No Certification, No Contract

A Practical Guide to CMMC Eligibility for Defense Subcontractor Executives

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

Introduction

Under current DoD contracting rules, a company that does not hold the required CMMC certification at the time of award is not eligible to receive the contract, regardless of past performance, pricing, or technical capability. That is the operating condition. Everything in this paper flows from it.

The Department of Defense finalized the CMMC program rule (32 CFR Part 170) in October 2024 and began a phased implementation that extends through November 2028. The rule replaced the prior model of self-attested compliance with a requirement for independent, third-party verification. Many prime contractors are not waiting for the final implementation phase. They are enforcing CMMC requirements now through supplier screening, flow-down clauses, and formal compliance questionnaires. For defense subcontractors, these CMMC requirements are not advisory. They are a condition of contract eligibility enforced through DFARS clauses and prime contractor supply chain controls.

This paper is a reference for reading and interpreting the specific contract instruments that carry CMMC obligations: the Section H flow-down clause, the Supplier Enablement Inquiry, and the compliance questionnaire. Each section deconstructs the language, identifies the regulatory authority behind it, and connects it to the business decision it creates.

Can You Bid Without CMMC Certification?

In practical terms, no. While a company may technically submit a proposal, a contractor that does not hold the required CMMC certification at the time of award is not eligible to receive the contract. Prime contractors are increasingly enforcing this condition before bids are even accepted, screening out suppliers that cannot demonstrate certification or a verified assessment timeline. The sections that follow explain exactly how this enforcement works at the contract, solicitation, and supply chain management level.

Where CMMC Requirements Appear in DoD Contracts

CMMC requirements enter a solicitation through two primary instruments. DFARS 252.204-7021 is the contract clause that establishes the certification obligation. DFARS 252.204-7025 is the companion solicitation provision that notifies offerors of the specific CMMC level required for the effort. Additional flow-down language typically appears in Section H (Special Contract Requirements), where the contracting officer may add supplementary conditions.

The Section H Flow-Down Clause and DFARS 252.204-7021

DFARS 252.204-7021 requires the contractor to maintain a current CMMC status for the information systems used in the performance of the contract, at the level specified in the solicitation through DFARS 252.204-7025. For contracts involving Controlled Unclassified Information (CUI), the specified level is typically CMMC Level 2, which requires implementation of all 110 NIST SP 800-171 security requirements and verification through a C3PAO assessment. A representative Section H flow-down provision reads as follows:

> *Pursuant to DFARS 252.204-7021, the Subcontractor shall maintain the required CMMC Level for the duration of this contract. For this effort, the Government has determined that the Subcontractor will handle Controlled Unclassified Information (CUI). Therefore, CMMC Level 2 (Advanced) is a mandatory condition for contract award and performance.*

Three elements of this clause carry direct consequences. First, "mandatory condition for contract award" means the certificate must be in hand before the contract is executed. Second, "duration of this contract" establishes an ongoing obligation across the full period of performance, including option years. DFARS 252.204-7021 further requires an annual affirmation of continued compliance submitted through eMASS by a designated affirming official, and the contractor must hold current CMMC status before exercising any option period or contract extension. Third, the determination that the subcontractor "will handle CUI" is

made by the Government based on the data flows inherent in the work. It sets the CMMC level and is not subject to contractor reinterpretation.

Key Contract Terms

Contract Term	Source	Operational Meaning
"CMMC Level 2 (Advanced)"	DFARS 252.204-7021; level per 252.204-7025	Full implementation of 110 NIST SP 800-171 controls, verified by C3PAO assessment. The level is stated in the solicitation provision.
"Mandatory condition for contract award"	Section H Flow-Down	Certificate must be held before award. No conditional awards, no exceptions.
"Duration of this contract"	DFARS 252.204-7021	Certification maintained through all performance periods. Annual affirmation required. Lapse equals breach.
"Will handle CUI"	Government Determination	The Government determines CUI presence based on data flows. This drives the CMMC level.
"CMMC Status" in SPRS	DFARS 252.204-7021	Certification status and annual affirmation are recorded in SPRS. This is the primary compliance indicator primes and the Government reference for eligibility.
"Flow-down to subcontractors"	DFARS 252.204-7021(c)	CMMC requirements must flow to all subcontractors processing, storing, or transmitting FCI or CUI.

