CMMC Level 2 Self-Assessment In-depth analysis

Amira Armond

Certified CMMC Assessor,
Provisional Instructor, CISSP, CISA

January 3, 2024

Screenshots taken from
https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program

Timeline for CMMC Level 2 self-assessments

§ 170.3(e)(1)

(1) *Phase 1*. Begins on the effective date of the CMMC revision to DFARS 252.204-7021. DoD intends to include CMMC Level 1 Self-Assessment or CMMC Level 2 Self-Assessment for all applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, include CMMC Level 1 Self-Assessment or CMMC Level 2 Self-Assessment for applicable DoD solicitations and contracts as a condition to exercise an option period on a contract awarded prior to the effective date. DoD may also, at its discretion, include CMMC Level 2 Certification Assessment in place of CMMC Level 2 Self-Assessment for applicable DoD solicitations and contracts.

Joint Surveillances good until >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>(early adopters)>>>>>(late adopters)>>>

Phase 1
Level 1 or Level 2
self-assessments
for all contracts
(no low scores
allowed).

Some contracts
require
certifications

Phase 2
Majority contracts require
Level 2 certifications.
DoD may delay certification
requirement until an option
year.

Some contracts require Level 3
certification.

Phase 3
Majority contracts, including
option years from earlier
contracts, require Level 2 or
3 certifications.

Phase 4
CMMC
requirements
in every DoD
contract

14 months?

Feb 2025?

6 months

Aug 2025?

12 months

Aug 2026?

12 months

Aug 2027?

Time

CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

KIERI

§ 170.23(a)(2)

(2) If a subcontractor will process, store, or transmit CUI in performance of the subcontract, CMMC Level 2 Self-Assessment is the minimum requirement for the subcontractor.

Analysis
Self-assessment also applies to subcontractors if they handle CUI.

§ 170.15(a)(1)

(1) *Self-Assessment*. The OSA must complete and achieve a MET result for all security requirements specified in § 170.14(c)(3). The OSA must conduct a self-assessment in accordance with the procedures set forth in paragraph (c)(1) of this section and submit assessment results in SPRS. To maintain compliance with CMMC Level 2 Self-Assessment requirements, the OSA must perform a CMMC Level 2 Self-Assessment on a triennial basis and submit the results in SPRS.

§170.14(c)(3):
"CMMC Level 2 requirements. The security requirements in CMMC Level 2 are identical to the requirements in NIST SP 800-171 Rev 2."

Procedure to perform self-assessment

§ 170.3(c) (c) *Procedures*. – (1) *Self-Assessment*. The OSA must perform a CMMC Level 2 Self-Assessment in accordance with NIST SP 800-171A (incorporated by reference, see § 170.2) and the CMMC Level 2 scoping requirements set forth in § 170.19(a) and (c) for the information systems within the CMMC Assessment Scope. The assessment must be scored in accordance with the CMMC Scoring Methodology described in § 170.24. If a POA&M exists, a POA&M closeout assessment must be performed by the OSA when all remaining requirements have been remediated. The POA&M closeout assessment must be performed within the 180-day closeout period.

Analysis

This is where scoping according to the CMMC Level 2 scoping guide is tied in (which adds Security Protection Data and requiring CMMC Level 2 for external service providers). NIST SP 800-171A is not versioned (an oversight?).

Plan of Action and Milestones (POA&Ms)
AKA “not all requirements are MET”

KIERI

§ 170.21(a)(2) (2) *CMMC Level 2 Self-Assessment and CMMC Level 2 Certification Assessment.* An OSA is only permitted to have a POA&M for CMMC Level 2 if all the following conditions are met:

(i) The assessment score divided by the total number of security requirements is greater than or equal to 0.8;

(ii) None of the security requirements included in the POA&M have a point value of greater than 1 as specified in the CMMC Scoring Methodology set forth in § 170.24, except SC.L2-3.13.11 CUI Encryption may be included on a POA&M if it has a value of 1 or 3; and

(iii) None of the following security requirements are included in the POA&M:

(A) AC.L2-3.1.20 External Connections (CUI Data).

(B) AC.L2-3.1.22 Control Public Information (CUI Data).

(C) PE.L2-3.10.3 Escort Visitors (CUI Data).

