When a Subcontractor Needs CMMC Certification and When It Does Not

A Practical Reading of 32 CFR 170.23 for Tier 2 and Tier 3 Defense Suppliers

David W. Koran
CyberAB Registered Practitioner Advanced
June 2026

Abstract

A defense manufacturer receives a notice from a prime contractor stating that CMMC requirements will flow down under 32 CFR 170.23. The owner has heard about Level 2 certification, the C3PAO assessment process, the cost of remediation, and the timing of the CMMC implementation cycle. The question on the table is whether the company actually needs to pursue certification and, if so, at what level.

This paper answers that question by reading the regulation. The text of 32 CFR 170.23 is short, and the logic is straightforward, but the practical implications are not always presented clearly. Most public discussions treat CMMC certification as a binary condition that any defense supplier must satisfy. The regulation is more discriminating than that.

The reader who finishes this paper will know how to map the operational reality of their business to the level of CMMC Status required by the regulation, and will know which questions to put back to the prime when the flowdown notice is ambiguous. The paper is written for the Tier 2 and Tier 3 subcontractor owner, not for the prime contractor or the legal advisor, although both will find the analysis usable.

The Subcontractor's Problem

The typical situation has the same structure across most cases. A defense prime contractor sends a notice to its supply base. The notice explains that CMMC requirements will appear in upcoming subcontracts, that suppliers should prepare to demonstrate compliance, and that suppliers who cannot demonstrate compliance may be ineligible for future work. The notice usually cites 32 CFR 170.23 but does not quote it.

The subcontractor receives the notice and faces three possible interpretations. The first interpretation is that the company is fine, because it is only a small supplier and the requirement is for the prime. The second interpretation is that the company must obtain CMMC Level 2 certification from an external assessor, because that is what the public discussion suggests. The third interpretation is that the company must figure out what it actually does in performance of the subcontract, then map that to the language of the regulation.

The first interpretation is wrong as a matter of regulation. The second interpretation is sometimes correct but often overshoots the actual requirement. The third interpretation is the one the regulation expects.

The cost difference between the interpretations is material. A subcontractor that handles only Federal Contract Information requires a Level 1 self-assessment, which is something the company itself performs and affirms. A subcontractor that handles Controlled Unclassified Information requires a Level 2 status, which is at minimum a self-assessment but may, depending on the prime contract, require a Certified Third Party Assessor Organization to conduct the assessment. The gap between a Level 1 self-assessment and a Level 2 C3PAO assessment, in terms of cost, time, and operational disruption, is substantial. Choosing the wrong starting point costs the company money it did not have to spend, or leaves it short of the requirement when an award is on the line.

The Full Text of 32 CFR 170.23

The regulation is reproduced below in its entirety as it appears in the Code of Federal Regulations as of the date of this paper. The text is short. The analysis in the remainder of this paper proceeds paragraph by paragraph through this language.

§ 170.23 Application to subcontractors.

(a) CMMC requirements apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit any FCI or CUI on contractor information systems in the performance of the DoD contract or subcontract. Prime contractors shall comply and shall require subcontractors to comply with and to flow down CMMC requirements, such that compliance will be required throughout the supply chain at all tiers with the applicable CMMC level and assessment type for each subcontract as follows:

(1) If a subcontractor will only process, store, or transmit FCI (and not CUI) in performance of the subcontract, then a CMMC Status of Level 1 (Self) is required for the subcontractor.

(2) If a subcontractor will process, store, or transmit CUI in performance of the subcontract, then a CMMC Status of Level 2 (Self) is the minimum requirement for the subcontractor.

(3) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for a CMMC Status of Level 2 (C3PAO), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.

(4) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for the CMMC Status of Level 3 (DIBCAC), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.

(b) As with any solicitation or contract, the DoD may provide specific guidance pertaining to flow-down.

Source: 32 CFR 170.23, codifying 89 FR 83214 (October 15, 2024). Authority: 5 U.S.C. 301; Sec. 1648, Pub. L. 116-92, 133 Stat. 1198.

