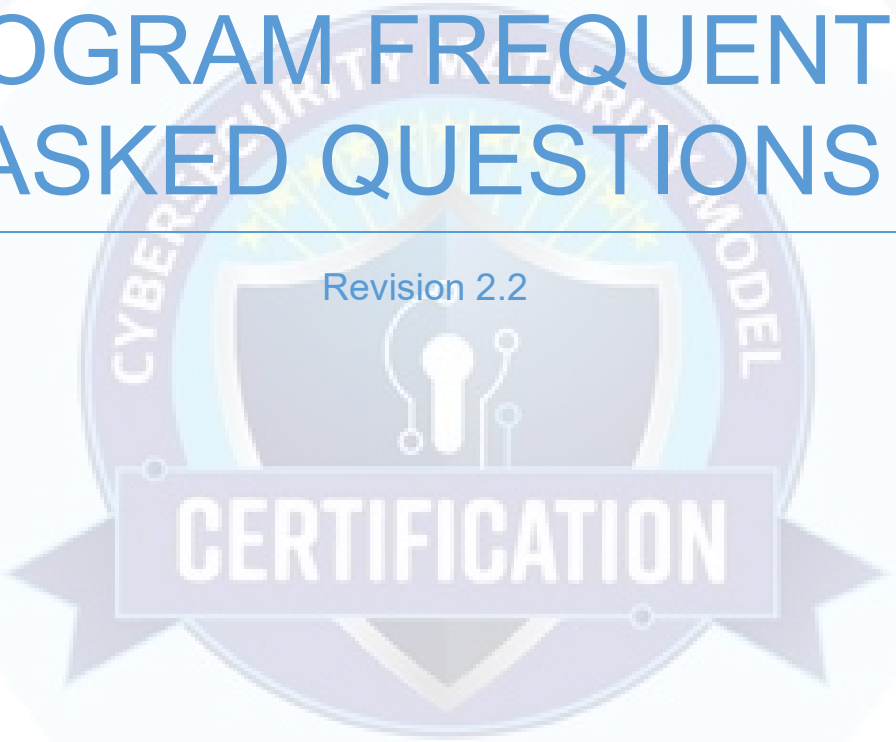
OFFICE OF THE CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF WAR (DoW OR DEPARTMENT)
**January 2026**

# CYBERSECURITY MATURITY MODEL CERTIFICATION PROGRAM FREQUENTLY ASKED QUESTIONS

Revision 2.2



# Contents

# Section A: ABOUT CMMC

### A-Q1. When will Cybersecurity Maturity Model Certification (CMMC) assessments be required for Department contracts?

**A-A1.** The Department will begin to incorporate CMMC assessment requirements in applicable procurements on November 10, 2025, when the revised Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7021 becomes effective. The first 12 months of implementation will primarily focus on self-assessments. For further information on the Department's phased implementation plan, please see 32 Code of Federal Regulations (CFR) 170.3(e).

### 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., DFARS 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 (DIB) 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 DIB reach cybersecurity compliance.

- The DoW CIO DIB Cybersecurity Program has compiled a list of no-cost Cybersecurity-as-a-Service resources to reduce barriers to DIB community compliance and support contract cybersecurity efforts at dibnet.dod.mil under *DoD DIB Cybersecurity-As-A Service (CSaaS) Services and Support*.
- 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 Defense Acquisition University offers free online CMMC and cybersecurity training: https://www.dau.edu/cybersecurity/training

- The Defense Acquisition University also offers a drop-down for CMMC web events: https://www.dau.edu/cybersecurity/cyber-solutions (click the drop-down labeled “CMMC Resources from the DoD CIO”)
- DoW's Office of Small Business Programs has compiled a list of resources on their website that are 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://dodcio.defense.gov/cmmc/Contact/.

Inquiries regarding CMMC Registered Practitioner (RP/RPA) and 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 Certified Professional (CCP) or CMMC Certified Assessor (CCA) application status should be directed to the Cybersecurity Assessor and Instructor Certification Organization (CAICO), at support@cyberab.org, or to the specific point of contact the individual has communicated with about the application process thus far.

***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 CFR Part 2002, which the Department implemented contractually through inclusion of DFARS clause 252.204-7012 in applicable contracts. Beginning November 10, 2025, and following the phased implementation plan outlined in 32 CFR 170.3(e), applicable contractors will be required to undergo a Level 2 self-assessment or a CMMC third-party assessment to verify compliance with those NIST SP 800-171 Revision 2 requirements.

### B-Q3. The CMMC model uses NIST 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 DFARS clause 252.204-7012 to maintain Revision 2 as the standard against which DIB companies will be assessed until Revision 3 has been incorporated into the 32 CFR CMMC Program rule through rulemaking. You can find more information on that deviation here: https://www.defense.gov/News/Releases/Release/Article/3763953/department-of-defense-issues-class-deviation-on-cybersecurity-standards-for-cov/.

### B-Q4. Can Department contractors implement NIST 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 (Q3 of this section) is withdrawn or otherwise superseded, DIB 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 CFR 170.23. The required CMMC level is based on the type of data—Federal Contract Information (FCI) or CUI—that will be processed, stored, or transmitted on a contractor's information system during the performance of a DoW 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 CMMC Level 2 (C3PAO), unless the Government provides specific contractual guidance (e.g., a Security Classification Guide).

### B-Q7. What is the difference between FCI and 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 (FAR) clause 52.204-21, and CUI is defined in 32 CFR 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 CUI still considered to be CUI?