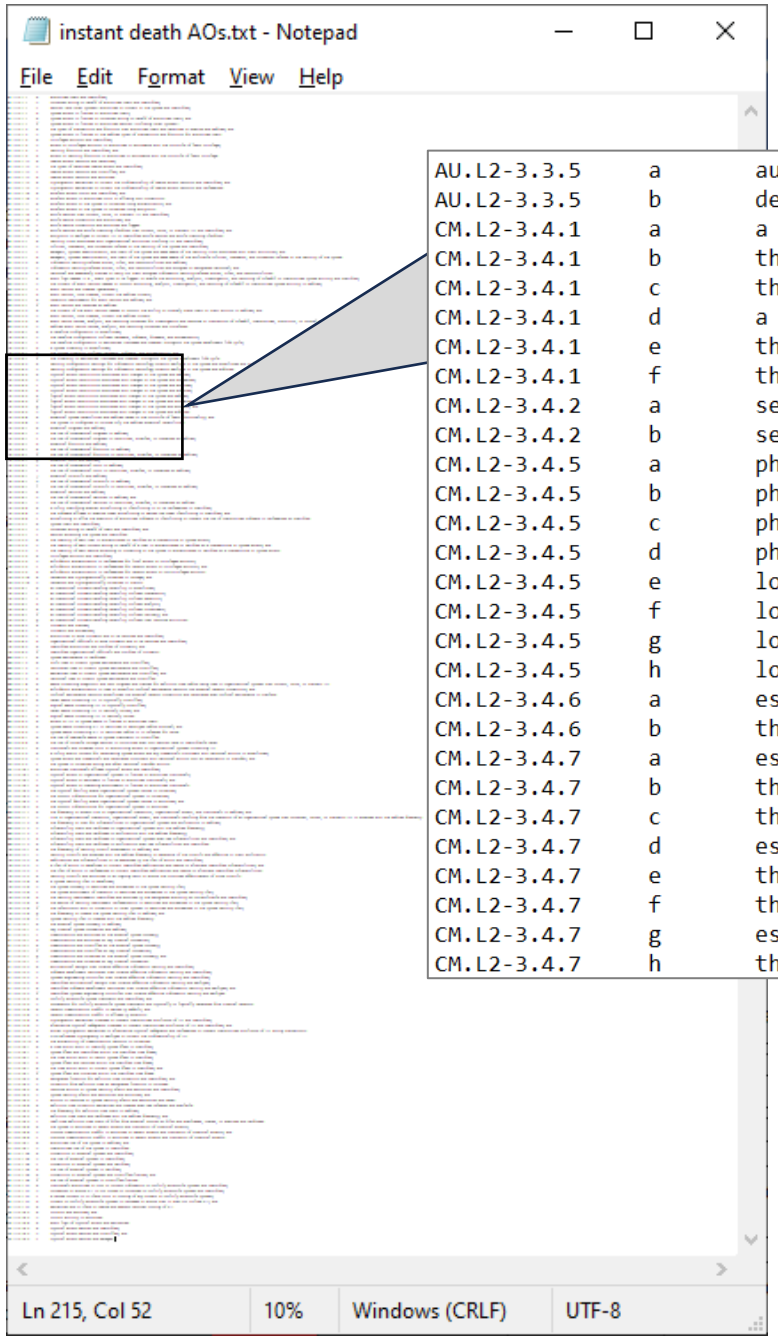
(D) PE.L2-3.10.4 Physical Access Logs (CUI Data).

(E) PE.L2-3.10.5 Manage Physical Access (CUI Data).

Self-assessment "only permitted" to have a POA&M if…?

Minimum score 88 / 110

67% of the assessment objectives must be perfectly MET (see next slide)



