OFFICE OF THE CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF WAR
May 2026

CYBERSECURITY MATURITY MODEL CERTIFICATION PROGRAM (CMMC) FREQUENTLY ASKED QUESTIONS

Revision 2.3

Contents

Section A: ABOUT CMMC

A-Q1. When will CMMC assessments be required for Department contracts?

A-A1. The Department began incorporating CMMC assessment requirements in applicable procurements on November 10, 2025, when the revised Defense Federal Acquisition Regulation Supplement clause 252.204-7021 became effective. The first 12 months of implementation will primarily focus on self-assessments. For further information on the Department's phased implementation plan, see 32 Code of Federal Regulations 170.3(e) and https://www.waru.edu/acquipedia-article/cmmc-phased-implementation.

A-Q2. How much will it cost to achieve CMMC compliance?

A-A2. Costs incurred to implement existing contract requirements for safeguarding information (e.g., Defense Federal Acquisition Regulation Supplement clause 252.204-7012) are not considered part of the CMMC compliance cost. However, the cost of achieving CMMC compliance (i.e., self-assessment or certification) depends on various factors, including, but not limited to, the CMMC level required, the complexity of the defense industrial base company's unclassified network, the existing cybersecurity posture of the organization, and market forces of supply and demand.

A-Q3. What resources are available to assist companies in complying with Department cybersecurity requirements?

A-A3. The Department provides resources to help businesses who wish to enter the defense industrial base reach cybersecurity compliance.

- The CMMC Accreditation Body, currently the Cyber AB, has a marketplace of certified CMMC assessors, professionals, and registered practitioner organizations that companies can engage now to prepare for CMMC implementation: https://cyberab.org/marketplace
- The Warfighting Acquisition University offers free online cybersecurity training, including convenient micro-learning articles and videos about CMMC topics.
    - Visit https://www.waru.edu/cybersecurity/cyber-solutions to access free training on various cybersecurity topics, including courses on CMMC available under the 'CMMC Resources from the DoW CIO' drop-down menu.
    - Visit https://www.waru.edu/acquipedia?combine=cmmc&title=&field_functional_area_target_id=All&field_topic_area_target_id=All to access free CMMC micro-learning videos on a variety of CMMC topics.
- The Department of War-Defense Industrial Base Collaborative Information Sharing Environment website has a list of no-cost cybersecurity resources to reduce barriers to defense industrial base community compliance and support contract cybersecurity efforts at https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/ under "Policy, Standards, and Resources" then "DoD DIB Cybersecurity Capabilities and Support."
- The Department of War Office of Small Business Programs has compiled a list of resources on their website aimed at helping small- and medium-sized businesses understand security requirements and reach compliance: https://business.defense.gov/Resources/FAQs/

A-Q4. Who is the point of contact for general inquiries regarding the CMMC Program?

A-A4. General inquiries regarding the CMMC Program, model, or policy can be directed to the CMMC Program Management Office using the contact form on our website: https://dowcio.war.gov/CMMC/.

Inquiries regarding CMMC Third-Party Assessment Organization (C3PAO) application status should be directed to the CMMC Accreditation Body, currently the Cyber AB, at support@cyberab.org, or to the specific point of contact the individual has communicated with about the application process thus far.

Inquiries regarding CMMC Registered Practitioner (RP/RPA), CMMC Certified Instructor (CCI), CMMC Certified Professional (CCP), or CMMC Certified Assessor (CCA) application status should be directed to the Cybersecurity Assessor and Instructor Certification Organization (CAICO) at to https://support.isaca.org/s/, where individuals can submit a case, initiate a chat, or call Toll-free: +1-855-549-2047 (or https://support.isaca.org/s/international-toll-free-numbers).

Return to top of section

Return to Table of Contents

Section B: CMMC MODEL

B-Q1. How will my organization know what CMMC level is required for a contract?

B-A1. Once CMMC is implemented contractually, the Department will specify the required CMMC level in the solicitation and the resulting contract.

B-Q2. What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and CMMC?

B-A2. NIST SP 800-171 is the federal safeguarding standard for controlled unclassified information (CUI) required by 32 Code of Federal Regulations (CFR) Part 2002, which the Department implemented contractually through inclusion of Defense Federal Acquisition Regulation Supplement clause 252.204-7012 in applicable contracts. As of November 10, 2025, applicable contractors are required to undergo a Level 2 self-assessment to verify compliance with those NIST SP 800-171 Revision 2 requirements. Beginning November 10, 2026, CMMC Level 2 third-party assessments will be required for applicable contractors to verify compliance with these standards.

