Cybersecurity Maturity Model Certification (CMMC)

Level 2 Self Certification

Frequently Asked Questions (FAQs)

Current as of: 19 Aug 2026

Contents

Note: On July 13, 2026, the Department of War announced the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements. All CMMC Phase I, level 1 and level 2 self-assessment requirements remain firmly in place.

1. Self-Assessment and Certification

Q1. What is the reality of a self-assessment being successful and compliant for a company to do internally, considering the complexity of Level 2 requirements?

A1. The process is extensive and requires strict adherence to NIST SP 800-171 Rev 2. The DoW acknowledges the burden; the Final Rule estimates a significant time and cost investment for small entities to conduct a Level 2 Self-Assessment. A successful internal assessment requires a dedicated effort to document all 110 controls, and the organization's Affirming Official must legally attest to compliance in the Supplier Performance Risk System (SPRS).

Sources: 32 C.F.R. § 170.16(a)(2) (Affirmation); 89 FR 83096 (Final Rule, Assessments and Affirmations

Q2. How can we ensure our in-house assessment and interpretation of the rules are correct and will hold up if questioned later, given that interpretations can vary?

A2. Organizations should strictly utilize the NIST 800-171A assessment guide to map their controls. The Final Rule mandates that all Level 2 assessments, both Self and Certified Third-Party Assessor Organization (C3PAO), be conducted strictly in accordance with NIST SP 800-171A assessment procedures.

Sources: 32 C.F.R. § 170.16(c)(1) (Assessment Procedures); 89 FR 83096 (Section 170.16 CMMC Level 2 Self-Assessment and Affirmation Requirements)

Q3. To clarify, can the assessment be done in-house, but the final certification must be done by a third party?

A3. CMMC Level 2 has two distinct tracks depending on the contract requirement. PPA requires contractors complete Level 2 (Self). If the contractor completes Level 2 (Self), an in-house assessment entered into SPRS and signed by an Affirming Official, it is sufficient to comply with the requirement. Companies may elect to voluntarily undergo a CMMC Level 2 (C3PAO assessment), and completed C3PAO assessments that are reported will be visible in SPRS.

Sources: 32 C.F.R. § 170.16 (CMMC Level 2 self-assessment and affirmation requirements).

Q4. Where can we find the direct link to the approved C3PAO list on the DoW marketplace?

A4. The list of approved C3PAOs is located under the "Marketplace" section on the DoW website/Cyber AB portal.
https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending

Q5. Is there a contingency plan if a material share of agents or Transportation Service Providers (TSPs) cannot meet the compliance deadline?

A5. The DoW views this change as strictly mandated. Although implementation of CMMC third-party assessments is currently paused, the underlying requirements to safeguard controlled unclassified information (CUI) remain firmly in place. These requirements, mandated by Title 32 of the Code of Federal Regulations Part 2002, require implementation of National Institute of Standards and Technology Special Publication 800-171. Self-assessments under CMMC Level 2 remain a requirement.

Sources: 32 C.F.R. § 170.3(e)(Phased Implementation)

Q6. Has the PPA considered requesting a compliance extension or phased implementation approach through March 2027?

A6. The PPA *has* adopted a phased implementation approach to comply with Phase 1 Department of War requirements, requiring Level 1 self-assessments be completed by companies in the Tender of Service by March 1, 2026, and level 2 self-assessments to be completed by March 1, 2027.

The Department of War remains in Phase 1 (requiring Level 1 and Level 2 Self-Assessments) of CMMC implementation. On July 13, 2026, the Department of War announced the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which was originally scheduled for November 10, 2026. All Phase I (CMMC Level 1 and Level 2) self-assessment requirements remain firmly in place. DoW's suspension of Phase 2 and 3 do not change the requirements of Phase I, which continues to be a current, valid requirement (including Level 1 and Level 2 Self-Assessments).

Sources: 32 C.F.R. § 170.3(e) (Phased Implementation), OSW Release, July 13, 2026

Q7. Will the DoW accept a System Security Plan (SSP) with a POA&M during the transition period, or is full compliance required by March 1, 2027?

A7. You will not turn your SSP into the DoW; you submit your compliance in SPRS. Under the Final Rule, a POA&M is acceptable ONLY if the overall assessment score is at least an 88 (out of 110) and no heavily weighted controls are on the POA&M. POA&Ms must be closed out within 180 days.

