

CMMC Flow-Down Responsibilities

Under DFARS 252.204-7021 (NOV 2025) and 32 CFR Part 170

Prepared for: OSC

Subject: Responsibilities and requirements under DFARS and the CMMC Final Rule for flow-down of cybersecurity requirements

Date: June 2026

Updated: August 2026

Update (July 2026): On July 13, 2026, the Department of War announced a 60-day review that suspends implementation of CMMC Phase 2. This does not repeal the program. 32 CFR Part 170 remains in effect, and safeguarding obligations under FAR 52.204-21, DFARS 252.204-7012, and NIST SP 800-171 remain fully in force. The phase dates below reflect the statutory baseline in 32 CFR 170.3(e); the Phase 2 (C3PAO) start is paused pending the outcome of that review.

Purpose

This document summarizes OSC's responsibilities under DFARS and the CMMC Final Rule for flow-down requirements. Because an OSC may handle both FCI and CUI and serve as a prime contractor on some contracts or a subcontractor on others, the material is organized around both distinctions. The type of information determines WHAT is required; the contract role determines WHO the obligations are owed to. Authoritative source citations appear throughout, with full references in the final section.

1. The Two Governing Authorities

CMMC flow-down obligations come from two complementary rules:

- **32 CFR Part 170 (the CMMC Program Rule).** Effective December 16, 2024. Section 170.23 ("Application to subcontractors") is the core flow-down provision.
- **The DFARS Final Rule (DFARS Case 2024-D025).** Published September 10, 2025; effective November 10, 2025. This rule placed the updated clause DFARS 252.204-7021 (NOV 2025) into contracts and added the solicitation notice provision DFARS 252.204-7025.

The scoping rule that drives everything: per 32 CFR 170.23(a), CMMC requirements apply at all tiers of the supply chain to any contractor or subcontractor that will process, store, or transmit FCI or CUI on its information systems in performance of the contract or subcontract, including subcontracts for commercial products and services. Suppliers that handle no covered information are outside the flow-down.

2. FCI vs. CUI: The Distinction That Drives Everything

Federal Contract Information (FCI)

Definition (FAR 4.1901 / FAR 52.204-21): Information not intended for public release that is provided by or generated for the Government under contract to develop or deliver a product or service. It excludes information the Government releases publicly and simple transactional information, such as payment processing data.

- **Examples:** contract performance reports, proposal responses, emails exchanged with the Government about contract execution, internal schedules tied to a Government deliverable.
- **Baseline obligation:** the 15 basic safeguarding requirements of FAR 52.204-21.
- **CMMC requirement:** Level 1 (Self). Annual self-assessment against those 15 requirements, with results and an affirmation entered in SPRS.

Controlled Unclassified Information (CUI)

Definition (32 CFR 2002.4(h)): Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. In the DoD context, this includes categories such as Controlled Technical Information (CTI), export-controlled data, and other items in the DoD CUI Registry.

- **Examples:** technical drawings and specifications, engineering data, source code for a weapon system component, research data with distribution restrictions. (Actual CUI determination depends on contract identification and the DoD CUI Registry categories.)
- **Baseline obligation:** NIST SP 800-171 (110 security requirements) under DFARS 252.204-7012, plus cyber incident reporting to DoD within 72 hours.
- **CMMC requirement:** Level 2 minimum. The assessment type (Self or C3PAO third-party) depends on the contract, with annual affirmations in SPRS.

CUI Designation and Marking Authority

CUI must be designated by the Government. Contractors have no authority to designate information as CUI on their own (32 CFR Part 2002; DoDI 5200.48 § 3.2.b). The contract, typically via the DD Form 254, CDRLs, SOW, or a CUI attachment, should identify what CUI is involved, and the Government is responsible for marking CUI it provides.

If OSC receives unmarked information it suspects is CUI, do not self-designate. Safeguard it provisionally and request a determination from the Contracting Officer in writing.

Note one exception: when the contract identifies CUI in scope and OSC creates or derives such information in performance, DoDI 5200.48 § 3.6.a requires OSC to apply the appropriate markings at the time of creation. That is executing the Government's designation, not making an independent designation.

Why the Distinction Matters Operationally

Every contract and subcontract should be scoped by asking what information will actually touch which systems. If a workflow involves only FCI, Level 1 obligations attach. The moment CUI enters a system, that system is in Level 2 scope. Many companies segment their environments into a defined CUI enclave precisely to keep Level 2 scope, and assessment cost, contained.

