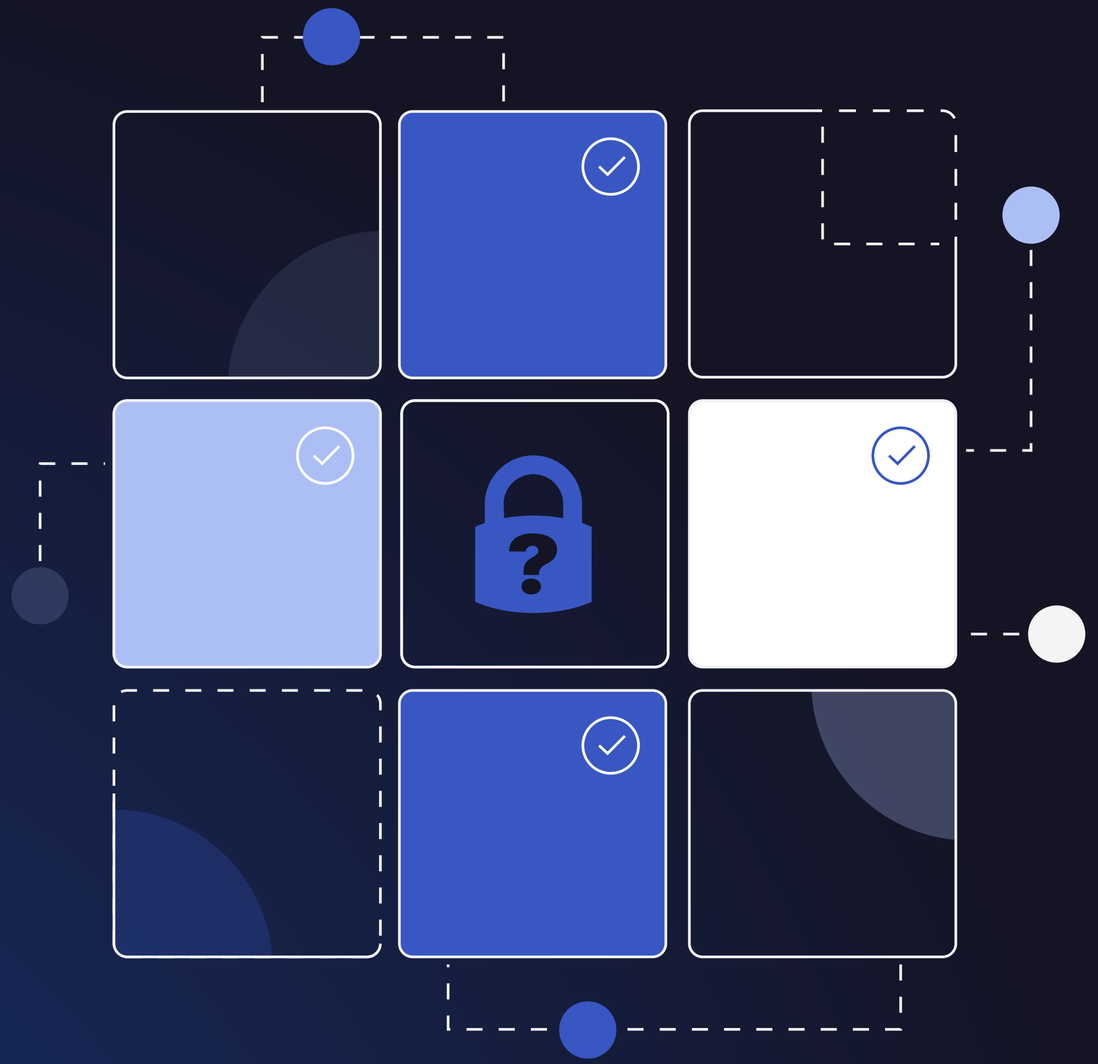
C3

A PRACTICAL GUIDE FOR DIB CONTRACTORS

The CMMC Level 2 Self-Assessment

What the rule requires, what good looks like, and how to avoid the traps.



Introduction

If you are reading this, you are likely in one of two situations. A Department of War (DoW) contract, solicitation, or option year extension has put a CMMC Level 2 self-assessment requirement in front of you for the first time. Or you have been through the process before, and the time has come for your annual affirmation or triennial reassessment. In either case, you are looking for a clear understanding of what the assessment actually requires and what it takes to produce a score you can defend.