B-Q3. The CMMC model uses National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2. Will the Department update the program to use NIST SP 800-171, Revision 3?

B-A3. Yes, the Department will incorporate Revision 3 with future rulemaking. In the interim, the Department has issued a class deviation to Defense Federal Acquisition Regulation Supplement clause 252.204-7012 to maintain Revision 2 as the standard against which defense industrial base companies will be assessed until Revision 3 has been incorporated into the 32 Code of Federal Regulations CMMC Program rule through rulemaking. You can find more information on that deviation here: https://www.war.gov/News/Releases/Release/Article/3763953/department-of-defense-issues-class-deviation-on-cybersecurity-standards-for-cov/.

B-Q4. Can Department contractors implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 3?

B-A4. Yes. Companies can implement Revision 3 but must use the Department's Organization-Defined Parameters (ODPs) defined in the April 2025 memorandum, "Department of Defense Organization-Defined Parameters for National Institute of Standards and Technology Special Publication 800-171 Revision 3" found here: https://dodcio.defense.gov/Portals/0/Documents/CMMC/OrgDefinedParmsNISTSP800-171.pdf. Because CMMC assessments will be conducted against Revision 2 until the class deviation memo (see Q3 of this section) is withdrawn or otherwise superseded, defense industrial base companies must ensure any identified gaps between Revision 2 and Revision 3 are addressed.

B-Q5. What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172 and CMMC?

B-A5. 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 in addition to the 110 requirements found in NIST SP 800-171 when the Department identifies CMMC Level 3 as a contract requirement.

B-Q6. Will CMMC requirements flow down to subcontractors?

B-A6. Yes, CMMC requirements will flow down to subcontractors as outlined in 32 Code of Federal Regulations 170.23. The required CMMC level is based on the type of data—Federal Contract Information (FCI) or Controlled Unclassified Information (CUI)—that will be processed, stored, or transmitted on a contractor's information system during the performance of a Department of War contract. Subcontractors handling FCI or CUI are subject to safeguarding requirements. Note that when the prime contract requires CMMC Level 3, the minimum flow-down requirement is a CMMC Level 2 independent assessment, unless the Government provides specific contractual guidance (e.g., a Security Classification Guide).

B-Q7. What is the difference between Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)?

B-A7. FCI and CUI are information that is 'not intended for public release.' However, CUI requires additional safeguarding and may also be subject to dissemination controls. FCI is defined in Federal Acquisition Regulation clause 52.204-21, and CUI is defined in 32 Code of Federal Regulations Part 2002. The Department's CUI Quick Reference Guide at https://www.dodcui.mil/ includes additional information on the marking and handling of CUI. CMMC makes no changes to CUI definitions or safeguarding requirements.

B-Q8. Is encrypted Controlled Unclassified Information (CUI) still considered to be CUI?

B-A8. In accordance with 32 Code of Federal Regulations Part 2002, CUI remains controlled until it is formally decontrolled. As such, encrypted CUI data retains the control designation given to the plain text counterpart. While it is true that certain risks (e.g., transmission across unsecured, "common carrier" networks) are accepted for cipher text that would not be accepted for plain text, this does not mean the original, controlled information, nor the data (plain or cipher text) representing it, is considered decontrolled. When properly implemented in accordance with National Institute of Standards and

Technology Special Publication 800-88, "Guidelines for Media Sanitization," cryptographic erase is acceptable for sanitation of controlled media before disposal or reuse.

Return to top of section

Return to Table of Contents

Section C: ASSESSMENTS

C-Q1. How frequently will assessments be required?

C-A1. Level 1 self-assessments will be required on an annual basis, and assessments for CMMC Levels 2 and 3 will be required every three years. An affirmation of continued compliance is required for all CMMC levels at the time of assessment and annually thereafter. Please reference 32 Code of Federal Regulations 170.3(e) for details on the Department's timeline for phased implementation of CMMC requirements in applicable procurements.

C-Q2. Will my organization need to be independently assessed if it does not handle Controlled Unclassified Information (CUI)?

