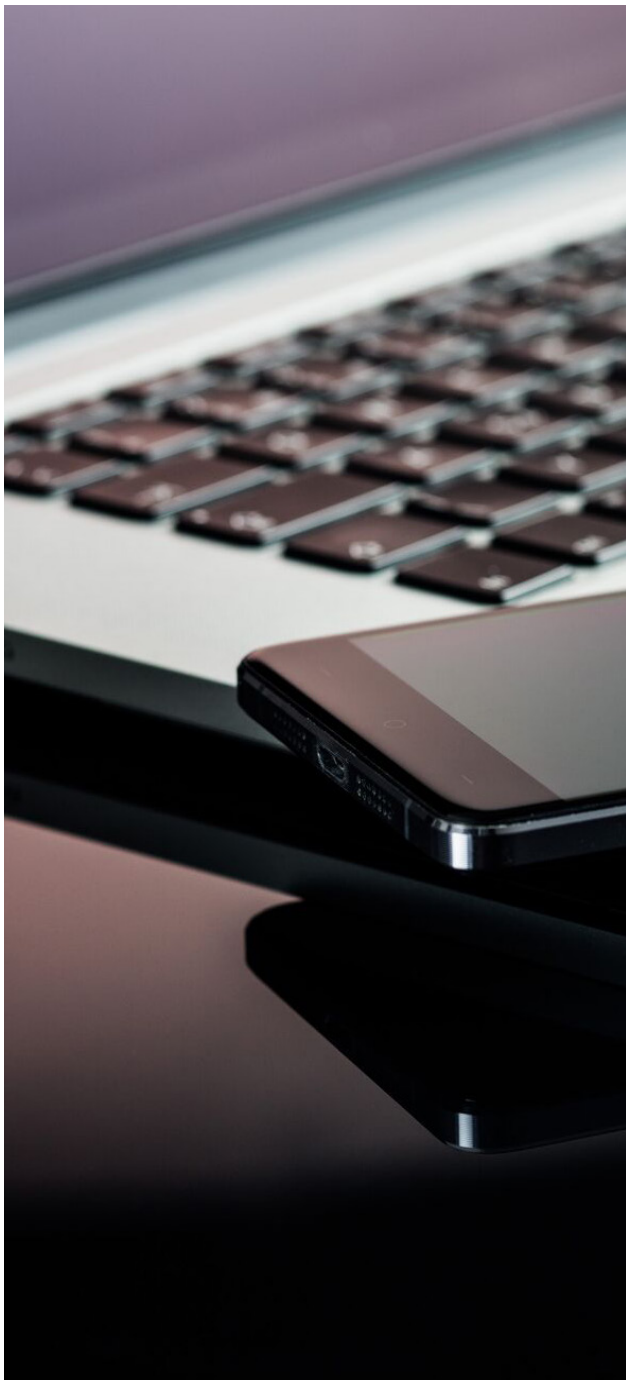
OCTOBER 2025

COVINGTON

Frequently Asked Questions Regarding the Cybersecurity Maturity Model Certification ("CMMC") Program for Government Contractors

Introduction

On September 10, 2025, the U.S. Department of Defense ("DoD") took the final regulatory step to implement the Cybersecurity Maturity Model Certification ("CMMC") Program by issuing the Procurement Rule that provides clauses and guidance on how the requirements for CMMC will be implemented in procurement contracts. Previously, in October 2024, DoD issued the CMMC Program Rule, which provided guidance on the technical controls and safeguarding requirements imposed on systems that process, store and transmit Federal Contract Information ("FCI") and Controlled Unclassified Information ("CUI") used in performance of a DoD contract (together the "Rules"). We have provided responses to certain key questions relating to these developments below to help contractors and subcontractors prepare for the Rules; however, we note that these FAQs are high-level, and the Rules include details not outlined here.



1 Who is subject to the CMMC requirements?

The CMMC Program applies to all contracts and subcontracts with DoD that include the appropriate DFARS clause (currently DFARS 252.204–7021).[1] The Program Office, rather than the Contracting Officer, will determine the appropriate CMMC level for a contract.

CMMC Level requirements flow down and apply to subcontractors under a DoD contract if the subcontractor processes, stores, or transmits FCI or CUI on its information systems in the performance of a government subcontract. Prime contractors are responsible for flowing down CMMC compliance requirements to subcontractors, and confirming a subcontractor's CMMC Program Status, in accordance with the solicitation and resulting contract based on the sensitivity of the information flowed down to each subcontractor.

