# ABOUT CMMC

### Q1. What is CMMC trying to address?

**A1.** The defense industrial base (DIB) is the target of more frequent and complex cyberattacks. CMMC is a key component of the Department's expansive DIB cybersecurity improvement effort. The program is designed to help ensure that defense contractors and subcontractors are compliant with existing information protection requirements for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) and are protecting that sensitive unclassified information at a level commensurate with the risk from cybersecurity threats, including advanced persistent threats.

### Q2. Where can I find the 32 CFR CMMC Program rule?

**A2.** The 32 CFR CMMC Program Rule can be found here. (https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program)

### Q3. Where can I find the 48 CFR CMMC Acquisition rule?

**A3.** The 48 CFR CMMC Acquisition Rule can be found here. (https://www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of)

### Q4. Will companies need to comply with CMMC 1.0 after the revised program is implemented?

**A4.** No, there is only one CMMC Program. The requirements have been revised since the initial publication, often referred to as "CMMC 1.0".

### Q5. Why did the DoD initiate rulemaking for CMMC?

**A5.** Rulemaking under Title 32 CFR is required to formally establish the DoD CMMC Program in regulation, and separate rulemaking under Title 48 CFR is required to update contractual requirements in the Defense Federal Acquisition Regulation Supplement (DFARS) to implement the program.

### Q6. When will CMMC be required for Department of Defense contracts?

**A6.** CMMC will be implemented contractually in the DoD when the DFARS clause 252.204-7021 is revised, and 60 days after the 48 CFR rule is published as final in the Federal Register.

### Q7. Why did the Department revise CMMC?

**A7.** The Department revised CMMC in response to feedback from industry, Congress, and other stakeholders. The DoD initiated an internal review of the program to focus on enhancing CMMC by (1) reducing costs, particularly for small businesses; (2) increasing trust in the CMMC assessment ecosystem; and (3) clarifying and aligning cybersecurity requirements to existing federal requirements and commonly accepted standards. DoD designed the revised CMMC framework to meet these goals, align with FY 2020 congressional guidance.

### Q8. How much will it cost to implement CMMC?

**A8.** The cost of implementing CMMC depends on various factors, including the CMMC level, the complexity of the DIB company's unclassified network, and market forces. However, costs incurred to meet existing contract requirements for safeguarding information (DFARS 252.204-7012) are not considered part of the CMMC implementation cost.

### Q9. What resources are available to assist companies in complying with DoD cybersecurity requirements?

**A9.** The DoD provides various no-cost Cybersecurity-as-a-Service resources to reduce barriers to DIB community compliance and support contract cybersecurity efforts. The DoD CIO DIB Cybersecurity Program has compiled a list of these services that is available at dibnet.dod.mil under *DoD DIB Cybersecurity-As-A Service (CSaaS) Services and Support*.

## CMMC MODEL

### Q10. How will my organization know what CMMC level is required for a contract?

**A10.** Once CMMC is implemented, the DoD will specify the required CMMC level in the solicitation and the resulting contract.

### Q11. What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and CMMC?

**A11.** DoD requires defense contractors' compliance with NIST SP 800-171 security requirements through inclusion of DFARS clause 252.204-7012 in contracts. CMMC assessment requirements will be included in DoD solicitations when the revised Title 48 CFR CMMC acquisition rule (DFARS 252.204-7021) becomes effective. Defense contractors will be required to undergo a self-assessment or a third-party assessment to determine whether that defense contractor has met applicable NIST SP 800-171 requirements.

### Q12. What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172 and CMMC?

**A12.** NIST SP 800-172 provides security requirements designed to address advanced persistent threats and forms the basis for CMMC level 3 security requirements. Contractors must implement 24 requirements from NIST SP 800-172 when DoD identifies CMMC Level 3 as a contract requirement.

### Q13. The CMMC model uses NIST SP 800-171, Revision 2. Will the Department update the program to use NIST SP 800-171, Revision 3?