Paragraph by Paragraph

Paragraph (a): The Umbrella Provision

Paragraph (a) does three things. First, it establishes who the requirement applies to. Second, it identifies the operational trigger that brings a contractor within scope. Third, it imposes the flowdown obligation on the prime.

The first point matters because the language is explicit that CMMC requirements apply throughout the supply chain at all tiers. There is no exemption for small suppliers, no carve-out for indirect suppliers, and no minimum dollar threshold below which the requirement disappears. A Tier 4 fastener supplier that handles CUI while performing a subcontract is within scope. A Tier 1 systems integrator that does not handle FCI or CUI in performance of its prime contract is not within the scope of section 170.23 for that contract, although other obligations may apply.

The second point is the operational trigger, and it is the most important sentence in the regulation. The trigger is whether the subcontractor will process, store, or transmit any FCI or CUI on contractor information systems in the performance of the DoD contract or subcontract. This is an operational test, not a contractual test. The relevant question is not what the subcontract says about cybersecurity. The relevant question is what the subcontractor will actually do with FCI or CUI in performing the work.

If the subcontract does not require the supplier to receive, generate, store, or transmit FCI or CUI in any form, the supplier is outside the scope of section 170.23 for that subcontract. This is a meaningful exemption and it is the one that most often gets missed. A subcontractor that performs work entirely on the basis of unclassified, publicly releasable specifications, that does not store any defense customer data, and that does not transmit any defense customer data, has nothing to demonstrate under section 170.23 for that subcontract.

The third point is the imposition of the flowdown obligation on the prime. The verb is shall, twice. The prime shall comply and shall require subcontractors to comply. This is a binding obligation on the prime, not a discretionary practice. A prime that fails to flow down CMMC requirements to subcontractors that will process, store, or transmit FCI or CUI creates contractual exposure for itself. The subcontractor is generally not the party that bears the regulatory consequence of a missed flowdown, although a subcontractor that holds itself out as compliant when it is not faces a different category of exposure under the False Claims Act.

Paragraph (a)(1): The FCI Only Case

Paragraph (a)(1) addresses the simplest case. If a subcontractor will only process, store, or transmit FCI and not CUI in performance of the subcontract, a CMMC Status of Level 1 (Self) is required. The word only is doing significant work in this sentence.

Federal Contract Information is the broader category. It covers information provided by or generated for the Government under a contract that is not intended for public release. Most purchase orders, most delivery schedules, most non-public administrative correspondence with a Federal customer, and many engineering specifications fall within the scope of FCI. Controlled Unclassified Information is the narrower category. It covers information that is designated by a Federal authority as requiring safeguarding or dissemination control under a specific statute, regulation, or government-wide policy. A drawing is not CUI merely because it relates to defense work. The controlling question is whether the information falls within a CUI category and has been designated, marked, or otherwise identified by the Government or an authorized holder as requiring CUI safeguarding or dissemination control. If the markings or instructions are absent or

inconsistent, the supplier should ask the prime or contracting authority for clarification rather than guessing.

The practical implication for the Tier 2 or Tier 3 supplier is that many subcontracts involve FCI but no CUI. A job shop that receives a purchase order involving nonpublic Federal contract information, but receives no CUI-marked or otherwise CUI-designated engineering data, may be in the FCI-only category for that subcontract. The required CMMC Status is Level 1 (Self), which consists of a self-assessment against the 15 requirements of FAR 52.204-21 and an affirmation submitted by the supplier.

The cost and operational impact of Level 1 (Self) is meaningfully lower than the cost of Level 2 in any form. A subcontractor that has concluded it needs Level 2, when in fact its work is FCI-only, has spent money and management attention that the regulation does not require. A subcontractor that has concluded its work is FCI only when one or more subcontracts involving CUI have, in fact, failed to meet a regulatory requirement.

The diagnostic question for the supplier is not which category the prime contract falls into. The diagnostic question is what the subcontract requires the supplier to receive, store, generate, or transmit. If anything in that operational list is CUI, paragraph (a)(1) does not apply, and the supplier must read paragraphs (a)(2) through (a)(4).

