POLSINELLI

Publications

October 1, 2025 • Updates

CMMC Is No Longer Optional: Final Rule Launches November 10

After years of drafts and false starts, the Department of Defense[1] has finished the legal two-step to operationalize its Cybersecurity Maturity Model Certification (CMMC) program. DoD's recent publication of the second of two companion rules makes CMMC no longer a mere policy aspiration but a binding legal requirement in future (and potentially existing) defense contracts. The vast majority of DoD contractors and subcontractors must implement and soon be prepared to certify compliance with specified government cybersecurity standards, or risk being shut out of the defense supply chain once the program's new contract and solicitation requirements begin phasing in on November 10, 2025.

Read on for a breakdown of what the final rule requires, who must comply (and who's exempt), how the CMMC levels work, when enforcement begins and what contractors should be doing now to prepare.

What Is CMMC, and What's Changed?

For those unfamiliar with it, CMMC is the DoD's standardized framework for protecting unclassified information on contractor information systems. It requires contractors to meet and certify compliance with tiered cybersecurity requirements — Level 1, Level 2 or Level 3 — based on the sensitivity of the unclassified data that a contractor handles.

Companies that handle only "Federal Contract Information" (FCI) must meet the standards for CMMC Level 1, and companies handling "Controlled Unclassified Information" (CUI) in the performance of their defense contracts must satisfy CMMC Level 2. A small minority of companies working on the most sensitive and mission-critical DoD programs will be held to Level 3.

The cybersecurity protections themselves are not new: the earliest iterations of these requirements appeared in Federal Acquisition Regulation (FAR) 52.204-21 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 dating back to 2016 and 2015, respectively. CMMC takes these existing contractual requirements a step further by increasing oversight and contractor certification obligations as well as bolstering government enforcement mechanisms; a key impact of this new regime will be increased contractor liability risk for noncompliance with these existing standards.

Related People

- Erin L. Felix
- Sarah S. Glover
- Cate Baskin
- Mary Ann H. Quinn
- Olivia Velasco

Related Capabilities

- Government Contracts
- Privacy & Cybersecurity

DoD finalized the CMMC program structure in Title 32 of the Code of Federal Regulations (32 CFR Part 170) in late 2024. This first rulemaking formally established CMMC's programmatic and technical requirements, including self-assessment and third party certification criteria mechanics as well as supply chain flowdown requirements. This rule also defined a three-year phased implementation schedule, which commences upon the publication and effectivity of a companion procurement rule in the DFARS. On September 10, 2025, DoD issued this long-anticipated DFARS rule.

Beginning Nov. 10, 2025, DoD will begin incorporating CMMC clauses into defense solicitations and contracts, and contractors that aren't prepared will soon be ineligible to bid or perform.

Who Must Comply, and Who's Exempt?

CMMC applies to **all contractors and subcontractors in the defense supply chain that process, store, or transmit FCI or CUI in the performance of a DoD-funded contract**. Contractors will be required, as a condition of award and for the entire life of the contract, to have:

1. a current CMMC status, at the specified level, entered in the DoD's Supplier Performance Risk System (SPRS) portal; and
2. a current affirmation of continuous compliance in SPRS for each contractor information system that will process, store, or transmit FCI or CUI in performance of the contract.

A narrow exception exists for contracts and subcontracts that are "solely for the acquisition of commercially available off-the-shelf (COTS) items." This carveout is very limited, however: to qualify, items must be sold, unmodified, and in substantial quantities in the commercial marketplace. The COTS definition is also limited to "goods" only, so contracts for services likewise do not qualify. In addition, procuring agencies differ in their categorizations of whether Software as a Service, 'XaaS', or other cloud-based licenses constitute the purchase of a good or a service, so contracts for such licenses and services may fall outside of this exception as well. And unlike many government contracting provisions, there is no 'de minimis' dollar value below which a contract is exempt from CMMC. **The exception is painfully simple: if a procurement is *solely* for the acquisition of COTS items, it is exempted; otherwise, CMMC requirements apply.**

Even if CMMC requirements apply, however, the government or a higher-tier contractor may still determine that an individual contract will not require a contractor to process, store, or transmit any FCI or CUI. If this occurs, no CMMC compliance level is necessary.

By design, CMMC applies to the entirety of the DoD supply chain unless the COTS exception applies. While the regulatory implementation is currently focused on "procurement contracts" that are governed by the FAR and DFARS**, DoD has consistently indicated that it intends to implement these requirements in all DoD-funded agreements, including Other Transaction Agreements**. The government is responsible for determining and stating in each solicitation, and resulting prime contract, the specific CMMC level required for that award: Level 1 (Self), Level 2 (Self), Level 2 (C3PAO), or Level 3 (DIBCAC).