C-A2. No, if a defense industrial base company does not process, store, or transmit CUI, it does not need an independent assessment. If the company handles Federal Contract Information only, a CMMC Level 1 self-assessment is required.

C-Q3. Will CMMC independent assessments be required for classified systems and/or classified environments within the defense industrial base?

C-A3. No. CMMC only applies to defense industrial base contractors' nonfederal unclassified information systems that process, store, or transmit Federal Contract Information or Controlled Unclassified Information.

C-Q4. Will the results of a company's assessment be made public? Will the Department be able to see assessment results?

C-A4. The public will not have access to a listing of defense industrial base companies that have completed their CMMC self-assessments or received CMMC certificates. Such information is available to the Department officers leading procurement activities.

A company can view their own scores and status in the Supplier Performance Risk System (SPRS). Suppliers may print verification of their status from SPRS to share with their Primes. Subcontractors may voluntarily share their CMMC Status, assessment scores, or certificates to facilitate business teaming arrangements. The Department expects that defense contractors will share information about CMMC Status with other defense industrial base members to facilitate effective teaming arrangements when bidding for Department contracts.

C-Q5. Does my company's administrative office or manufacturing facility require a specific Commercial and Government Entity (CAGE) code for that location to submit and comply with CMMC?

C-A5. No, a specific CAGE code for each location is not required. An existing CAGE code within the company's hierarchy may be used to submit the appropriate assessment

identified by the CMMC Unique Identifier (UID). The CMMC Assessment Boundary scope for a CMMC UID is documented in the System Security Plan and network diagrams association with that assessment. The Department of War (DoW) Contracting Officer will verify the company's CMMC Status in SPRS using the CMMC UID(s) provided in the proposal. CAGE codes (including the Highest-Level Owner) are only to enforce authorized access to the data in the Supplier Performance Risk System (SPRS); to perform annual affirmations; and for metrics purposes.

Any company information systems not represented by the CMMC UID(s) provided for a solicitation are considered non-compliant and cannot be used to process, store, or transmit FCI or CUI during contract performance.

C-Q6. If a company is a Joint Venture (JV), does the JV need its own CMMC Status, or can the CMMC Status of each JV partner suffice?

C-A6. Offerors, including JVs, must identify all CMMC Unique Identifiers (UIDs) in their proposal that will be used to process, store, or transmit Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) during contract performance. All processing, storing, or transmitting of FCI and CUI must be limited to the CMMC UIDs identified in the proposal.

The identified CMMC UIDs may apply to individual JV members or to the JV itself, if the JV operates using systems and networks that serve multiple members. In either case, the CMMC UIDs must represent the scope of the systems and networks used during contract performance.

C-Q7. Which requirements are considered "critical" and are not allowed in a Plan of Action and Milestones (POA&M)?

C-A7. Critical requirements are identified in 32 Code of Federal Regulations 170.21.

C-Q8. What happens after a Plan of Action and Milestones (POA&M) Closeout Assessment if one or more of the security requirements on the POA&M still aren't met?

C-A8. During the 180-day period after achieving a Conditional CMMC Status, a POA&M Closeout Assessment can only be finalized in the CMMC Enterprise Mission Assurance Support System (eMASS) one time. In the case where one or more security requirements are still NOT MET, the Conditional CMMC Status will be terminated once the POA&M Closeout Assessment is finalized in CMMC eMASS, and the Organization Seeking Assessment will have to begin again with a new assessment to achieve a CMMC Status. If a POA&M Closeout Assessment is not finalized in CMMC eMASS within 180 days of the CMMC Status Date, the Conditional CMMC Status will automatically expire.

C-Q9. What is the difference between an Operational Plan of Action (OPA) and a Plan of Action and Milestones (POA&M)?

C-A9. OPAs are measures implemented to manage risks or vulnerabilities, such as applying patches, addressing temporary deficiencies, or performing routine system maintenance. OPAs are not tied to a specific timeline for completion and are typically used to address vulnerabilities or deficiencies that arise after the initial implementation of security requirements.

Under the CMMC framework, POA&Ms are formal plans that identify cybersecurity gaps the Organization Seeking Assessment must address to achieve CMMC compliance. These gaps must be resolved within 180 days, as outlined in 32 Code of Federal Regulations 170.21.