3. Responsibilities When OSC Is the Prime (or Higher-Tier Sub)

In this role, OSC is the enforcement point. Under DFARS 252.204-7021, OSC must:

1. **Determine each sub's required level.** The prime, not the sub, determines the CMMC level for each subcontract based on the information that will be flowed down, using the matrix in 32 CFR 170.23(a):

- 2.

Flow-Down

If the OSA employs subcontractors to fulfill the contract, those subcontractors must also have a minimum CMMC Status as shown in table 2.

Table 2—Minimum Flow-Down Requirements

Prime contractor requirement	Minimum subcontractor requirement If the subcontractor will process, store, or transmit	
	FCI	CUI
Level 1 (Self)	Level 1 (Self)	N/A.
Level 2 (Self)	Level 1 (Self)	Level 2 (Self).
Level 2 (C3PAO)	Level 1 (Self)	Level 2 (C3PAO).
Level 3 (DIBCAC)	Level 1 (Self)	Level 2 (C3PAO).

Note: Under 170.23(b), CMMC not only applies to the Prime contractor but also to every subcontractor, sub-subcontractor, sub-sub-subcontractor, etc. no matter the depth. DoD may issue contract-specific flow-down guidance. Treat this matrix as the floor, not necessarily the ceiling.

3. **Control what you flow down.** The level you must impose follows the information you share. If a sub only needs FCI to perform, share only FCI. Flowing CUI to a sub that doesn't need it puts them in Level 2 scope unnecessarily and creates compliance risk for both parties.
4. **Verify before award.** Before awarding any subcontract, confirm the sub holds a current CMMC certificate or current CMMC status at the appropriate level. See Section 5 for timing details.

5. **Enforce affirmations.** Ensure each sub completes an affirmation of continuous compliance, signed by its affirming official (32 CFR 170.4), in SPRS for each in-scope information system. This must be done prior to award and annually thereafter.
6. **Include the clause in subcontracts.** Flow the -7021 requirements down contractually so the same obligations cascade to every lower tier that handles FCI or CUI. Suppliers that handle neither are outside the flow-down.

Key risk: OSC is legally responsible for its supply chain's compliance. Knowingly awarding to a non-compliant sub while representing compliance creates False Claims Act exposure. Because affirmations are annual, this is an ongoing risk throughout performance, not a one-time issue at award.

4. Responsibilities When OSC Is the Subcontractor

In this role, OSC is the verification target. Before a prime can award to OSC, expect the following:

1. **A current CMMC status at the level the prime determines.** The required level is driven by what the prime flows down: FCI only means Level 1 (Self); CUI means Level 2 at minimum, with the assessment type (Self vs. C3PAO) following the prime's own contract requirement. Practical implication: if OSC handles CUI for a prime whose contract requires Level 2 (C3PAO), a self-assessment will not be sufficient. Third-party certification is required.
2. **Clarity on the information involved.** Before accepting a subcontract, get the prime to identify in writing whether the effort involves FCI only or CUI, and which CUI categories apply. This determination drives scope, required level, and cost to perform. Push back on unmarked or ambiguous data.
3. **Assessment results visible in SPRS.** Primes will check SPRS before issuing awards. Many major primes are also embedding CMMC status declarations into their annual supplier registrations and reps & certs.
4. **A pre-award and annual affirmation.** OSC's designated affirming official must sign an affirmation of continuous compliance for each in-scope information system, completed before award and maintained annually in SPRS.
5. **OSC's own flow-down program.** If OSC uses lower-tier suppliers who handle FCI or CUI under the subcontract, OSC carries the same prime-style obligations to them: level determination, pre-award verification, affirmation enforcement, and contractual flow-down.

Practical takeaway: Because OSC handles both information types across changing roles, the durable posture has two parts. First, maintain Level 1 compliance enterprise-wide as the floor. Second, maintain a defined CUI environment certified to Level 2. For companies performing CUI work across multiple primes, Level 2 (C3PAO) is usually the right target, since it ensures an assessment-type mismatch never stalls a teaming arrangement or award.