Why Prime Contractors Are Screening Suppliers Before Bidding

Before releasing a formal solicitation, many prime contractors now issue a preliminary screening to their supply chain. These communications go by different names: Supplier Enablement Inquiry, Supply Chain Readiness Assessment,

Cybersecurity Compliance Verification Request. The function is the same in every case. The prime is identifying which suppliers can demonstrate CMMC readiness and which cannot, then building its team sheet accordingly. This practice has accelerated since 2025, with primes enforcing requirements well ahead of the DoD phased rollout through their own flow-down and supplier management processes.

A representative inquiry reads as follows:

> *To ensure supply chain continuity and satisfy DOD cybersecurity requirements for Solicitation DOD-AF-2026-0812, all tiered suppliers must provide documented evidence of CMMC Level 2 Readiness. Failure to provide current CMMC status in the Supplier Performance Risk System (SPRS) or a verified timeline for CMMC Certification by August 2026 will result in immediate disqualification from the bidding process.*

What This Language Means

"All tiered suppliers" extends the CMMC requirement beyond the direct subcontractor relationship. Any subtier supplier who will access CUI in the performance of the work faces the same obligation. The prime is establishing accountability through every level of its supply chain.

"Documented evidence" is not a verbal assurance or a letter of intent. The prime expects artifacts: a current System Security Plan, a Plan of Action and Milestones if applicable, and a confirmed C3PAO engagement letter with a scheduled assessment date.

"Current CMMC status in SPRS" reflects the shift from the legacy NIST SP 800-171 self-assessment score (established under DFARS 252.204-7019 and 252.204-7020) to the contractor's CMMC certification status and annual affirmation record as the primary data point. An organization that holds only a legacy self-assessment score without a current or in-progress CMMC certification faces increasing difficulty passing prime contractor supply chain reviews.

"Immediate disqualification" is a binary outcome, not a negotiation opening. The prime's own contractual obligations to the Government require a compliant supply

chain. A supplier that cannot demonstrate readiness is a risk the prime will not absorb.

The CMMC Compliance Questionnaire: What Primes Are Asking and Why

Beyond the formal contract language and enablement letters, prime contractors increasingly issue structured compliance questionnaires. These instruments vary in format but converge on the same core areas. The following table maps the standard questionnaire categories to the underlying reason the prime is asking.

Questionnaire Categories

Category	Typical Questions	Why the Prime Is Asking
CMMC Status and SPRS Record	Current CMMC certification status? Last annual affirmation date? Conditional or final certificate?	Validates that the certification record is posted and current. Primes cross-reference SPRS directly for eligibility determinations.
System Security Plan	Current SSP? CUI boundary defined? Last review date?	The SSP is the foundational assessment artifact. Without it, a C3PAO engagement cannot proceed.
C3PAO Engagement	C3PAO engaged? Scheduled assessment date? Certificate status?	Assessment scheduling capacity is limited. This determines whether the subcontractor's timeline aligns with the award date.
POA&M and Remediation	Open POA&M items? Projected remediation completion date?	Open items may support conditional certification with a 180-day remediation window. Open-ended remediation signals structural gaps.

Incident Response	Documented IR plan? Incidents reported to DIBCNET in the past 24 months?	DFARS 252.204-7012 requires 72-hour incident reporting. Failure to report creates program-level exposure.
CUI Handling	Procedures for identifying, marking, storing, transmitting CUI? Access controls?	Operational CUI procedures are a prerequisite for CMMC Level 2 assessment readiness.