This guide answers those questions honestly. A Level 2 self-assessment is a defined, documented process—the same process a third-party assessor would follow—conducted by your organization on its own information system. It is not a shortcut. It is not a checkbox. And it is not something you can perform against a system that does not yet exist.

The guidance here applies equally whether you are approaching your first Level 2 self-assessment, conducting the triennial reassessment, or reviewing your compliance program for the annual affirmation. The rigor, the evidence standards, and the reporting requirements do not change based on which one you are doing, and neither does the Affirming Official's legal exposure for the attestation that follows.

This guide does not constitute legal advice. It is not a substitute for reading the CMMC Assessment Guide—Level 2, NIST SP 800-171A, or the text of 32 CFR Part 170. Those are the authoritative sources, and they are cited throughout. This guide is meant to help you navigate them with confidence.

How to Use This Guide

This guide is written to be read start to finish, but each section is self-contained and works as a reference. If you are new to CMMC, read sequentially. If you are deep in an assessment and need to confirm a specific point (what must go into SPRS, what counts as evidence, what a POA&M can and cannot include), jump to the relevant section.

1. What a Level 2 Self-Assessment Actually Is

A CMMC Level 2 self-assessment evaluates your organization against all 110 security requirements of NIST SP 800-171 Revision 2. Those 110 requirements break down into 320 assessment objectives defined in NIST SP 800-171A Jun2018, and the assessment is made at the objective level, not the requirement level.

The methodology is the same methodology a CMMC Third-Party Assessor Organization (C3PAO) would apply in a Level 2 certification assessment. The evidence standards are the same. The scoring is the same. The primary difference between a Level 2 (Self) and a Level 2 (C3PAO) is who conducts the assessment.

FROM THE CMMC ASSESSMENT GUIDE

"The security requirements for a Level 2 self-assessment and a Level 2 certification assessment are the same, the only difference in these assessments is whether it is conducted by the OSA or by an independent C3PAO."

CMMC Assessment Guide—Level 2, v2.13

Mythbusting the Self-Assessment

The market is full of well-intentioned but incorrect framing around what a Level 2 self-assessment entails. The table below addresses the four most common misconceptions.

MYTH	FACT
A Level 2 self-assessment is a lighter, faster version of a C3PAO assessment.	The 320 assessment objectives and the assessment methodology are identical. Only the assessor role differs. DoW estimates a small business, working with an External Service Provider (ESP), will spend 140 hours to complete a self-assessment.
You can self-assess your system before it is fully built or before your documentation is finalized.	An assessment evaluates implementation. You cannot score a requirement as MET against evidence that does not exist. The CMMC Assessment Scope must be defined, the system must be operational, and the documentation must be final before the self-assessment begins.
Submitting a score in SPRS is the self-assessment.	SPRS is the reporting mechanism. The self-assessment is the process that produces the score: evaluating every objective against evidence using the examine, interview, and test methods, and making a MET / NOT MET / NOT APPLICABLE determination for each one.
An ESP or MSP can perform the self- assessment on your behalf.	An ESP can support implementation, documentation, and evidence gathering. The Organization Seeking Assessment (OSA) retains accountability for every MET / NOT MET determination, the SPRS submission, the Affirming Official attestation, and the six-year evidence retention. The attestation carries legal weight under the False Claims Act.

"The only difference between a Level 2 (Self) and a Level 2 (C3PAO) is who conducts it."

2. Before You Begin: What Has to Be True

A self-assessment is an evaluation of a system that exists, operates, and produces evidence. If your information system is still being built, still being documented, or still being configured, you are not ready to self-assess. You are still implementing.

The preconditions below represent the minimum state your program must reach before a self-assessment can be conducted with integrity. Skipping any of them does not accelerate the timeline; it produces a score you cannot substantiate, which is a much larger problem than a missed deadline.

- **The CMMC Assessment Scope is defined and documented.**
  Your asset inventory, network diagram, and treatment of each asset category (CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets) are in the System Security Plan. See the *CMMC Scoping Guide*—Level 2 for the asset categorization framework and the documentation requirements associated with each category.

- **The information system is implemented and operational.**
  Controls are in place, configured, and functioning. The system has been running long enough to generate operational evidence (logs, records, change history). There is no uniform standard for what "long enough" means, but 90 days of operational evidence is generally considered sufficient.