When a significant change occurs in an information system that affects the satisfaction of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 security requirements, the appropriate course of action—whether to create a POA&M or an OPA—depends on the nature and timing of the change. If the significant change introduces a temporary deficiency or vulnerability after the system was initially compliant, an OPA may be created to document the remediation plan. However, if the significant change is identified during a CMMC assessment and results in a security requirement being assessed as NOT MET, a POA&M must be created to address the gap within the 180-day remediation window. For more information, please reference FAQ C-Q8.

For detailed definitions, refer to 32 Code of Federal Regulations 170.4.

C-Q10. I have entered my company's CMMC self-assessment into the Supplier Performance Risk System (SPRS) and have received the following error(s) for 'CMMC Status Type': No CMMC Status or No CMMC Score. How can I fix this?

C-A10. There are a few reasons you may be getting the "No CMMC Score" or "No CMMC Status" landing page after attempting to submit your assessment results into the SPRS platform.

No Score:

- You have received a "No Score" because you marked "Not Met" for security requirement CA.L2-3.12.4 – SYSTEM SECURITY PLAN.

  The absence of an up-to-date system security plan at the time of the assessment will result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204–7012.' (Please see 32 Code of Federal Regulations (CFR) 170.24 for more details on the CMMC Level 2 scoring methodology, with reference to 170.24I(2)(i)(B)(5)).

No Status:

- The assessment score divided by the total number of CMMC Level 2 security requirements is less than 0.8.
- You have security requirements that, in accordance with 32 CFR 170.21, are not permitted on a Plan of Action and Milestones (POA&M) for the purposes of achieving a certification.
    - Please carefully review each security requirement for which you have provided a POA&M to ensure each of those requirements are not one of the (6) prohibited in accordance with 32 CFR 170.21(a)(2)(iii).
    - You may reference the 32 CFR 170.24 CMMC Scoring Methodology for further detail regarding the security requirements of your assessment.

C-Q11: Are CMMC assessments required for organizations that only handle hard-copy Controlled Unclassified Information (CUI)?

C-A11. Based on the lesser risk associated with paper-only scenarios, organizations that only handle hard-copy CUI data are not required to complete a CMMC third-party assessment. However, the organization may elect to conduct a CMMC self-assessment, or a third-party assessment, on the environment for a higher degree of assurance.

Nonetheless, contractors and subcontractors are required to protect hard-copy CUI. When Defense Federal Acquisition Regulation Supplement clause 252.204-7012 is included in a contract and flowed down to applicable subcontracts, all organizations that process, store, or transmit CUI (including in hard-copy form) remain obligated to safeguard that information in accordance with the applicable security requirements of National Institute of Standards and Technology Special Publication (NIST SP) 800-171 and DoD Instruction 5200.48 (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF?ver=2020-03-06-100640-800).

Additionally, if a contractor or subcontractor that was only provided hard-copy CUI plans to place that CUI on an information system digitally (e.g., by scanning, entering, photographing, uploading, printing, or emailing), that information system is expected to satisfy applicable CMMC assessment requirements prior to the CUI being placed on the system.

For organizations that handle paper CUI in addition to processing, storing, or transmitting CUI on a contractor-owned information system, the necessary CMMC assessment will address both the paper CUI and the digital CUI, in accordance with the applicable NIST SP 800-171 security requirements.

C-Q12: What qualifies as a "significant change" that would require an Organization Seeking Assessment to undergo a new evaluation under the CMMC Program?

C-A12. The CMMC Program's three-year assessment cycle and annual affirmation processes are designed to accommodate changes to your environment. Organizations must focus on maintaining compliance with the CMMC security requirements for their CMMC Status and annually affirm that continuing compliance. The decision of whether a change is significant enough to require a reassessment is the responsibility of the Affirming Official, who bears the legal and contractual risk of continued compliance and may benefit from consultation with authorized independent consultants.

The following CMMC security requirements specifically address changes:

- Control Controlled Unclassified Information flow through the environment (AC.L2-3.1.3)
- Actively manage changes (CM.L2-3.4.3)
- Perform security impact analysis for changes (CM.L2-3.4.4)
- Conduct risk assessments (RA.L2-3.11.1)
- Utilize plans of action to reduce or eliminate deficiencies/vulnerabilities (CA.L2-3.12.2)
- Monitor security controls continuously (CA.L2-3.12.3)
- Update the System Security Plan (SSP) (CA.L2-3.12.4)

Architectures vary, and it is not practical to present a single prescriptive definition of significant change. This FAQ provides an example of each possible case: (1) a change that clearly requires reassessment, (2) a change that does not require reassessment, and (3) a change that requires careful evaluation and consultation with the Affirming Official.