**B-A8.** In accordance with 32 CFR 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.

***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 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. Please reference 32 CFR 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 CUI?

**C-A2.** No, if a DIB company does not process, store, or transmit CUI, it does not need an independent assessment. If the company handles FCI 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 DIB?

**C-A3.** No, CMMC only applies to DIB contractors' nonfederal unclassified information systems that process, store, or transmit FCI or CUI.

### C-Q4. Will the results of a DIB 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 DIB 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 DIB 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. Another existing CAGE in the company's hierarchy may be used to submit the appropriate assessment identified by the CMMC Unique Identifier (UID). The CMMC UID must contain the scope that covers the assessment. CAGE codes (including the Highest-Level Owner) are only for metrics purposes; to enforce authorized access to the data in SPRS; and to perform annual affirmations.

### C-Q6. Which requirements are considered "critical" and are not allowed in a Plan of Actions and Milestone (POA&M)?

**C-A6.** Critical requirements are identified in 32 CFR 170.21.

### C-Q7. What happens after a POA&M Closeout Assessment if one or more of the security requirements on the POA&M still aren't met?

**C-A7.** 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-Q8. What is the difference between an Operational Plan of Action (OPA) and a POA&M?

**C-A8.** Operational Plans of Action (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 CFR 170.21.

When a significant change occurs in an information system that affects the satisfaction of NIST 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-Q7.

For detailed definitions, refer to 32 CFR 170.4.

### C-Q9. I have entered my company's CMMC self-assessment into 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-A9.** 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 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 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-Q10: Are CMMC assessments required for organizations that only handle hard-copy CUI?

**C-A10.** No. Organizations that **only handle hard-copy CUI** should **not** be required to complete a CMMC Assessment. CMMC assessment requirements address cybersecurity-related risk to CUI and apply only when the CUI is processed, stored, or transmitted on a contractor-owned information technology system. Nonetheless, contractors are required to protect the hardcopy CUI. Per DoDI 5200.48, paragraph 1.1(b), any contractor or subcontractor that receives CUI is required to safeguard that information with Government training and safeguarding requirements.

Additionally, if a contractor who was only provided hardcopy CUI plans to place the hardcopy CUI on an information technology system (e.g., scanned, entered, photographed, uploaded, printed, emailed), then that information technology system is subject to the 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 in a contractor-owned information technology 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. For further information about DoD policy regarding safeguarding CUI, refer to DoDI 5200.48 [www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF?ver=2020-03-06-100640-800].

### C-Q11: Can encryption alone create logical separation for a network within a CMMC Assessment Scope?

**A-Q11.** 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., firewall, routers, VPNs, VLANs). While properly implemented encryption provides necessary confidentiality protection, it does not, by itself, prevent data transfer or enforce the security boundary of a network.

### C-Q12: Our enclave does not have a direct internet connection. Instead, it relies on enterprise networking components residing outside of the enclave. All CUI data is properly encrypted before leaving our enclave. Must the enterprise networking components be brought into our enclave's CMMC Assessment Scope?

**A-Q12:** 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.

***Return to top of section***

***Return to Table of Contents***

## Section D: IMPLEMENTATION

### D-Q1. How will the DoD implement CMMC?

**D-A1.** Beginning November 10, 2025, the Department will implement CMMC requirements in 4 phases over a three-year period, as described in 32 CFR 170.3(e). 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. The first 12 months of implementation focus primarily on CMMC Level 1 and 2 self-assessments.

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

**D-A2.** Whether a company has previously been awarded a defense contract that includes 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 FAR clause 52.204-21 (for FCI) or DFARS clause 252.204-7012 (for CUI). 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-Q5. Can non-U.S. citizens or organizations be part of the CMMC Ecosystem, e.g., C3PAOs?

**D-A5.** Yes. Individuals and organizations that meet all requirements established under the Title 32 CFR CMMC Program rule are eligible, as appropriate, to apply to be members of the CMMC Ecosystem, regardless of nationality or country of origin.

### D-Q6. Starting November 10, 2025, does Department policy (ref: https://dodprocurementtoolbox.com/uploads/DOPSR_Cleared_OSD_Memo_CMMC_Implementation_Policy_d26075de0f.pdf) require Program Managers to include CMMC Level 2 (C3PAO) in a solicitation if the contractor will handle CUI from the Defense Organizational Index Grouping?

**D-A6.** 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 FCI 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 CFR Part 170 with language that provides PMs some discretion to include CMMC Level 2 (C3PAO) 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 (C3PAO) 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 (C3PAO) 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 CUI?**

**E-A1.** Yes. Per DFARS 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-FedRAMP Moderate cloud service offering store encrypted CUI data?**

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

**E-Q3. An Organization Seeking Assessment (OSA) stores 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 an MSP), and our security tools are managed by a different ESP (that is a Managed Security Service Provider). No 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 OSA's assessment against applicable security requirements. The ESPs do not require their own CMMC certification.

**E-Q5. We store CUI in the cloud and our MSP administers the environment. Is the MSP a CSP?**

**E-A5.** 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 modifies the basic cloud service, then the MSP may be a CSP and must meet applicable FedRAMP or equivalency requirements.

### E-Q6. 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?

**E-A6.** 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.

### E-Q7: Is the endpoint used to access a VDI required to be "in scope" for NIST SP 800-171 when implementing its controls to protect CUI, or can the endpoint be considered "out of scope" if CUI remains entirely within the VDI instance?

**E-A7:** 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/PIN.
- 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.

***Return to top of section***

***Return to Table of Contents***

## Document Revision History

Department / Organization Title

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) |