Sources: 32 C.F.R. § 170.21(a)(2) (Plan of Action and Milestones); 89 FR 83096 (Section 170.16 CMMC Level 2 Self-Assessment and Affirmation Requirements)

2. Cloud Services and FedRAMP

Q1. Is it required to use FedRAMP certified cloud services, or are commercial cloud services acceptable?

A1. Carriers must use FedRAMP certified product **or** commercial solutions that do not have an official FedRAMP certification but have equivalent or greater features/capabilities are acceptable under CMMC Level 2 guidance. The TSP is responsible for verifying and documenting this equivalency (e.g., via a Service Level Agreement).

Sources: 32 C.F.R. § 170.16(c)(2) (Cloud Service Providers)

Q2. Does this mean Microsoft 365 (M365) Commercial is sufficient, and we do not need to upgrade to a more expensive Government cloud version like Government Community Cloud (GCC) High?

A2. Standard M365 Commercial lacks several features necessary for FedRAMP equivalency out-of-the-box. TSPs choosing to use it must do their due diligence to document FedRAMP Moderate equivalency, including managing Customer Responsibility Matrix (CRM) controls. GCC and GCC High natively meet FedRAMP Moderate/High standards.

Sources: 32 C.F.R. § 170.16(c)(2) (Cloud Service Providers)

Q3. Could you provide further clarification on FedRAMP requirements for AI cloud solutions in addition to email solutions?

A3. The Final Rule applies to *any* Cloud Service Provider (CSP). Any use of an AI tool where CUI data is input requires that the AI tool be FedRAMP certified **or** a commercial solution that does not have an official FedRAMP certification but has equivalent or greater features/capabilities to those required are acceptable under CMMC Level 2 guidance.

Sources: 32 C.F.R. § 170.16(c)(2) (Cloud Service Providers)

Q4. Are FedRAMP-authorized AI environments required when processing CUI or covered DP3 data?

A4. Yes. Inputting any CUI data into an AI tool means the tool is processing CUI. It becomes an in-scope CUI Asset and the underlying cloud service must be FedRAMP Moderate authorized or equivalent.

Sources: CMMC Level 2 Scoping Guide v2.0, Section 2.1 (CUI Assets); 32 CFR § 170.19(c)(1) (CMMC Level 2 Scoping)

3. Data Security and Encryption

Q1. Is encryption required for emails containing Controlled Unclassified Information (CUI)?

A1. Yes. Federal Information Processing Standard (FIPS)-validated encryption is required for data in transit and in storage for all CUI.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.11, 3.13.8);

Q2. We're concerned about protecting emails sent to external partners (e.g., sending a Government Bill of Landing). Do we need a secure email portal?

A2. If the communication contains CUI, it must be encrypted in transit using FIPS-validated cryptography. TSPs must utilize an encrypted portal, secure email gateway, or other compliant method.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8)

Q3. What are the expectations for encrypting communications with Military Claims Offices, Service members, and their spouses, especially when they might use personal email accounts (like Gmail)?

A3. Any transmission containing CUI must be encrypted in transit using FIPS-validated encryption, regardless of the recipient's domain (e.g., Gmail). The TSP must provide a secure way for the recipient to access the data.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8).

Q4. Will Government systems prevent receiving emails sent via GCC or Commercial Office 365 message encryption?

A4. There may be outstanding technical compatibility issues between commercial and Government IT systems. If commercial partners experience issues sending or receiving encrypted emails across domains, please utilize alternative secure means of encryption to transmit CUI such as DoW Safe (https://safe.apps.mil/my.policy).

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8).

Q5. Is the Government's email system considered appropriate for receiving CUI without further encryption from the sender?

A5. No, the sender is still responsible for encrypting the data in transit. Any transmission containing CUI must be encrypted in transit using FIPS-validated encryption, regardless of the recipient's domain (e.g., Gmail). The TSP must provide a secure way for the recipient to access the data.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8).

Q6. What should Industry expect regarding how the Government will securely email Controlled Unclassified Information (CUI) to TSPs?

A6. TSPs receive CUI information and orders through the Defense Personal Property System. TSPs will only receive emails from PPA members on a case-by-case basis and will be sent encrypted or via DoW Safe (https://safe.apps.mil/my.policy).

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8).

Q7. What is required or expected when two TSPs with conflicting security policies need to share CUI for a directed shipment?