1. A reassessment is required if any security requirement or assessment objective was assessed as N/A (or assessed as MET by virtue of N/A) but, after a change, is now applicable since that security requirement or assessment objective has never been assessed. For example, if a WiFi capability is added to a system that achieved its CMMC Status while not allowing WiFi, then reassessment is required because AC.L2-3.1.16 and AC.L2-3.1.17 were N/A and are now applicable.

2. Routine changes to maintain security posture, such as patching or upgrading a security solution for a new like solution with the same or better security capabilities (e.g., replacing an old Federal Information Processing Standards (FIPS) 140.2 firewall with a FIPS 140.3 firewall), are expected changes covered by the security requirements above and are not considered significant changes.
3. Major functionality changes, changes that require a new security approach or design not present in the previously assessed system and its SSP, or changes which reduce or remove support for a CMMC security requirement, require additional consideration. For example, if a Windows-based environment is merged into a LINUX-based environment, and both environments have an active CMMC Status, then the resulting system may have continuing compliance with the lower of the two CMMC Statuses. However, without a CMMC Status on the Windows-based environment, a reassessment is required, since the Windows systems and security tools have not been assessed and do not exist in the LINUX-based environment. The determining factor is whether the resulting environment includes systems, configurations, or security tools that have not previously been assessed.

It is important to consider that the next three-year assessment will evaluate whether each of these changes have been properly managed according to CMMC security requirements and performed as stated in the SSP. Failure to sufficiently demonstrate adherence to the previous SSP may result in a future failed assessment.

Return to top of section

Return to Table of Contents

Section D: IMPLEMENTATION

D-Q1. How will the Department implement CMMC?

D-A1. The first phase of CMMC implementation began on November 10, 2025. CMMC assessment requirements will be implemented using four phases over a three-year period, as described in 32 Code of Federal Regulations 170.3(e). The phases add CMMC Level requirements incrementally, starting with Level 1 and Level 2 self-assessments in Phase 1, and ending with full implementation of program requirements in Phase 4. 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 defense supply chain.

D-Q2. How can businesses best prepare for CMMC?

D-A2. Whether a company has previously been awarded a defense contract that includes Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 or is brand new to defense contracting, the best way that company can prepare for CMMC is by carefully conducting a self-assessment of their contractor-owned information system(s) to make sure they have implemented the necessary cybersecurity measures to comply with each requirement of Federal Acquisition Regulation clause 52.204-21 (for Federal Contract Information) or DFARS clause 252.204-7012 (for Controlled Unclassified Information). If the

self-assessment identifies any unmet requirements, companies should take corrective action to address those gaps and fully implement the necessary security measures before initiating a CMMC assessment.

D-Q3. Will CMMC apply to non-U.S. companies?

D-A3. Yes. When CMMC requirements are identified in Department solicitations, they will apply to all companies performing under the resulting contract, whether domestic or international.

D-Q4. Can non-U.S. citizens or organizations be part of the CMMC Ecosystem, e.g., Authorized CMMC Third-Party Assessment Organizations?

D-A4. Yes. Individuals and organizations that meet all requirements established under the Title 32 Code of Federal Regulations CMMC Program rule are eligible, as appropriate, to apply to become members of the CMMC Ecosystem, regardless of nationality or country of origin.

D-Q5. Starting November 10, 2025, does Department policy require program managers (PMs) to include CMMC Level 2 independent assessment requirements in a solicitation if the contractor will handle Controlled Unclassified Information (CUI) from the Defense Organizational Index Grouping?

Policy referenced: https://dodprocurementtoolbox.com/uploads/DOPSR_Cleared_OSD_Memo_CMMC_Implementation_Policy_d26075de0f.pdf)

D-A5. No. during Phase 1, the Department's intent is that all solicitations focus on including the right CMMC self-assessment requirement, which means CMMC Level 1 when only Federal Contract Information will be processed/stored/transmitted and CMMC Level 2 (Self) when any CUI will be processed/stored/transmitted in contractor-owned information systems.