- **All documentation is final, not draft.**
  Policies, procedures, and the System Security Plan are final and approved, and they describe how the organization actually operates.

- **Roles and responsibilities are assigned.**
  The personnel responsible for each control family can be identified. This includes third parties (MSPs, MSSPs, consultants) when they perform the work.

- **Evidence for each assessment objective is identifiable.**
  You know where to find the evidence that supports each of the 320 assessment objectives. You do not need to have gathered it all yet, but you must know where it lives.

- **An Affirming Official is designated.**
  A senior representative with authority to affirm the organization's compliance has been identified. They understand what they will be attesting to.

FROM NIST SP 800-171A

Evidence *is defined as: "Grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood."*

Evidence used to support a finding of MET must be in final form. Drafts, working papers, and unofficial or unapproved policies are not acceptable.

3. How the Assessment Works

Every CMMC Level 2 assessment—whether conducted by your organization or by a C3PAO—is built on a single framework defined in NIST SP 800-171A and operationalized in the CMMC Assessment Guide—Level 2.

Each of the 110 security requirements is decomposed into assessment objectives. Each assessment objective is a determination statement: a specific question the assessor must answer. The assessor applies one or more of three assessment methods to reach a finding.

The Three Assessment Methods

METHOD	WHAT IT MEANS	WHAT IT LOOKS LIKE IN PRACTICE
Examine	Reviewing, inspecting, observing, or analyzing an assessment object (a document, a mechanism, or an activity).	Reading a policy or procedure. Inspecting a firewall configuration. Reviewing audit logs. Observing a facility's visitor log. Analyzing a network diagram against the assessment scope.
Interview	Discussions with individuals or groups who perform, oversee, or are affected by the control.	Talking with a system administrator about how patching occurs. Discussing account management with the person who provisions and deprovisions users. Asking the facilities manager how visitor escort works.
Test	Exercising an assessment object (an activity or mechanism) under specified conditions and comparing actual behavior to expected behavior.	Watching MFA actually enforce at login on a sample of systems. Confirming that a removable media control actually blocks an unauthorized USB device. Tracing a log entry from the event through the SIEM.

FROM NIST SP 800-171A

"Organizations are not expected to employ all assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to determine the level of effort needed and the assurance required for an assessment... based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied."

NIST SP 800-171A Jun2018, Chapter 2

3. How the Assessment Works

Depth and Coverage: How Much Rigor Is Enough?

NIST defines two attributes that describe the level of effort applied to each method:

Depth

Addresses the rigor and level of detail of the assessment. NIST defines three levels: basic (high-level review sufficient to confirm implementation is free of obvious errors), focused (more in-depth analysis providing increased confidence that controls operate as intended), and comprehensive (probing, detailed analysis supporting confidence that controls operate consistently over time).

Coverage

Addresses the scope or breadth of the assessment: how many objects of each type are examined, how many individuals are interviewed, and how representative the sample is.

For a self-assessment, the practical minimum is basic depth and basic coverage for each assessment objective. Your review must be rigorous enough to confirm implementation is free of obvious errors, and your sample must be representative enough to confirm the control operates across the CMMC Assessment Scope rather than in one favorable case.

Recommended exception: For requirements that cannot be placed on a POA&M and for 5-point requirements where a NOT MET has the largest scoring impact, consider applying focused depth or focused coverage. The higher the stakes of an incorrect determination, the more assurance you should want in the evidence supporting it.

4. Sample Control Walkthrough

To move from abstract process to something concrete, this section walks through one complete Level 2 security requirement: SI.L2-3.14.1, Flaw Remediation. The same pattern—requirement statement, assessment objectives, three methods, evidence, determination—applies to every one of the 110 Level 2 requirements.

SI.L2-3.14.1—Flaw Remediation

Identify, report, and correct system flaws in a timely manner.

Assessment Objectives

This single requirement decomposes into **six assessment objectives.** Each must yield a finding of MET or NOT APPLICABLE for the overall requirement to be MET. A single NOT MET objective fails the entire requirement.

3.14.1[a]

The time within which to identify system flaws is specified.

3.14.1[b]

System flaws are identified within the specified time frame.

3.14.1[c]

The time within which to report system flaws is specified.