Certain CMMC requirements also apply to in-scope systems provided by external service providers used by contractors and subcontractors under the Rules, discussed in some additional detail below.

1 DFARS clause 252.204–7021 provides for the insertion of the CMMC Requirements.

2 What are the safeguarding and assessment requirements at each level of CMMC?

The Rules authorize DoD to confirm that a defense contractor or subcontractor has implemented and maintains security requirements for one of three specified CMMC levels–Level 1, Level 2, or Level 3–and one of three assessment types–self-assessment, third party assessment, or government assessment–throughout the contract period of performance.

A DoD solicitation and/or contract will specify the minimum CMMC status required for a contractor to be eligible for the award or as a condition of the contract.[2]

The three CMMC levels are summarized as follows:

	LEVEL 1	LEVEL 2	LEVEL 3
APPLICABILITY	Processing, storing, or transmitting of FCI	Processing, storing, or transmitting of CUI	Processing, storing, or transmitting of some CUI (e.g., especially sensitive information)
SECURITY REQUIREMENTS	17 requirements in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 Rev. 2 (which map to 15 controls required by FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems)[3]	110 NIST SP 800-171 R2 required by DFARS 252.204-7012	▪ Contractors must obtain a CMMC Level 2 Final Certification Assessment for information systems within the Level 3 CMMC Assessment Scope as a prerequisite ▪ Contractors must also meet 24 additional security requirements from NIST SP 800-172 for assets and systems in scope under the Rules
ASSESSMENT REQUIREMENTS	Self-assessment annually	Either a third-party or self-assessment every three years. During the first year, self-attestations are expected to be sufficient for most DoD contracts. Then most Level 2 contracts will require an assessment by an authorized or accredited third party ("C3PAO"), though some contracts that involve comparatively less sensitive forms of CUI will still permit self-assessments	Requires a Defense Contract Management Agency ("DCMA") Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC")-led assessment every three years
PLANS OF ACTION AND MILESTONES ("POA&MS")	No exceptions or POA&Ms permitted	DoD requires that contractors have met all security controls, but allow for certain specific, limited instances in which some controls may not yet be fully implemented and subject to POA&Ms (e.g., conditional certification for 180 days for some controls while working to meet NIST standards)	The Rules provide for certain specific, limited instances in which a contractor may be able to use a POA&M if not every control has been met

2 The certification level required is generally based on the type of information that will need to be safeguarded during contract performance, and considerations including criticality of the associated mission capability, type of acquisition program or technology, threat of loss of the information, and impacts from exploitation of information security deficiencies.

3 Security requirements are specified for each level based on FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems and are cumulative (Level 1), as well as NIST SP 800-171 Rev. 2 (Level 2) and NIST SP 800-172 (Level 3).

3 Do I need to have a CMMC certification to receive an award from DoD?

If a DoD contract includes a CMMC requirement, to be eligible for an award, a contractor must adhere to the appropriate requirements and obtain certification for the minimum CMMC level in accordance with the solicitation.

Contracting officers will not make award, exercise an option, or extend the period of performance on a contract if the offeror or contractor does not have the (i) passing results of a current certification assessment or self-assessment for the required CMMC level, and (ii) an affirmation of continuous compliance with the security requirements in DoD's Supplier Performance Risk System ("SPRS") for all information systems that process, store, or transmit FCI or CUI during contract performance.

4 How does CMMC compare to my current DOD safeguarding obligations?

While the CMMC Program requirements track closely with existing NIST standards and existing FAR and DFARS requirements, the anticipated impact on defense contractors and subcontractors could be significant for contracts requiring the storing, processing, or transmission of FCI or CUI. For example:

- The Rules require contractors to identify each of the information systems that will process, store, or transmit FCI and/or CUI and other relevant assets that may be in scope for CMMC assessment requirements. This includes information systems provided by external service providers.
- The Rules require greater specificity for categorizing assets into varying CMMC Program categories to determine scope and corresponding requirements.
- The Rules also impose new assessment and affirmation processes for all contractors to be eligible for certain DoD contracts, with the majority of DoD contractors having to make at least an attestation to implementation of minimum cybersecurity requirements.
- Further, the Rules take a more stringent approach towards compliance, and once implemented, provide little flexibility for closing gaps on controls, prohibit the use of POA&Ms for CMMC Level 1 and permit businesses to obtain limited, conditional certification for 180 days if they are non-compliant with certain controls that are included on a POA&M. However, unlike the current regulatory scheme, certain controls must be met at the time of award.