**A13.** The Department followed federal rulemaking guidelines when including NIST SP 800-171 Revision 2 in the Title 32 CFR CMMC rule. The Department will incorporate Revision 3 with future rulemaking. The Department has issued a class deviation to DFARS clause 252.204-7012 to allow contracting officials to assess against Revision 2 until Revision 3 has been incorporated through rulemaking. You can find more info on that deviation here.

### Q14. Will prime contractors and subcontractors be required to maintain the same CMMC level?

**A14.** No, a lower CMMC level may apply to the subcontractor if the prime only flows down limited information. Additionally, if a prime contractor requires a CMMC level 3 certification, then a CMMC level 2 certification is the minimum requirement for CUI flowed down to the subcontractor, unless otherwise specified in the contract.

### Q15. What is the difference between FCI and CUI?

**A15.** FCI is any information that is 'not intended for public release,' CUI is information that requires safeguarding and may also be subject to dissemination controls. FCI is defined in FAR clause 52.204-21, and CUI is defined in Title 32 CFR Part 2002. The Department's CUI Quick Reference Guide includes additional information on the marking and handling of CUI.

### Q16. Will the CMMC Program address proper marking of legacy FOUO information and CUI?

**A16.** Marking of legacy FOUO and CUI is outside the purview of the CMMC Program and the CMMC Program makes no change to information marking requirements. The CUI Program was established federally through Title 32 CFR Part 2002 and within DoD through DoD Instruction 5200.48. Not all, but some information previously marked as FOUO will qualify as CUI. Contactors should seek DoD guidance to understand which legacy FOUO information should be marked and controlled as CUI.

## ASSESSMENTS

### Q17. How does my company become a C3PAO?

**A17.** Interested organizations should refer to the CMMC AB website (currently Cyber AB) for additional information on becoming a candidate C3PAO.

### Q18. What is the difference between authorized and accredited C3PAOs.

**A18.** The only difference between authorization and accreditation is the status of the CMMC Accreditation Body. Prior to the CMMC AB achieving its full ISO/IEC 17011 compliance, the interim term "authorized" is used for C3PAOs.

### Q19. How frequently will assessments be required?

**A19.** Once CMMC is implemented through the Title 48 CFR rule, Level 1 self-assessments will be required on an annual basis and CMMC Levels 2 and 3 will be required every 3 years. An affirmation of continued compliance is required for all CMMC levels at the time of assessment and annually thereafter.

### Q20. Who will perform independent CMMC assessments?

**A20.** DoD will only accept CMMC Level 3 assessments provided by the DIBCAC and CMMC Level 2 assessments conducted by an authorized or accredited C3PAO. C3PAOs shall use only certified CMMC assessors to conduct CMMC assessments.

### Q21. Will my organization need to be independently assessed if it does not handle CUI?

**A21.** No, if a DIB company does not process, store, or transmit CUI but does handle FCI, then only a CMMC Level 1 self-assessment would be required. Contractors are required to safeguard information by inclusion of contract clauses such as FAR 52.204-21 (for FCI) or DFARS 252.204-7012 (for CUI). DoD's intent under the CMMC Program is to require assessment against the required cybersecurity standards (i.e., NIST SP 800-171) only when safeguarding of CUI is required. For some CUI, DoD will accept a self-assessment rather than requiring certification based on assessment by a C3PAO or the Government.

### Q22. Will CMMC independent assessments be required for classified systems and / or classified environments within the DIB?

**A22.** No, CMMC only applies to DIB contractors' nonfederal systems unclassified networks that process, store, or transmit FCI or CUI.

### Q23. Will the results of a DIB company's assessment be made public? Will the DoD be able to see assessment results?

**A23.** No, DIB companies' assessments will not be made public. However, the DoD will have access to assessment information.

### Q24. How much will CMMC certification assessment cost?

**A24.** The cost of a CMMC Level 2 certification assessment will depend upon several factors, including the complexity of the DIB company's unclassified network for the certification scope, and market forces. DIBCAC assessments required for CMMC Level 3 certification will be conducted free of charge.

### Q25. When will we know which requirements are considered "critical" and won't be allowed in a Plan of Actions and Milestones (POA&M)?