While it is true that the phases are codified in 32 Code of Federal Regulations (CFR) Part 170 with language that provides PMs some discretion to include CMMC Level 2 independent assessment requirements in solicitations during Phase 1, it is not required. Practically speaking, this means the policy allows for (and the Department anticipates) that during Phase 1, there will be some solicitations issued that only include a CMMC Level 2 self-assessment requirement, even in cases when the CUI to be shared comes from the Defense Organizational Index Group.

PMs may also discuss with their Contracting Officer the possibility of including the CMMC clause with the requirement to have a CMMC Level 2 self-assessment at the time of award but specifying that a CMMC Level 2 independent assessment will be required at the time of any option period exercise.

PMs should only make use of the discretion provided in 32 CFR 170.3(e) to include a CMMC Level 2 independent assessment during Phase 1 when, informed by adequate market research, there is reason to believe that enough qualified offerors (including their subcontractors) exist to provide for adequate competition to meet the solicitation requirement.

Return to top of section

Return to Table of Contents

Section E: EXTERNAL SERVICE PROVIDERS

E-Q1. Must my Cloud Service Provider (CSP) meet Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline requirements if it processes, stores, or transmits Controlled Unclassified Information (CUI)?

E-A1. Yes. Per Defense Federal Acquisition Regulation Supplement clause 252.204-7012, if the contractor intends to use a CSP to store, process, or transmit CUI in the performance of a contract, the contractor shall require and ensure that the CSP meets security requirements equivalent to those established by the Government for the FedRAMP Moderate baseline. This can be met by using a FedRAMP-Moderate-authorized service provider, or a provider that meets the requirements for equivalency as specified in the Department's December 2023 memo, "Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings" (https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf)

E-Q2. Can a non- Federal Risk and Authorization Management Program (FedRAMP) Moderate cloud service offering store encrypted Controlled Unclassified Information (CUI) data?

E-A2. No. If a contractor intends to use an external Cloud Service Provider in the performance of a Department of War contract to store encrypted CUI data, the contractor shall require and ensure that the Cloud Service Provider meets security requirements equivalent to those established for the FedRAMP Moderate baseline.

E-Q3. An Organization Seeking Assessment (OSA) stores Controlled Unclassified Information (CUI) in a system provided by a Managed Service Provider (MSP) that is not a cloud offering. Does the MSP require its own CMMC assessment?

E-A3. No. 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. If the MSP chooses to attain a CMMC certification to simplify the OSA's assessment, the assessment level and type need to be the same, or above, as the level and type specified in the OSA's contract with the Department and cover those assets that are in scope for the OSA's assessment.

E-Q4. We separately outsource our IT support to an External Service Provider (ESP) that is a Managed Service Provider (MSP), and our security tools are managed by a different ESP that is a Managed Security Service Provider (MSSP). No Controlled Unclassified Information (CUI) is sent to either vendor. Are they required to be assessed?

E-A4. Yes. In a scenario where IT support is handled by an MSP and where security protection data is handled by an MSSP, both the MSP and the MSSP qualify as ESPs and will be assessed as part of the Organization Seeking Assessment's assessment scope against applicable security requirements. The ESPs do not require their own CMMC certification.

E-Q5. We store Controlled Unclassified Information (CUI) in the cloud, and our Managed Service Provider (MSP) administers the environment. Is the MSP a Cloud Service Provider (CSP)?

E-A5. It depends on the relationships between the CSP, the MSP, and the Organization Seeking Assessment. If the cloud tenant is subscribed/licensed to the Organization Seeking Assessment, even if the MSP resells the service, then the MSP is not a CSP. If the MSP contracts with the CSP and modifies the basic cloud service, then the MSP may be a CSP and must meet applicable Federal Risk and Authorization Management Program or equivalency requirements.

Return to top of section

Return to Table of Contents

Section F: SCOPING

F-Q1: Controlled Unclassified Information (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?

F-A1. 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.

F-Q2: Is the endpoint used to access a Virtual Desktop Infrastructure (VDI) required to be "in scope" for National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 when implementing its controls to protect Controlled Unclassified Information (CUI), or can the endpoint be considered "out of scope" if CUI remains entirely within the VDI instance?