The Three CMMC Levels and What They Require

The CMMC framework defines three certification levels, each tied to the sensitivity of the unclassified information handled in contract performance. Most contractors will fall under Level 1 or Level 2. Only a narrow class of companies working on the most sensitive

mission-critical programs will be subject to Level 3.

- **Level 1 applies to Federal Contract Information.** It maps to 15 “basic” safeguards enumerated in FAR 52.204-21.
    - Contractors must complete an annual self-assessment against these safeguards and submit an annual affirmation in SPRS by a senior company “Affirming Official.”
- **Level 2 applies to Controlled Unclassified Information.** It aligns with 110 security controls enumerated in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2.
    - Depending on the procurement, DoD can require either self-assessment or mandate independent, third-party certification via a CMMC Third-Party Assessment Organization (C3PAO). These are separate CMMC designation levels: Level 2 (Self) and Level 2 (C3PAO).
    - In either case, the contractor must have its certification and affirmation of compliance on file at the time of the contract or subcontract award. Results are posted to the SPRS portal or, for certifications, to the Enterprise Mission Assurance Support Service (eMASS).
- **Level 3 applies to a small number of contractors supporting high-priority DoD missions.** It layers “enhanced” requirements from NIST SP 800-172 on top of Level 2.
    - Assessments are conducted directly by the Defense Contract Management Agency’s Defense Industrial Base Cybersecurity Assessment Center (DCMA DIBCAC) every three years.
- **Temporary “conditional” status may be available for Levels 2 and 3.** Contractors that have not fully implemented all 110 NIST SP 800-171 controls may still qualify for temporary Conditional CMMC status at Level 2 or Level 3. Conditional CMMC status may last for no more than 180 days.
    - To be eligible, a contractor must: achieve a minimum passing score of 80%; have gaps only in certain permitted controls; and have an approved Plan of Action and Milestones (POA&M) to remediate its deficiencies.
    - If the contractor fails to close all open items on its POA&M within the 180-day timeline, its CMMC status is no longer valid, and the contractor must report this to its immediate customer.
    - POA&M closeouts require an additional assessment – self, C3PAO, or DIBCAC – depending on the applicable CMMC level. The contractor must then re-affirm its CMMC status once it achieves its “Final” certification status.

New Contract and Pre-Award Requirements

The new DFARS rule also adds several contract requirements that apply to both prime contractors and subcontractors. Key provisions include:

- **Notice of CMMC Level Requirements** (DFARS 252.204-7025): A new solicitation provision in which the government will specify the CMMC level that will apply to any resulting contract, and which the prime contractor must meet as a condition of award.
- **CMMC Requirements** (DFARS 252.204-7021): A revised mandatory contract clause that likewise reflects the applicable CMMC level that the contractor’s covered information systems must maintain for the life of the awarded contract.
- **Affirming Official Designation:** Each contractor must formally designate an “Affirming Official” — a senior representative within the organization who is responsible for ensuring the company’s compliance with CMMC and has authority to formally affirm the company’s continuing compliance.
- **CMMC UID Tracking:** Contractors must **identify prior to award each contractor information system that will process, store, or transmit FCI or CUI in**

performance of the anticipated contract. SPRS assigns each information system a unique, 10-character "CMMC UID" upon submission of a CMMC assessment. Prime contractors must include every CMMC UID in their proposal and keep the list current throughout the life of the contract. Subcontractors must provide their CMMC UIDs to the prime contractor to include in the proposal to DoD.

- **Ongoing Reporting Requirements:** Contractors must report to the contracting officer for the life of the contract any changes to the list of previously identified CMMC UIDs used in performance of the contract.

Phased Implementation

The CMMC program will roll out over three years, beginning Nov. 10, 2025. During this period, DoD will gradually increase enforcement based on the contract type, certification level, and whether a new award or option period is at stake.

Phase	Start Date	Key Requirements/What Happens
Phase 1	November 10, 2025	• Requires CMMC Status of Level 1 (Self) or Level 2 (Self) as a condition of award for new DoD solicitations and resulting contracts. • DoD has discretion to require Level 2 (C3PAO) instead of Level 2 (Self). • DoD has discretion to require Level 1 (Self) or Level 2 (Self) as a condition to exercise an option period on a contract awarded prior to November 10th.
Phase 2	November 10, 2026	• Adds requirement for Level 2 (C3PAO) to applicable solicitations, but DoD has discretion to delay inclusion of Level 2 (C3PAO) to an option period instead of as a condition of contract award. • DoD has discretion to add Level 3 (DIBCAC) in new solicitations and contracts.
Phase 3	November 10, 2027	• Adds Level 2 (C3PAO) as a condition to exercise an option period on a contract awarded after November 10, 2025. • Adds requirement for Level 3 (DIBCAC) to applicable solicitations, but DoD has discretion to delay inclusion of Level 3 (DIBCAC) to an option period instead of as a condition of contract award.
Phase 4	November 10, 2028	• Full implementation: CMMC program requirements apply to all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.