AU.L2-3.3.5	a	audit record review, analysis, and reporting processes for investigation and
AU.L2-3.3.5	b	defined audit record review, analysis, and reporting processes are correlate
CM.L2-3.4.1	a	a baseline configuration is established;
CM.L2-3.4.1	b	the baseline configuration includes hardware, software, firmware, and docume
CM.L2-3.4.1	c	the baseline configuration is maintained (reviewed and updated) throughout t
CM.L2-3.4.1	d	a system inventory is established;
CM.L2-3.4.1	e	the system inventory includes hardware, software, and documentation; and
CM.L2-3.4.1	f	the inventory is maintained (reviewed and updated) throughout the system dev
CM.L2-3.4.2	a	security configuration settings for information technology products employed
CM.L2-3.4.2	b	security configuration settings for information technology products employed
CM.L2-3.4.5	a	physical access restrictions associated with changes to the system are defir
CM.L2-3.4.5	b	physical access restrictions associated with changes to the system are docum
CM.L2-3.4.5	c	physical access restrictions associated with changes to the system are appro
CM.L2-3.4.5	d	physical access restrictions associated with changes to the system are enfor
CM.L2-3.4.5	e	logical access restrictions associated with changes to the system are define
CM.L2-3.4.5	f	logical access restrictions associated with changes to the system are docume
CM.L2-3.4.5	g	logical access restrictions associated with changes to the system are approv
CM.L2-3.4.5	h	logical access restrictions associated with changes to the system are enforc
CM.L2-3.4.6	a	essential system capabilities are defined based on the principle of least fu
CM.L2-3.4.6	b	the system is configured to provide only the defined essential capabilities.
CM.L2-3.4.7	a	essential programs are defined;
CM.L2-3.4.7	b	the use of nonessential programs is defined;
CM.L2-3.4.7	c	the use of nonessential programs is restricted, disabled, or prevented as de
CM.L2-3.4.7	d	essential functions are defined;
CM.L2-3.4.7	e	the use of nonessential functions is defined;
CM.L2-3.4.7	f	the use of nonessential functions is restricted, disabled, or prevented as c
CM.L2-3.4.7	g	essential ports are defined;
CM.L2-3.4.7	h	the use of nonessential ports is defined;

215 of 320 (67%) assessment objectives are not allowed POA&M

Instant Death Assessment Objectivess

Everyone needs to understand that this statement “67% of assessment objectives must be MET” does not mean that you can miss 23% of the requirements and be OK.

It means that you have two tests:
A 215-question test which must have a perfect score to pass.
(assessment objectives for requirements that aren’t allowed on the POA&M)
A 105-question test which can have lots of NOT METs and still pass.
(assessment objectives for requirements that are allowed on the POA&M)

You must pass both tests for a conditional self-assessment.
After the POA&M period runs out (180 days), you must pass both tests with **perfect scores** for a final self-assessment.

§ 170.16(a)(1)(ii)

(ii) *Conditional self-assessment*. OSAs have achieved CMMC Level 2 Conditional Self-Assessment if the Level 2 self-assessment results in a POA&M and the POA&M meets all the CMMC Level 2 POA&M requirements listed in § 170.21(a)(2).

§ 170.16(a)(1)(ii)(B)

(B) *POA&M closeout*. The OSA must implement all CMMC Level 2 security requirements and close out the POA&M within 180 days of the initial self-assessment. Upon remediation of the remaining requirements, the OSA must perform a POA&M closeout self-assessment and post compliance results to SPRS. If the POA&M is not closed out within the 180-day timeframe, the Conditional Level 2 Self-Assessment status of the OSA will expire. If Conditional Level 2 Self-Assessment expires within the period of performance of a contract, standard contractual remedies will apply, and the OSA will be ineligible for additional awards with CMMC Level 2 Self-Assessment or higher requirements for the information system within the CMMC Assessment Scope.

as a condition of contract award.

Analysis

The rule only allows POA&M under extremely limited conditions.
The rule requires a self-assessment as a condition of contract award.

The intent of the rule appears to be:
Only companies with perfect compliance are allowed to submit a self-assessment. Only companies with self-assessments are eligible for contracts.

Discussion

A senior official from the prime contractor and any applicable subcontractor will be required to affirm continuing compliance with the specified security requirements after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS (see § 170.22 for details on Affirmation requirements and procedures).

Analysis

A senior official must affirm continued compliance. This allows DoD to hold individuals accountable.

Expect to submit an affirmation (scope has not changed, self-assessment still 100%) to SPRS every 12 months going forward.

External Service Providers

Analysis

The topic of External Service Providers and Cloud Service Providers deserves its own paper (coming up soon).
However, it is vital to account for external service providers during self-assessment, and the procedures for CMMC Level 2 self-assessment include specific callouts to cloud providers and FedRAMP.

You will see that the language of the text is inconsistent regarding FedRAMP and security cloud providers. This looks like a mistake which will almost certainly be corrected by DoD.

If DoD creates a new scope based on “Security Protection Data” which requires FedRAMP equivalency for cloud vendors, DoD will greatly increase cost and requirements compared to the most liberal reading of DFARS 252.204-7012.

§ 170.19(c)(2) (2) If the OSA utilizes an External Service Provider (ESP), other than a Cloud Service Provider (CSP), the ESP must have a CMMC Level 2 Final Certification Assessment. If the ESP is internal to the OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. If using a CSP for Level 2 Self-Assessment, see § 170.16(c)(2). If using a CSP for Level 2 Certification Assessment, see § 170.17(c)(5).