Paragraph (a)(2): CUI Without a Specified Assessment Type

Paragraph (a)(2) addresses the case where the subcontractor will process, store, or transmit CUI but the prime contract itself does not carry a specific Level 2 (C3PAO) or Level 3 (DIBCAC) requirement. In that case, the minimum CMMC Status for the subcontractor is Level 2 (Self).

Level 2 (Self) requires the supplier to implement the 110 security requirements of NIST SP 800-171 Revision 2 as applicable to the contractor information system within the CMMC Assessment Scope, document those implementations in a System Security Plan, conduct a self-assessment, score the results, and affirm continuous compliance. A senior company official must sign the affirmation. The score is reported in the Supplier Performance Risk System.

The operational lift required to satisfy Level 2 (Self) is substantially greater than that required to satisfy Level 1 (Self). The number of security requirements is more than seven times larger, the documentation expectations are significantly higher, and the affirmation creates personal accountability for the official who signs. The financial cost of moving from the current state to Level 2 (Self) varies widely with the maturity of the supplier's existing controls, but for most small manufacturers, it is measured in tens of thousands of dollars and several months of effort.

The minimum language matters. Paragraph (a)(2) sets a floor, not a ceiling. A prime contract may require something higher than Level 2 (Self) for its subcontractors, and paragraphs (a)(3) and (a)(4) address the two specific cases in which the floor moves up. Paragraph (b) addresses the case in which the DoD provides specific guidance that supersedes the cascade.

Paragraph (a)(3): When the Prime Contract Requires Level 2 (C3PAO)

Paragraph (a)(3) addresses the case where the subcontractor will process, store, or transmit CUI and the prime contract has a requirement for Level 2 (C3PAO). In that case, the subcontractor's minimum CMMC Status is also Level 2 (C3PAO).

Level 2 (C3PAO) requires the same 110 security requirements as Level 2 (Self), but the assessment is conducted by a Certified Third Party Assessor Organization rather than by the supplier itself. The C3PAO will examine evidence, interview personnel, observe systems, and produce a finding of compliance, conditional compliance, or noncompliance for each requirement. The result is recorded in the Supplier Performance Risk System and remains valid for three years.

The practical implication is that when the prime contract requires a C3PAO assessment, the requirement fully propagates to the subcontractor that handles CUI. The supplier cannot satisfy the requirement with a self-assessment in this case. The cost and timeline of a C3PAO assessment are materially higher than a self-assessment, and the supplier must select an authorized C3PAO from the approved registry, schedule the assessment, prepare the evidence package, and pass the examination.

The supplier should not assume that a prime contract at Level 2 (Self) carries forward to require Level 2 (C3PAO) for the subcontractor. The cascade in paragraph (a)(3) is triggered specifically when the prime contract has the C3PAO assessment requirement. A prime at Level 2 (Self) requires its CUI handling subcontractors to be at Level 2 (Self) at a minimum, not Level 2 (C3PAO).

Paragraph (a)(4): When the Prime Contract Requires Level 3 (DIBCAC)

Paragraph (a)(4) is the provision most often misread. It addresses the case in which the subcontractor will process, store, or transmit CUI, and the prime contract includes a requirement for Level 3 (DIBCAC). In that case, the minimum CMMC Status for the subcontractor is Level 2 (C3PAO), not Level 3 (DIBCAC).

Section 170.23 does not require Level 3 (DIBCAC) to flow down to subcontractors through the default cascade. Under that cascade, a subcontractor that handles CUI on a Level 3 prime contract requires Level 2 (C3PAO) at a minimum. Separate contractual, program-specific, or DoD-directed requirements must be analyzed on their own terms. In this scenario, the DIBCAC assessment is reserved for the prime contractor itself rather than being imposed across the supply base by the regulation.

There is a practical reason for this design choice. Level 3 implements requirements drawn from NIST SP 800-172, the enhanced security requirements for protecting CUI in environments associated with high-value assets or critical defense programs. The implementation cost of those enhanced requirements is high. Imposing Level 3 on every CUI-handling supplier in a Level 3 program supply chain would render the program economically infeasible for most suppliers. The regulation caps the supplier requirement at Level 2 (C3PAO) regardless of how high the prime contract reaches.