Sample Questionnaire: 10 Questions to Expect

The following table presents a representative set of questions drawn from the types of compliance questionnaires currently circulating in the defense supply chain. These are not hypothetical. They reflect the data points prime contractors are requesting to evaluate subcontractor eligibility.

#	Question	What This Reveals
1	Does your organization currently hold a CMMC Level 2 certification (conditional or final)?	Immediate eligibility determination. A "no" triggers follow-up on timeline and readiness artifacts.
2	What is your current CMMC status as reflected in SPRS?	Validates that the certification record is posted. Primes cross-reference SPRS directly.
3	When was your most recent annual CMMC affirmation submitted, and who is the designated affirming official?	A lapsed or missing affirmation can disqualify a contractor from option year exercises.
4	Does your organization maintain a current SSP that defines your CUI environment boundary? When was it last updated?	The SSP is the most referenced artifact in a C3PAO assessment. An outdated or nonexistent SSP signals fundamental unreadiness.
5	Have you engaged a C3PAO? If yes, what is your scheduled assessment date?	Determines whether the certification timeline is realistic relative to the award date.

6	Do you have open POA&M items? If yes, what is the projected remediation completion date?	Evaluates whether remaining gaps are manageable within the 180-day conditional window or structural.
7	Describe your process for identifying, marking, storing, and transmitting CUI.	Tests whether the compliance program is operationalized or theoretical.
8	Do you have a documented cyber incident response plan? Have you reported any incidents to DIBCNET in the past 24 months?	Assesses both preparedness and disclosure history under DFARS 252.204-7012.
9	Do you use external service providers (MSPs, MSSPs, cloud providers) to process, store, or transmit CUI? If yes, are they CMMC-certified at the required level?	External providers within the CUI boundary are in scope for the assessment. An uncertified provider is a compliance gap.
10	Have you verified the CMMC certification status of your own subtier suppliers who will access CUI in this effort?	DFARS 252.204-7021 requires flow-down to all tiers. This tests whether the subcontractor has conducted its own supply chain due diligence.

Each response communicates more than a data point. A company that provides its certification status, affirmation date, C3PAO engagement, and projected timeline is communicating operational maturity. Vague timelines or qualifications such as "we are working on it" signal risk. Questionnaire responses should be treated with the same precision as a financial disclosure, because they become part of the contractual record and may be referenced in future audits or disputes.

The Business Impact of CMMC: Revenue, Disqualification, and Legal Exposure

Timeline Compression and the Readiness Gap

The practical window between a prime contractor's Supplier Enablement Inquiry and the contract award date is typically 120 to 180 days. Within that window, the subcontractor needs a mature SSP, a completed or nearly completed remediation of any POA&M items, and a scheduled or completed C3PAO assessment. Organizations that are beginning their compliance journey at the point they receive the inquiry face a readiness gap that is difficult to close.

Closing that gap requires capital allocation for technology investments, personnel time for documentation and implementation, and organizational change management to embed security practices into daily operations. These are decisions that take months to execute. If the inquiry arrives in April and the award decision is in October, the preparation needed to have been underway well before the inquiry was issued.

False Claims Act Exposure

The contractor's CMMC status and affirmation record in SPRS is a formal representation to the United States Government. If that representation does not accurately reflect the organization's implemented security controls, the contractor faces potential liability under the False Claims Act. The Department of Justice has pursued contractors who misrepresent their cybersecurity posture through its Civil Cyber-Fraud Initiative, which provides for treble damages and per-claim penalties. The CMMC status and any underlying assessment data must be the product of a rigorous, documented, and honest process. Any gap between the recorded status and actual implementation should be reflected in a POA&M with defined remediation milestones.

The SPRS Delta: When the Reported Score Does Not Match Reality

There is a specific condition that warrants direct attention. If there is any difference between the compliance posture reported in SPRS and the actual implemented state of the organization's security controls, that difference will surface during the C3PAO assessment. The assessment is a controls-level examination. The assessor will evaluate each of the 110 NIST SP 800-171

requirements against documented evidence and operational practice. A score posted to SPRS that reflects controls the organization has not actually implemented is not a gap that can be explained away during the assessment. It is a documented misrepresentation to the United States Government, and it creates the precise condition the Department of Justice targets through the False Claims Act.