Analysis

This excerpt is from §170.19 CMMC Scoping. It looks like this adds requirements for External Service Providers (CMMC Level 2 **final certification** for non-clouds and Security Protection Data) for self-assessments.

How will ESPs achieve final certification assessments before their clients start self-assessments?

§ 170.16(c)(2)

(2) *Self-Assessment of Cloud Service Provider*. An OSA may use a Federal Risk and Authorization Management Program (FedRAMP) Moderate (or higher) cloud environment to process, store, or transmit CUI in execution of a contract or subcontract with a requirement for CMMC Level 2 under the following circumstances:

Analysis

This excerpt is from §170.16 CMMC Level 2 Self-Assessment and Affirmation requirements.

Self-assessment instructions only requires FedRAMP for cloud providers used to store, process, transmit **CUI**. Cannot find mention of Security Protection Data in relation to Cloud Service Providers in the rule.

This appears to be an oversight rather than intentional.
The Q&A section describes DoD's intent: "If an OSC uses an external CSP to process, store, or transmit CUI **or to provide security protection for any such component**, the OSC must ensure the CSP's product or service offering […] is authorized as FedRAMP Moderate…"

§ 170.23(a)(2)

(i) The Cloud Service Provider's (CSP) product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or

(ii) The Cloud Service Provider's (CSP) product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline. Equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2 requirements.

Analysis

Verifying FedRAMP authorization or obtaining an SSP and CRM for each cloud that holds your CUI is a basic requirement of self-assessment.

Lack of any third-party verification for CSPs seems problematic when FedRAMP equivalency is often a multi-million-dollar investment.

KIERI

§ 170.23(a)(2)

(iii) In accordance with § 170.19, the OSA's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's System Security Plan (SSP).

Analysis

Cannot simply point to the cloud provider and say that they perform all requirements on your behalf.

This portion of the rule seems to assume that that assets running on Infrastructure-as-a-Service cloud providers are secured by the cloud provider (they are not).

Cloud providers that are truly performing FedRAMP requirements will provide a Customer Responsibility Matrix which clearly states customer responsibilities for securing IaaS assets.

What will happen if a cloud provider falsely claims that it performs all requirements on behalf of clients?

Oversight of CMMC Level 2 Self-Assessment

KIERI

§ 170.6(b)

(b) The CMMC PMO is responsible for investigating and acting upon indications that an active CMMC Self-Assessment, described in §§ 170.15 and 170.16, or CMMC Certification Assessment, described in §§ 170.17 and 170.18, has been called into question. Indications that may trigger investigative evaluations include, but are not limited to, reports from the CMMC Accreditation Body, a C3PAO, or anyone knowledgeable of the security processes and activities of the OSA.

(c) If the investigative results show that adherence to the provisions of this rule have not been achieved or maintained, the CMMC PMO may revoke the validity status of the appropriate existing CMMC Self-Assessment(s) or CMMC Final Certification Assessment(s).

Analysis

During self-assessment period, risk of adverse reports is primarily from competitors.

Fairly easy to look up external service providers (clouds, MSPs) for compliance.

RPOs / C3PAOs not incentivized to harm their clients.

§ 170.16(a)(1)(iv)

(iv) *CMMC status revocation*. If the CMMC PMO determines that the provisions of Level 1 or Level 2 of this rule have not been achieved or maintained, as addressed in § 170.6, a revocation of the validity status of the CMMC Level 2 Self-Assessment may occur. At that time, standard contractual remedies will apply and the OSA will be ineligible for additional awards with CMMC Level 2 Self-Assessment or higher requirements for the information system within the CMMC Assessment Scope until such time as a valid CMMC Level 2 Self-Assessment is achieved.