F-A2: Yes, the endpoint could be considered "out of scope," but this depends on how the VDI and VDI server are implemented. Some VDI systems include features that cache data on the client device or allow the virtual desktop to connect to the local machine's file system, printers, or other resources for user convenience. For NIST SP 800-171 compliance, these features must be disabled on the server side to ensure that unmanaged endpoints cannot mount drives, print files, or perform other actions that invoke system protocols (e.g., file handling, print spooling) beyond the basic VDI protocol (e.g., transmitting only video, keyboard, and mouse data).

If the VDI is properly configured to prevent copying (including screenshots), saving, or printing CUI on the endpoint (except within a NIST SP 800-171-compliant system), and multifactor authentication is implemented for access to the VDI server, the endpoint would not be considered "in scope."

To achieve this:

- The virtual desktop server must be configured to block copy-paste, file transfers, or any other data exchange across the session.
- The VDI should only transmit video, keyboard, and mouse data.
- Users must log into the virtual desktop and handle CUI entirely within the session.

- Multifactor authentication to the VDI server must be separate from the unmanaged client, such as using a hardware-based one-time password token or Public Key Infrastructure token with a password/Personal Identification Number.
- Only authorized users should be allowed to access the virtual desktop environment, and access should be restricted to allowable locations.

By ensuring these configurations, the endpoint used to access the VDI can remain "out of scope" for NIST SP 800-171 and CMMC compliance.

F-Q3: Can encryption alone create logical separation for a network within a CMMC Assessment Scope?

F-A3. No. Logical separation occurs when data transfer between physically connected assets (wired or wireless) is prevented by non-physical means such as software or network assets (e.g., firewalls, routers, Virtual Private Networks, Virtual Local Area Networks). While properly implemented encryption provides necessary confidentiality protection, it does not, by itself, prevent data transfer or enforce the security boundary of a network.

F-Q4: Our enclave does not have a direct internet connection. Instead, it relies on enterprise networking components residing outside of the enclave. All Controlled Unclassified Information (CUI) data is properly encrypted before leaving our enclave. Must the enterprise networking components be brought into our enclave's CMMC Assessment Scope?

F-A4: No. So long as the enclave is otherwise logically separated from the greater enterprise network, the transmission of properly encrypted CUI data does not incur an extension of the CMMC Assessment Scope to include the enterprise networking components.

F-Q5: How do I properly handle changes to my system while maintaining continued CMMC compliance?

F-A5: For any changes to your environment that may impact processing, storing, or transmitting Federal Contract Information or Controlled Unclassified Information (CUI), security requirements, or CMMC Assessment Scope, you should:

1. **Before Implementation: Evaluate the Change**
    a. Perform security impact analysis per CM.L2-3.4.4 (if a new risk is identified during this analysis that is not addressed in the existing System Security Plan (SSP), then you probably have a significant change)
    b. Assess effects on CUI flow per AC.L2-3.1.3
    c. Document in your change management process per CM.L2-3.4.3
    d. Review planned change with Affirming Official to gain consensus on whether change will impact continuing compliance
2. **During Implementation: Document in Operational Plan of Action**
    a. Describe the change and any temporary risks per CA.L2-3.12.2
    b. Identify personnel responsible for implementation
    c. Track progress
3. **After Implementation: Update SSP**

a. Document the completed change per CA.L2-3.12.4
b. Update all sections affected by the change
c. Review changes with Affirming Official prior to next annual affirmation to ensure agreement on continuing compliance

Document Revision History

Office of Department of War Chief Information Officer/CMMC Program Management Office

Version No.	Action Date	Summary of Revisions
1	10/14/2024	Initial release of document
2	9/25/2025	Major overhaul of document to reflect the Title 48 CFR Part 204 effective date and updated FAQs received to CMMC inquiries mailbox; updated formatting
2.1	11/17/2025	Addition of 4 new FAQs (B-Q8, C-Q8, E-Q2, and E-Q7); updated formatting to more easily differentiate between document sections
2.2	1/5/2026	Addition of 3 new FAQs (C-Q10, C-Q11, C-Q12)
2.3	4/29/2026	Addition of micro-learning video links to A-A1 and A-A-3; addition of new CAICO contact information to A-A4; addition of new Section (F: Scoping); restructuring of existing FAQs in Sections C and E to new Section F (now F-Q1-4); addition of clarifying sentence at end of B-A8; addition of 3 new FAQs (C-Q6, C-Q11, F-Q5)