What Prime and Subcontractors Need to Know

CMMC requirements will flow down to all subcontractors and non-COTS vendors that will "process, store, or transmit FCI or CUI" in the performance of a DoD-funded agreement. If your information systems process, store, or transmit FCI or CUI, you should assume that your upcoming solicitations and contracts will soon begin to incorporate CMMC requirements.

- **Primes must manage downstream compliance.** Prime and higher-tier contractors are tasked with ensuring their supply chains meet the 'appropriate' CMMC status for the information handled. Just as the government will identify the applicable CMMC level for the prime contract, primes and higher-tier contractors will be responsible for determining whether or what level of CMMC will apply to their lower-tier procurements. The CMMC program framework defines minimum subcontractor flowdown levels based on the prime contract's CMMC level.
- **Minimum compliance may not be enough.** Higher-tier contractors may decide for business and competitive reasons to align themselves only with subcontractor and vendor teams that already meet a certain, higher CMMC threshold — regardless of whether, in practice, the lower-tier supplier would handle data requiring that stricter requirement. This could make CMMC a competitive differentiator for defense subcontractors and vendors, not just a compliance hurdle.

- **Access to compliance information is limited**. Like primes, subcontractors must submit their CMMC certification statuses and affirmations of continuous compliance directly into SPRS. But higher-tier contractors will not have access to other companies' SPRS information. This disconnect could lead to significant negotiations and disagreements over how much sensitive internal information a subcontractor must share with its customer to validate its compliance status.
- **Higher CMMC levels may appear sooner.** Regardless of the "official" timeline, the government retains discretion to include higher levels of CMMC in a solicitation or contract, and prime contractors may also do the same either strategically or in response to a specific opportunity.

Readiness Checklist: Key Steps to Act on Now

CMMC requirements can be extensive for organizations, and it takes time—not to mention funding, resources, and outside support—to bring cybersecurity programs into compliance.

If you have not yet started, there are several steps you should be taking now to improve readiness:

- **Map your in-scope systems and identify your intended certification level based on the nature of the company's current and desired defense business.**
    - If you handle only FCI, plan for Level 1 (Self).
    - If you create, receive, or store CUI, assume Level 2, and consider whether your program is likely to require a C3PAO assessment in Years 1–2. *(DoD published internal selection guidance for program offices; expect more Level 2 (C3PAO) in Phases 2–3.)*
- **Conduct a pre-audit assessment.**
    - Before the formal self or C3PAO assessment, conduct a full internal or external pre-audit to test readiness. Confirm your documentation, controls, boundaries, and implementation truly align with your System Security Plan.
    - Use this mock audit to practice interviews, evidence collection, and control validation, and to obtain actionable feedback regarding potential gaps.
- **Identify gaps against NIST SP 800-171 Rev. 2.**
    - Treat the 110 controls and the 32 CFR scoring method as your working canon.
    - If you rely on POA&Ms, confirm that the items listed on your POA&M are eligible for inclusion and model whether you can clear the 80% minimum score and move to a "Final" status within 180 days. Do not assume you will be granted an extension.
- **Designate an Affirming Official.**
    - The individual must be a senior leader with authority to bind the organization, who understands CMMC obligations, and who is willing and legally able to personally attest to the accuracy of the company's submission.
- **Document the paperwork that proves it.**
    - You will need an accurate SSP, tight evidence trails, and annual executive affirmations in SPRS after assessments.
    - If you are headed for Level 2 (C3PAO), get on an assessor's calendar now — C3PAO backlogs are already filling up quickly.
- **Assess your flow-down and enclave strategy.**
    - Only flow down CUI to subcontractors that actually need it. Fewer CUI recipients means fewer Level 2 obligations in your supply chain.
    - Consider enclaving CUI to shrink your assessed footprint.

Looking Ahead: Enforcement Is Coming, But Compliance Is Achievable

The CMMC program is a critical component of DoD's strategy to protect sensitive information and intellectual property from foreign adversaries and other cyber threats. While the program presents challenges, particularly for predominantly commercial businesses and small businesses with fewer available resources, its phased implementation and allowance of temporary POA&Ms provide a pathway for contractors to achieve compliance.

As the November 10th implementation date looms, contractors and subcontractors should be actively preparing to meet these requirements to maintain eligibility for defense contracts. Polsinelli has a deep bench of experienced professionals who can assist with further questions as well as with navigating your company's CMMC compliance journey.

[1] President Trump signed an Executive Order on September 5, 2025, renaming the Department of Defense to the Department of War. As of the date of this alert, CMMC program requirements and published regulations continue to reference the Department of Defense, and this alert similarly retains this naming convention for consistency.