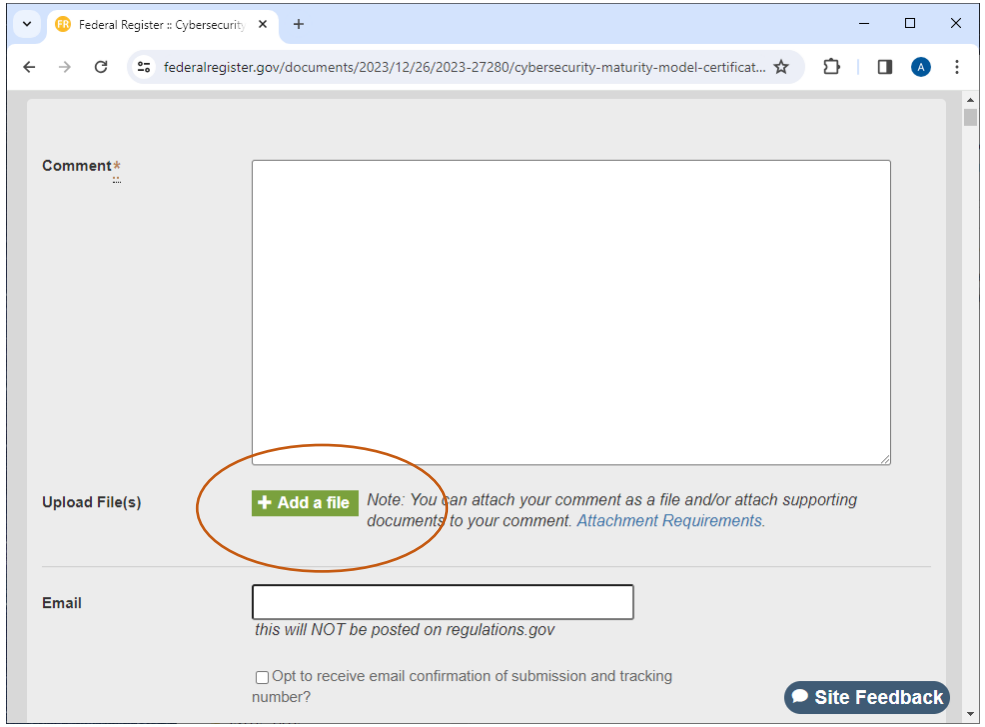
Links to self-assessment guidance and how to comment

CMMC Rule and Level 2 Assessment Guidance

- **32 CFR CMMC home and comments:** https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program
- Downloadable PDF of Federal Register text (this version has page numbers): https://public-inspection.federalregister.gov/2023-27280.pdf

- **CMMC Guidance documents home and comments:** https://www.regulations.gov/docket/DOD-2023-OS-0096/document
- Notice of Guidance for CMMC: https://www.regulations.gov/document/DOD-2023-OS-0096-0001
- CMMC Model Overview: https://www.regulations.gov/document/DOD-2023-OS-0096-0006
- Scoping Guide – CMMC Level 2: https://www.regulations.gov/document/DOD-2023-OS-0096-0003
- Assessment Guide – CMMC Level 2: https://www.regulations.gov/document/DOD-2023-OS-0096-0005