**A25.** Critical requirements are identified in the Title 32 CFR CMMC final rule section §170.21.

### Q26. How would a company deal with operational requirements where full CMMC implementation breaks required information system functionality?

**A26.** If an information system is not able to provide adequate information security, DoD CUI should not be processed, stored, or transmitted in or on that system.

### Q27. Can DoD contractors implement NIST SP 800-171 Revision 3?

**A27.** Yes, DoD contractors can implement NIST SP 800-171 Revision 3 at will. But the CMMC assessment will still be conducted against NIST SP 800-171 Revision 2 using NIST SP 800-171A (June 2018) per the DoD and CMMC Assessment Methodology.

### Q28. What NIST SP 800-171 Revision 2 requirements would have to be implemented that are not covered in NIST SP 800-171 Revision 3?

**A28.** Full compliance with NIST SP 800-171 Revision 3 does not automatically guarantee compliance with all aspects of NIST SP 800-171 Revision 2. To ensure compliance, contractors need to identify and implement any security requirements, and their assessment objectives, from NIST SP 800-171A (June 2018) that are not covered in NIST SP 800-171 Revision 3. This may include specific security requirements that were revised, removed, or altered in the transition from NIST SP 800-171 Revision 2 to NIST SP 800-171 Revision 3. Furthermore, NIST SP 800-171 Revision 3 includes numerous organization-defined parameters (ODP) – each ODP selection will impact the alignment with the corresponding security requirements or assessment objectives from NIST SP 800-171A (June 2018). It is important to document and demonstrate compliance with the revision specified in your contract to meet all applicable requirements.

### Q29. Does my cloud service provider (CSP) require FedRAMP authorization?

**A29.** Yes, if the product/service provided by the CSP is used to process, store, or transmit Controlled Unclassified Information (CUI), the Cloud Service Offering (CSO) must meet FedRAMP Moderate, or equivalency requirements as determined by DoD policy at the time of the assessment.

**Q30. An OSA stores CUI in a system provided by our Managed Service Provider. It is not a cloud offering. Does the MSP require its own CMMC assessment?**

**A30.** No, but because CUI is stored in the MSP's systems, the services provided are in scope for the OSA's CMMC assessment and shall be assessed as part of the assessment. The MSP must satisfy all security requirements related to the processing, storage, or transmission of CUI. The MSP is not required to have its own CMMC assessment but may elect to perform its own self-assessment or undergo a certification assessment. The MSP's assessment level and type need to be the same, or above, as the level and type specified in the OSA's contract with the DoD and cover those assets that are in scope for the OSA's assessment.

**Q31. We separately outsource our IT support to an MSP and our security tools are managed by a different MSSP. No CUI is with either vendor. Are they required to be assessed?**

**A31.** In both cases, the MSP and MSSP services provided are both considered ESPs are the services are assessed as a Security Protection Asset Critical.

**Q32. Our MSP uses cloud tools to collect asset inventory, perform vulnerability scans, administer some assets, etc. Is the MSP a CSP?**

**A32.** No. The use of cloud tools to deliver a service does not make the MSP a CSP.

**Q33. Our MSP remotely accesses our on-premises and cloud environments. CUI is stored in both environments. Does the MSP require a CMMC certification?**

**A33.** No, as long as CUI is not processed, stored, or transmitted on MSP systems.

**Q34. We store CUI in the cloud and our MSP administers the environment. Is the MSP a CSP?**

**A34.** It depends on the relationships between the CSP, the MSP, and the OSA. If the cloud tenant is subscribed/licensed to the OSA (even if the MSP resells the service), then the MSP is not a CSP. If the MSP contracts with the CSP and further modifies the basic cloud service, then the MSP is a CSP and must meet applicable FedRAMP or equivalency requirements. A Cloud Service Provider (CSP) means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

**Q35. CUI is processed, stored, and transmitted in a Virtual Desktop Infrastructure (VDI). Are the endpoints used to access the VDI in scope as CUI assets?**

**A35.** An endpoint hosting a VDI client is considered an Out-of-Scope Asset if it is configured to not allow any processing, storage, or transmission of CUI beyond the

Keyboard/Video/Mouse sent to the VDI client. Proper configuration of the VDI client must be verified. If the configuration allows the endpoint to process, store, or transmit CUI, the endpoint will be considered a CUI Asset and is in scope of the assessment.

