAO)

Thank You.



Powered by Aprio[®]