5. Timing: When Subcontractor Verification Must Occur

The Trigger Is Subcontract Award

DFARS 252.204-7021 requires verification prior to awarding a subcontract or other contractual instrument, not at prime contract award and not at proposal submission. Two details in the clause language matter:

- **“Or other contractual instrument.”** The obligation is not limited to formal subcontracts. Purchase orders, task orders under existing supplier agreements, and similar ordering instruments are captured. Each time OSC issues a new instrument to a supplier who will touch FCI or CUI under a -7021 contract, the verification obligation applies again, even mid-performance.
- **“Current.”** The sub must already hold the status at award. “Working toward certification” does not satisfy the clause. A current status is generally one not more than three years old that remains valid throughout performance. A Conditional status (achieved with a permissible POA&M closed out within 180 days per 32 CFR 170.21) counts as current during its window.

Verification Is Continuous, Not One-Time

The clause imposes a two-part timing requirement: the sub's certificate or status must be verified before award, and affirmations of continuous compliance must be confirmed before award and annually for the life of the subcontract. The prime's verification duty runs throughout performance.

When the Obligation Attaches: The Phased Rollout

The pre-award verification duty exists only when the prime contract contains the -7021 clause. Clause inclusion follows the four-phase schedule in 32 CFR 170.3(e):

Phase	Begins	What Is Included
Phase 1	Nov 10, 2025	Level 1 (Self) or Level 2 (Self) in applicable solicitations and contracts as a condition of award. At DoD's discretion: inclusion as a condition of option exercise on earlier awards, and Level 2 (C3PAO) in place of Level 2 (Self).
Phase 2	Nov 10, 2026 (paused pending DoW review, July 2026)	Adds Level 2 (C3PAO) for applicable solicitations and contracts as a condition of award. Hard planning deadline for third-party certification.
Phase 3	Nov 10, 2027 (contingent on review outcome)	Adds Level 3 (DIBCAC) requirements for applicable contracts.
Phase 4	Nov 10, 2028 (contingent on review outcome)	Full implementation. All applicable DoD contracts (except those solely for COTS items) involving FCI or CUI include the appropriate CMMC level as a condition of award, including option periods on earlier contracts.

Important: The rollout is contract-driven, not organization-wide. Some solicitations will require Level 2 certification earlier than the phase schedule suggests, and primes may impose flow-down requirements that run ahead of the federal baseline, including in supplier registrations. OSC should scrutinize every solicitation, task order, and supplier agreement for the -7021 clause rather than relying on phase dates. As of July 2026, Phase 2 (Level 2 C3PAO) implementation is paused pending the Department of War review; Phase 1 self-assessment obligations and all safeguarding requirements remain in effect.

Practical Workflow Implications

- **As a prime:** build a CMMC gate into the procurement cycle before PO or subcontract issuance, checking SPRS for the sub's current status and affirmation under its CMMC UID.
- **As a sub:** certification cannot start when the RFP drops. Median time from solicitation to award runs roughly 45 days, while reaching assessment-readiness typically takes 12 to 18 months for a full enterprise (some tightly-bounded enclave deployments can be ready in five to six months). A sub that waits for a flowed-down requirement to appear has already missed the award.

6. Authoritative Sources

- 32 CFR 170.23 — Application to subcontractors (eCFR) — <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.23>
- 32 CFR 170.3 — Applicability and phased implementation (eCFR) — <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-A/section-170.3>
- 32 CFR Part 170 — Full CMMC Program Rule (eCFR) — <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170>
- DFARS 252.204-7021 (NOV 2025) — Full clause text (Cornell LII) — <https://www.law.cornell.edu/cfr/text/48/252.204-7021>
- FAR 52.204-21 — Basic Safeguarding of Covered Contractor Information Systems (FCI baseline) — <https://www.acquisition.gov/far/52.204-21>
- 32 CFR Part 2002 — Controlled Unclassified Information (CUI definition and program) — <https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002>
- DoDI 5200.48 — Controlled Unclassified Information (designation, marking, legacy information) — <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF>
- DoD CUI Registry — CUI categories — <https://www.dodcui.mil>
- CMMC Program Final Rule, 89 FR 83092 (Oct. 15, 2024) (Federal Register) — <https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program>

This document summarizes regulatory requirements for planning purposes and does not constitute legal advice. Contract-specific obligations are governed by the clauses incorporated into each solicitation, contract, and subcontract.