A7. Regardless of conflicting internal policies, both TSPs are required to ensure that CUI is protected with FIPS-validated encryption during transit and while at rest.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8)

Q8. Is FIPS-validated encrypted transmission required for all external CUI transfers?

A8. Yes. FIPS-validated encryption is required for data in transit for all CUI.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8)

Q9. Does document labeling alone satisfy transmission requirements for CUI, or is encryption always mandatory?

A9. Encryption is always mandatory. Document labeling does not satisfy transmission requirements; CUI must be encrypted in transit as well as in storage.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2

Q10. Is FIPS-validated encrypted messaging required for operational SMS/MMS communications, and are there compliant alternatives for carrier messaging?

A10. Yes. FIPS-validated encryption is required for data in transit, which explicitly includes SMS and MMS messaging. Standard carrier text messaging is not compliant for transmitting CUI.

Sources: 32 C.F.R. Part 2002 (h)(2); NIST SP 800-171 Rev 2 (3.13.8)

Q11. Does Government Bill of Lading (GBL) information, by itself, meet the CUI definition under 32 C.F.R. Part 2002?

A11. A blank GBL is not CUI. Populated GBLs are only accessible to TSPs by logging into DPS and are marked as CUI.

Sources: Seven Part Analysis

4. Subcontractors and Partners

Q1. How can we be sure that third-party certifiers are knowledgeable about the unique aspects of the moving and storage industry?

A1. C3PAOs evaluate against NIST 800-171 controls, which are industry-agnostic cybersecurity standards. Authorized C3PAOs are strictly trained and vetted by the Cyber Accreditation Body to evaluate IT environments, not specific industry operational models.

Sources: 32 C.F.R. § 170.8 (CMMC Accreditation Body)

Q2. How are we expected to handle compliance verification for large partners like UPS and airlines who may not provide specific attestations? Is there a master list of compliant companies?

A2. Prime contractors must verify that the subcontractor has an active, valid CMMC score in SPRS. Prime contractors may do this by requesting subcontractors provide a screenshot showing current CMMC compliance.

Sources: 32 C.F.R. § 170.23(a)(2) (Subcontractor Flow-Down)

Q3. For subcontractors, is their self-certification of compliance sufficient for our records?

A3. Under the Code of Federal Regulations (CFR) flow-down requirements, if an entity handles CUI, they are in full scope. Prime contractors must verify that the subcontractor has an active, valid CMMC score in SPRS.

Sources: 32 C.F.R. § 170.23(a)(2) (Subcontractor Flow-Down)

Q4. Does a subcontractor need to attest in the official SPRS system, or is attesting to the prime contractor sufficient, as it was for Level 1?

A4. Yes, the subcontractor must have their own entry. The prime contractor's responsibility is to flow down CMMC assessment requirements as described in 32 CFR §170.23 and also to refrain from disseminating FCI or CUI to subcontractors that have not indicated meeting the CMMC level described in that section for the type of information to be shared. However, prime contractors should communicate early and often with prospective subcontractors to confirm current CMMC status, including whether the level matches that required.

Sources: 32 C.F.R. § 170.23(a)(2) (Subcontractor Flow-Down)

Q5. What is our level of compliance responsibility for contract drivers who are given access to sensitive paperwork?

A5. If an entity (including a trucker or driver) handles CUI, they are in full scope. The CMMC Level 2 Scoping Guide dictates that if they process CUI digitally (e.g., via mobile device apps or email), those devices are CUI Assets. If they are handed paper media ONLY and they return it or destroy it (and certify destruction), the digital scope is bypassed.

Sources: 32 CFR § 170.19(c)(1) (CMMC Level 2 Scoping); *CMMC Level 2 Scoping Guide v2.0, Section 2.1 (CUI Assets)*

Q6. Will all subcontractors be required to complete their own CMMC Level 2 self-assessment within SPRS?

A6. Yes, if they process, store, or transmit CUI digitally, they must meet the same CMMC level as the Prime for that specific data and have an active score in SPRS before the Prime can flow the data down to them.

Sources: 32 C.F.R. § 170.23 (a)(2) (Subcontractor Flow-Down)

Q7. Are independent Drivers/Owner-Operators who utilize Prime CMMC-compliant systems required to obtain CMMC Level 2 compliance independently?

A7. If they utilize the Prime's systems (e.g., accessing an app via Virtual Desktop Infrastructure or logging into the Prime's enclave), they may be treated as End Users within the Prime's assessed boundary, provided the Prime's SSP documents this architecture and manages the risk (Contractor Risk Managed Assets). If they use their own IT to store/process CUI, they must obtain compliance independently.