If an organization has reason to believe that its reported SPRS score or CMMC status does not accurately reflect its current security posture, the appropriate response is to pause forward compliance assertions and engage legal counsel before taking any further steps. Under counsel's direction, a qualified third-party practitioner should conduct an independent scope discovery to establish the actual state of the environment, identify the specific controls that are and are not implemented, and determine the true delta between the reported position and operational reality. This is not a remediation exercise. It is a factual determination that must be completed before the organization can make informed decisions about how to proceed, what to disclose, and how to correct the record.

This step is not optional. An organization that proceeds to a C3PAO assessment with a known delta between its reported and actual compliance posture is compounding its exposure, not resolving it. The time to address this is before the assessment, not during it, and the process should be guided by counsel from the outset.

Revenue Retention

The practical consequence of the certification requirement is that work a company has performed for years under existing contracts may not be available for recompete if certification is not in place by the new solicitation date. In practical terms, this is not simply contract loss. It is competitive displacement, where certified competitors replace incumbents who cannot meet the eligibility threshold. Defense revenue that was historically retained through strong past performance and competitive pricing now has a gating prerequisite that is entirely separate from those factors. For companies where defense contracts represent a significant share of revenue, the certification timeline is a financial planning

variable that belongs in the same conversation as capital expenditure and workforce planning.

What to Do with This Information

Verify the SPRS record. If the organization has not yet achieved CMMC certification, confirm that the current assessment posture accurately reflects implemented controls. If the SPRS record is outdated or based on an informal methodology, it is a liability. A qualified practitioner can validate the current state and identify remaining steps before a C3PAO assessment.

Confirm the SSP. The SSP should describe the CUI environment boundary, the controls in place, and the roles responsible for maintaining them. If the SSP does not exist or has not been updated to reflect the current environment, the organization is not assessment-ready.

Engage a C3PAO now. Assessment scheduling capacity is limited. Lead times extend to several months. Waiting for a prime contractor's inquiry to trigger this action compresses the timeline to a degree that may not be recoverable.

Assign ownership. CMMC certification determines contract eligibility. The executive responsible for revenue retention in the defense portfolio should have direct visibility into the compliance program, assessment timeline, and resource allocation.

Audit the subtier supply chain. DFARS 252.204-7021 requires flow-down to all subcontractors processing, storing, or transmitting CUI. If the organization has not verified the CMMC status of its own subtier suppliers, it cannot provide an accurate questionnaire response and may be creating a compliance gap. Subcontract templates should include flow-down language and verification requirements.

Treat questionnaire responses as legal representations. Every response to a prime contractor's compliance questionnaire becomes part of the contractual record. Inaccurate or aspirational responses create exposure. Apply the same standard of accuracy used for financial certifications.

About the Author

David W. Koran, CyberAB Registered Practitioner Advanced (RPA), is the founder of David Koran & Associates, a CMMC compliance consulting firm serving Defense Industrial Base contractors and their legal counsel. The firm specializes in readiness, enablement, and implementation services for organizations navigating the CMMC certification process. Mr. Koran is an Associate Member of the American Bar Association Section of Public Contract Law and the author of *The CMMC Decision*. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements.

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7020, NIST SP 800-171 DoD Assessment Requirements.

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7021, Cybersecurity Maturity Model Certification Requirements.

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7025, Notice of CMMC Level Requirements.

National Institute of Standards and Technology, Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Title 32 Code of Federal Regulations Part 170, Cybersecurity Maturity Model Certification (CMMC) Program, Final Rule (October 2024).

U.S. Department of Justice, Civil Cyber-Fraud Initiative, https://www.justice.gov/civil/cyber-fraud-initiative

Supplier Performance Risk System (SPRS), https://www.sprs.csd.disa.mil