There is one caveat worth noting. Paragraph (b) preserves DoD's ability to provide specific guidance pertaining to flowdown for a particular procurement. In principle, a specific program could require something different. In practice, the Level 2 cap (C3PAO) is the operative rule for the vast majority of subcontractors.

Paragraph (b): The DoD Guidance Reservation

Paragraph (b) is one sentence. It states that, as with any solicitation or contract, the DoD may provide specific guidance pertaining to flowdown. This reservation allows the Department to require something different for a specific procurement when the cascade in paragraph (a) does not meet the program's needs.

Two implications follow from this reservation. First, the cascade described in paragraphs (a)(1) through (a)(4) is the default, not an absolute rule. Second, the specific terms of the prime contract and the associated solicitation control if they say something different. A supplier should not rely solely on the cascade if the prime contract or the prime's flowdown notice specifies a requirement that differs from the default. The prime is in a position to know what its solicitation actually requires, and the supplier should read the flowdown notice for any departure from the cascade before concluding its obligation.

A Decision Framework for the Subcontractor

The analysis above can be reduced to three questions that a subcontractor owner can ask themselves to determine what section 170.23 actually requires for a particular

subcontract. The questions are sequential. The answer to each one either ends the inquiry or determines the next question.

Question one: Will the performance of this subcontract require the company to process, store, or transmit any FCI or CUI on company information systems?

If the honest answer is no, the subcontract is outside the scope of section 170.23. The company has no CMMC Status obligation under section 170.23 for that subcontract. The honest answer requires the supplier to think operationally rather than contractually. The relevant question is whether the work will actually involve receiving, storing, generating, or transmitting FCI or CUI. If it will not, the inquiry ends.

Question two: If the answer to question one is yes, will the work involve CUI specifically, or only FCI?

If the work involves only FCI and no CUI, the required CMMC Status is Level 1 (Self) under paragraph (a)(1). If the work involves CUI, the inquiry proceeds to question three. The diagnostic for whether information is CUI is whether the information falls within a CUI category and has been designated, marked, or otherwise identified by the Government or an authorized holder as requiring CUI safeguarding or dissemination control.

Question three: If the work involves CUI, what assessment type does the prime contract require?

If the prime contract requires Level 2 (Self), the subcontractor requires Level 2 (Self) at a minimum under paragraph (a)(2). If the prime contract requires Level 2 (C3PAO), the subcontractor must also be Level 2 (C3PAO) under paragraph (a)(3). If the prime contract requires Level 3 (DIBCAC), the subcontractor requires Level 2 (C3PAO), not Level 3, under paragraph (a)(4). The maximum requirement under the default cascade in paragraph (a) is Level 2 (C3PAO) unless there is specific DoD flowdown guidance under paragraph (b).

Reduced to a table, the cascade looks as follows.

What the subcontract requires you to handle	CMMC Status of the prime contract	Minimum CMMC Status for the subcontractor
No FCI and no CUI	Any	None under 32 CFR 170.23
FCI only	Any	Level 1 (Self)
CUI	Level 2 (Self)	Level 2 (Self)
CUI	Level 2 (C3PAO)	Level 2 (C3PAO)
CUI	Level 3 (DIBCAC)	Level 2 (C3PAO)

What the Subcontractor Should Ask the Prime

1. Does this subcontract involve FCI, CUI, both, or neither?

2. Will the supplier process, store, or transmit the information on its own contractor information systems?

3. What CMMC Status and assessment type applies to the associated prime contract?

4. Is the subcontractor expected to achieve Level 1 (Self), Level 2 (Self), or Level 2 (C3PAO)?

5. Are there any program-specific DoD flowdown instructions beyond 32 CFR 170.23?

What to Do When the Prime's Notice Is Ambiguous

Many flowdown notices arrive without specifying which assessment type the prime contract carries or whether the subcontractor will receive CUI. The subcontractor cannot complete the analysis above without that information. The correct response is to ask the prime directly, in writing, for two specific pieces of information. First, whether the prime contract requires Level 2 (Self), Level 2 (C3PAO), or Level 3 (DIBCAC). Second, whether the supplier's performance of the subcontract will involve CUI or only FCI.