Sources: 32 CFR § 170.19(c)(1) (CMMC Level 2 Scoping); *CMMC Level 2 Scoping Guide v2.0 (CRMA and VDI Scoping definitions)*

Q8. Are laborers who are provided customer CUI to perform their duties required to meet CMMC Level 2 requirements?

A8. As with drivers, if they handle CUI digitally on their own devices, they are in scope. If they only receive physical paper and return/destroy it, or if they only access a securely contained Prime system, their independent scope is eliminated or absorbed by the Prime.

Sources: 32 CFR § 170.19(c)(1) (CMMC Level 2 Scoping); *CMMC Level 2 Scoping Guide v2.0, Section 2.1 (CUI Assets)*

Q9. Should Drivers, Owner-Operators, and laborers be treated as subcontractors for purposes of CMMC compliance?

A9. Yes. If they are external corporate entities/contractors handling CUI on their own infrastructure, they fall under the Code of Federal Regulations flow-down requirements and are considered subcontractors who must meet CMMC requirements.

Sources: 32 C.F.R. § 170.23 (a)(2) (Subcontractor Flow-Down).

Q10. Do third-party service personnel, such as repair workers handling claims with CUI, need to be CMMC certified?

A10. Generally, no. Sharing a description of the item, address, and first name constitutes PII, but usually does not rise to the level of CUI PRVCY. Without CUI in the data flow, CMMC Level 2 does not apply to that specific transaction. TSPs should recommend that the repairperson purge all data containing PII after completion.

Sources: 32 CFR § 170.19(c)(1) (CMMC Level 2 Scoping); *CMMC Level 2 Scoping Guide v2.0, Section 2.1 (CUI Assets)*

5. Scope and Applicability

Q1. When a Service member's storage converts to self-pay, is that shipment still within the scope of CMMC requirements?

A1. Once a shipment converts to self-pay, the Service member must sign a commercial storage agreement, and the shipment is no longer under a Government contract. CMMC requirements do not apply to non-Government contracts. Once the Service member requests delivery of their shipment, the shipment then reconverts to a Government contract, reinstating CMMC requirements.

Sources: 32 C.F.R. § 170.3(a) (Applicability).

Q2. Are there any exceptions to CMMC assessment requirements for the transportation industry, or do all rules apply uniformly?

A2. There are no exceptions for the transportation industry. The Final Rule applies uniformly to all DoW contractors processing CUI. The DoW has stated this change is mandated and all industry partners are required to comply.

Sources: 32 C.F.R. § 170.3(a) (Applicability).

Q3. How are international service providers expected to demonstrate compliance when U.S. cloud or data residency requirements conflict with local laws?

A3. Neither NIST SP 800-171 nor CMMC are geographically bound. Therefore, if the international service provider is the prime contractor, then they are responsible for certifying CMMC compliance in SPRS. However, if the international service provider is hired by the prime contractor, as a subcontractor, then the prime contractor is responsible for determining how its subcontractors verify compliance.

Sources: 32 C.F.R. § 170.3(a) (Applicability).

Q4. Has an assessment been conducted on the potential impact of CMMC implementation on DP3 capacity, particularly among small carriers and rural agents?

A4. The DoW conducted a Regulatory Impact Analysis within the Final Rule that estimates compliance costs and impact on small businesses broadly across the Defense Industrial Base, acknowledging that costs may be significant. However, the PPA has not published a specific capacity impact study solely for the DP3 / Household Goods moving sector.

Sources: 89 FR 83096 (Final Rule, Section V: Regulatory Impact Analysis); 32 C.F.R. Part 2002 (CUI Requirements)

Q5. What specific CMMC scoping guidance applies to TSPs whose CUI handling is limited solely to shipment documentation and PII?

A5. If an entity handles CUI (even limited amounts), the systems processing that CUI are designated as "CUI Assets" and are in full scope. To limit scope, TSPs must physically or logically isolate the CUI handling (e.g., using enclaves) so that the rest of their corporate network becomes "Out-of-Scope Assets." Handling paper media only and subsequently destroying it also bypasses digital scoping.

Sources: 32 CFR § 170.19(c)(1) (CMMC Level 2 Scoping); *CMMC Level 2 Scoping Guide v2.0, Section 2.1 (CUI Assets)*