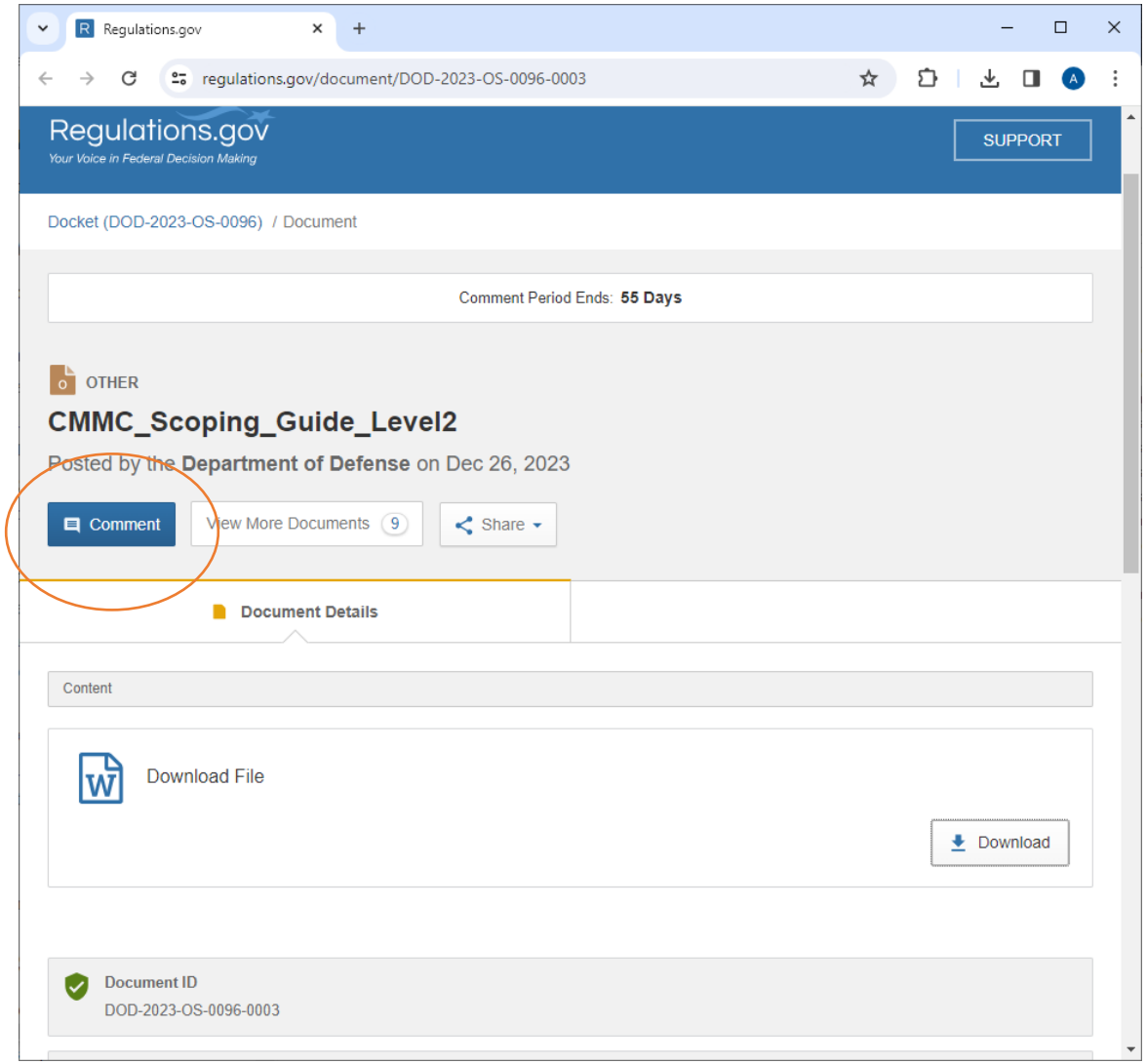
KIERI



Experienced commenters typically upload a thoughtful paper of all their comments rather than using the form.
Expect less visibility when commenting on specific documents.

CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

KIERI



Tips for submitting Effective Comments (from Regulations.gov)

- Address trade-offs and opposing views in your comment
- If you disagree with a proposed action, suggest an alternative (including not regulating at all) and include an explanation and/or analysis of how the alternative might meet the same objective or be more effective.
- Consider including examples of how the proposed rule would impact you negatively or positively.
- If you are uploading more than one attachment to the comment web form, it is recommend that you use the following file titles:
  - Attachment1_<insert title of document>
  - Attachment2_<insert title of document>
  - Attachment3_<insert title of document>
- There is no minimum or maximum length for an effective comment
- The comment process is not a vote – one well supported comment is often more influential than a thousand form letters

CYBER AB CMMC CERTIFICATION
AUTHORIZED C3PAO

KIERI

Have you seen our CMMC Rule Webinar yet?

https://youtu.be/xHtHuYyynIQ

Kieri Solutions, an Authorized C3PAO

www.kieri.com

- Assessment and preparation assistance
  - Expertise: 9 Certified CMMC Assessors and Instructors, plus CCPs
  - Fortune 100s to small businesses
- Kieri Reference Architecture (KRA)
  - Do-it-yourself (or with help) *functional and expandable* Level 2 enclave.
  - Microsoft 365 / Windows Laptops / BYOD Phones
- Kieri Compliance Documentation (KCD)
  - Do-it-yourself docs and instructions to run a compliant IT Department
  - Uses behavior stacking, just-in-time procedures, convenient record-keeping
  - Training library and monthly Q&As

AUTHORIZED C3PAO

Kieri Solutions cannot certify companies that we've consulted for (including KRA / KCD)

Kieri Solutions, an Authorized C3PAO

www.kieri.com

Self-assessment-specific offerings!

Our KCD and KRA products include…

- Self-assessment templates for internal staff
  - Automatic scoring, charts and summary views
  - Detailed findings and assessor notes
  - Training to perform self-assessment correctly
- Recommended tests and examinable evidence for each assessment objective
- Plan of Action & Milestones template

Kieri certified assessors can help your team perform a self-assessment

- Your team may review/adjust/repair issues before submitting to SPRS
- Provides assurance to internal leadership (important for shareholders)
- Eligible for certification assessment later if no consulting provided