5 How and when will CMMC be implemented?

DoD will implement the CMMC Program in four phases. Over a four-year period, CMMC level requirements will be incrementally added to solicitations, then to contracts, ending with full implementation of requirements in Phase 4.[4]

PHASES, EFFECTIVE DATES AND SECURITY REQUIREMENTS

PHASE 1	**Effective date of the final Procurement Rule - November 10, 2025**	
	■ Focuses on new contract awards and solicitations, rather than modifications. ■ Requires that solicitations and contracts include Level 1 or Level 2 self-assessment requirements as a condition of the contract award. ■ DoD may include Level 2 (C3PAO) (instead of self-assessments) for applicable solicitations and contracts and as a condition to exercise an option period on a contract awarded before the effective date.	■ DoD may also include the requirement for Level 2 (C3PAO) in place of Level 2 (Self) for applicable DoD solicitations and contracts.
PHASE 2	**One calendar year after the start of Phase 1 - November 10, 2026**	
	■ Requires that solicitations and contracts include Level 2 (C3PAO) as a condition of contract award where applicable, but that DoD may delay inclusion of the requirement for Level 2 (C3PAO) to an option period instead of as a condition of award.	■ Also provides that DoD may include Level 3 (DIBCAC) for applicable solicitations and contracts.
PHASE 3	**One calendar year after the start of Phase 2 - November 10, 2027**	
	■ Requires that solicitations and contracts include the requirement for Level 2 (C3PAO) as a condition of contract award and as a condition to exercise an option period on a contract awarded after the effective date.	■ In addition, all applicable DoD solicitations and contracts must include the requirement for Level 3 (DIBCAC) as a condition of contract award; or DoD may delay the inclusion of requirement for Level 3 (DIBCAC) to an option period instead of as a condition of a contract award.
PHASE 4	**One calendar year after the start of Phase 3 - November 10, 2028**	
	■ Requires that solicitations and contracts include the requirement for Level 2 (C3PAO) as a condition of contract award and as a condition to exercise an option period on a contract awarded after the effective date.	

4 According to DoD, the phased implementation will help minimize financial impacts on contractors, allow contractors time to understand and implement CMMC requirements, provide time to train assessors, and limit disruptions on the supply chain.

6 Should I be doing anything to prepare?

The level of effort to become compliant will vary, but could be significant, depending on the scale of a contractor's covered systems and the maturity of its cybersecurity program and capabilities. If contractors and subcontractors are not already doing so, they should consider some of the following steps:

- Inventory covered systems relative to the CMMC Program to define in-scope assets under the Rules.
  - This includes certain products and services from external service providers.
- Develop a process for confirming subcontractor and external provider compliance under the Rules.
  - Contractors are required to confirm subcontractor status under the Rules. There are no specific requirements for how that confirmation is obtained. Options include screenshots from the subcontractor's entry in SPRS and a variety of certification approaches. This assessment of subcontractors could be done on a contract-by-contract basis, but a more efficient approach may be to integrate into a company's supplier qualification process if one exists.
- Assess cybersecurity program for gaps with current requirements and identify reasonable timeframes for addressing any such gaps. In addition to technical compliance, contractors need to implement the compliance program and personnel responsible for ongoing implementation of CMMC requirements.
- Assess budgeting needs to become compliant and maintain compliance with the desired CMMC Level, particularly if compliance will require significant uplifts in security programs and/or relevant solicitations and contracts will require third party assessments.

7 What new certifications will be required under CMMC?

All contractors must provide affirmation of compliance to help monitor and enforce accountability. These certification requirements are outlined as follows:

- If subject to Level 1 requirements, contractors must verify through an annual self-assessment that all requirements have been fully implemented and submit an affirmation in SPRS attesting that they have implemented and will maintain implementation of all applicable CMMC security requirements in their CMMC level for all information systems within the relevant CMMC assessment scope ("affirmation of continuous compliance").
- If subject to Level 2 requirements, after achieving conditional or final compliance, the contractor must submit an affirmation of continuing compliance in SPRS. Contractors must reaffirm continuing compliance with Level 2 Status annually, but only need to conduct a new assessment every three years. Contractors will need to consider what they need to do short of a full assessment to permit that affirmation of continuing compliance.
- If subject to Level 3 requirements, Contractors must submit an affirmation of continuing compliance with Level 2 and Level 3 requirements into SPRS after achieving Conditional and Final Level 3 Status annually. To maintain Level 3 Status, contractors must also obtain Level 2 and Level 3 Certification Assessments every three years.