A prime that is paying attention to its own flowdown obligation under paragraph (a) will be able to answer both questions. A prime that cannot answer either question has not done the work the regulation requires. The supplier is entitled to that information, and

acting on uncertainty about whether the work involves CUI is worse than asking the question and waiting for the answer.

The regulation establishes the operational test for what is required, but the contractual mechanism for enforcing the requirement is the inclusion of DFARS 252.204-7021 in the subcontract. If that clause appears in a subcontract that the subcontractor's operational analysis places outside the cascade, the resolution is to ask the prime in writing whether the clause was inserted intentionally and, if not, to seek a modification through the contracting authority. The subcontractor cannot unilaterally read itself out of a clause included in a signed subcontract, even if the regulatory cascade does not require it.

What Not to Do

Three responses are common, and three responses are wrong. The first wrong response is to assume the requirement does not apply because the company is small or remote from the prime contract. The cascade explicitly reaches all tiers and provides no exemption for small suppliers. The second wrong response is to assume the requirement is Level 2 (C3PAO) because that is the level the public discussion most often references. The cascade is more discriminating. Many subcontracts require only Level 1 (Self). Some subcontracts require no CMMC Status at all. The third wrong response is to assume the prime will tell the supplier exactly what to do. Some primes will. Many primes are still working out their own flowdown processes. The supplier who waits for clarity that may never arrive will be in worse shape than the supplier who reads the regulation and asks the diagnostic questions.

A fourth point belongs alongside these three. Some primes proactively flow down requirements stricter than the regulatory cascade requires, including supplier questionnaires, attestation programs, or contractual minimums above the Level 1 (Self) or Level 2 (Self) floors. The regulation does not prohibit a prime from imposing requirements above the cascade as a matter of supplier program policy. Where this occurs, the supplier's obligation is to read the specific contract and supplier program terms rather than to rely on the regulatory cascade alone. The cascade tells the supplier what the regulation requires. The contract and the supplier program specify what the prime requires.

Closing Observation

Section 170.23 is shorter than most discussions of it. The regulation establishes an operational test, not a contractual one. It cascades through four cases that map cleanly

to the supplier's actual circumstances. Under the default cascade, it caps the supplier requirement at Level 2 (C3PAO) regardless of how high the prime contract reaches, unless specific DoD flowdown guidance or contract terms require a different analysis. A supplier that reads the regulation and answers three questions honestly can determine what is required of it without depending on the prime's clarity, public discussion, or the marketing language used by vendors selling compliance products.

The reading of the regulation in this paper is not legal advice. It is a practitioner's reading of the operative text, intended to help the subcontractor owner think clearly about an obligation that affects business decisions. A supplier facing a specific contractual or compliance question should obtain advice from qualified counsel and from a practitioner with operational familiarity with the supplier's environment.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced and the author of The CMMC Decision (second edition). He is an Associate Member of the American Bar Association Section of Public Contract Law and a professional member of ISACA.

His practice focuses on CMMC readiness, enablement, and implementation work with defense industrial base contractors and the legal counsel that advises them. His operational background includes work in manufacturing environments, enterprise resource planning systems, shop-floor and CNC workflows, export-controlled manufacturing workflows, and Microsoft 365 deployments. He regularly writes about the operational and regulatory dimensions of the CMMC Program at davidkoran.com.

He can be reached at dkoran@davidkoran.com or 802-335-2662.

References

32 CFR 170.23, Application to subcontractors. Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.23

32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Final rule. 89 FR 83214 (October 15, 2024). https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements. Defense Federal Acquisition Regulation Supplement. https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. Federal Acquisition Regulation. https://www.acquisition.gov/far/52.204-21

NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-172/final

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements. Final rule. Federal Register, September 10, 2025. https://www.federalregister.gov/documents/2025/09/10/2025-17132/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of