# IMPLEMENTATION

### Q36. How will the DoD implement CMMC?

**A36.** Once the Title 32 CFR CMMC Program rule and the Title 48 CFR CMMC acquisition rule are effective, the DoD will implement CMMC requirements in 4 phases over a three-year period to reduce implementation risk. The phased implementation plan is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. It will also minimize financial impacts to defense contractors, especially small businesses, and disruption to the existing DoD supply chain.

Following this phased implementation plan, solicitations and resulting defense contracts involving the processing, storing, or transmitting of FCI or CUI on a nonfederal system will have a CMMC level and assessment type requirement that a contractor must meet to be eligible for a contract award.

### Q37. How can businesses best prepare for CMMC implementation?

**A37.** Whether your company has previously been awarded a DoD contract that includes DFARS clause 252.204-7012 or is brand new to DoD contracting, the best way to prepare for implementation of CMMC is to carefully conduct a self-assessment of your contractor-owned information systems to make sure you have implemented the necessary cybersecurity measures to comply with each requirement of FAR clause 52.204-21 or DFARS clause 252.204-7012. Review the appropriate security requirements and carefully consider whether they have been implemented to secure any contractor-owned information systems which will be used to process, store, or transmit DoD controlled unclassified information during contract performance. Before initiating an assessment, take corrective actions to meet any security requirements that necessitate implementation to comply with CMMC requirements. Companies may use cloud service offerings to meet the cybersecurity requirements that must be assessed as part of the CMMC requirement. The DoD CIO DIB Cybersecurity Program has compiled a list of current resources available at dibnet.dod.mil under DoD DIB Cybersecurity-as-a-Service (CSaaS) Services and Support.

### Q38. Will CMMC apply to non-U.S. companies?

**A38.** Yes, when CMMC requirements are identified in DoD solicitations, they will apply to all companies performing under the resulting DoD contract.

### Q39. Can non-U.S. citizens or organizations be part of the CMMC Ecosystem, e.g., C3PAOs?

**A39.** Individuals and organizations that meet all requirements established under the Title 32 CFR CMMC Program rule are eligible, as appropriate, to be members of the CMMC Ecosystem, regardless of nationality.

### Q40. Do foreign countries need to develop their own assessment and training organizations, then obtain CMMC Program acceptance agreements with the U.S.?

**A40.** No, foreign partners need not establish unique assessment, training, or a non-U.S. based CMMC program; rather, they can use the CMMC program established by the Title 32 CFR CMMC Program rule. For instance, the Cyber AB may accredit, as appropriate, international organizations that meet all requirements established under the Title 32 CFR CMMC Program rule. Non-U.S. companies may then choose to use either an approved U.S.-based or foreign-based C3PAO to assess them.

### Q41. Our corporate security team provides our SOC and monitors deployed security tools. They are not a part of our business unit or CAGE code, but we are all employees of the same company. Is the security team/SOC an External Service Provider?

Possibly. In this context, EXTERNAL can include organizations within the same corporate entity; they do not need to be independent third parties. According to the CMMC Program, Controlled Unclassified Information (CUI) or Security Protection Data (SPD) (e.g., log data, configuration data) must be processed, stored, or transmitted on the External Service Provider (ESP) assets to be considered an ESP (170.4). In this case, the SOC is handling SPD on behalf of the Organizational Subunit (OSA). The organizational structure within the company will determine if the SOC is external to the OSA. Since the SOC is at a different organizational level and is not covered by the same CAGE code, it is likely to be considered an ESP. For the SOC to be considered an ESP during an assessment, a “service description and customer responsibility matrix (CRM)” are required. It is also possible to assign a CAGE code and include the SOC in the assessment.