3.14.1[d]

System flaws are reported within the specified time frame.

3.14.1[e]

The time within which to correct system flaws is specified.

3.14.1[f]

System flaws are corrected within the specified time frame.

4. Sample Control Walkthrough

Applying the Three Methods

A defensible self-assessment of this requirement typically draws on evidence from all three methods. The table below shows how an OSA might approach each method, with realistic examples drawn from the potential assessment objects in NIST SP 800-171A.

METHOD	WHAT TO DO	EXAMPLE EVIDENCE
Examine	Review the organization's documentation for defined time frames (objectives a, c, e) and recent operational records for evidence of timely execution (objectives b, d, f).	• System and Information Integrity policy specifying flaw identification, reporting, and remediation time frames. • Vulnerability scan schedule and most recent scan reports. • Patch management procedure identifying who receives flaw reports and how quickly. • Change control records showing recent patches or fixes applied within the specified window.
Interview	Confirm that the people responsible for flaw remediation understand the time frames, follow the procedure, and know how to escalate exceptions.	• System administrator responsible for patching. • Personnel with information security responsibilities (typically the person overseeing vulnerability management). • Personnel from an External Service Provider (e.g., an MSP) if they perform flaw remediation on the OSA's behalf.
Test	Exercise the processes and mechanisms to confirm they work as described, not just as documented.	• Trace a known vulnerability from discovery (scan output) through reporting to remediation, and confirm timing against the documented windows. • Sample a recent patch cycle and verify on a representative set of systems that the patches were actually applied. • Observe the patch management tool run or review its logs for a recent deployment.

ONE NOT MET OBJECTIVE FAILS THE ENTIRE REQUIREMENT

If your organization has a clear vulnerability management policy, scans regularly, and applies patches within the specified time frame—but has not specified a time frame for reporting flaws (objective [c])—then objective [c] is NOT MET.

That single gap causes SI.L2-3.14.1 to be scored NOT MET, which subtracts 5 points from your total. The control's overall finding reflects the weakest objective, not the average. This is why the objective-level breakdown matters.

5. Evidence: What Counts, How Much, and How to Retain It

Evidence is the substance of a Level 2 self-assessment. Everything else—the objectives, the methods, the determinations, the score—rests on it. If the evidence does not exist, or does not support the finding, the determination is not defensible. This section covers what qualifies as evidence, how much is enough, and how to retain it for the required six years.

"Evidence does not need to be voluminous. It needs to be final, relevant to the specific objective, and capable of substantiating the finding."

What Qualifies as Evidence

Evidence comes in three categories that map directly to the three assessment methods. A single assessment objective is often supported by evidence from more than one method—an interview identifies a document, an examination of the document shows the policy, and a test demonstrates the mechanism enforces the policy.

EXAMINE (EXAMPLES)	**INTERVIEW** (EXAMPLES)	**TEST** (EXAMPLES)
• Policies and procedures • System Security Plan • Network diagrams • Asset inventory • Configuration settings • Access control lists • Audit logs and records • Training records • Change management records	• System and network administrators • Security and compliance staff • HR personnel (for onboarding / offboarding) • Facilities staff (physical security) • Configuration management owners • End users subject to the control • Leadership responsible for the program	• Demonstrating MFA actually enforces • Confirming log events reach the SIEM • Observing a removable media block • Tracing a patch through deployment • Running through an incident response playbook • Witnessing a backup and restoration

How Much Evidence Is Enough?

NIST SP 800-171A Jun2018 does not prescribe a minimum quantity. Instead, it gives the assessor two questions to ask for every objective. The self-assessor should ask the same two questions, and answer them honestly:

- **Is the evidence sufficient to support a defensible MET determination?** Not "can I argue for MET," but "would an independent assessor looking at this same evidence reach the same conclusion?"
- **Does the evidence reflect the whole CMMC Assessment Scope, not just one favorable instance?** If you have 50 endpoints in scope, your evidence should reflect something about all 50, not just the IT director's laptop.

A useful third question comes from the rule itself: could you substantiate this finding to a DCMA DIBCAC assessor tomorrow? The Government reserves the right to verify self-assessment results at any time. If the answer is uncertain, the objective is not yet MET—regardless of how badly you want it to be.

Evidence Retention - FROM THE RULE

"The artifacts used as evidence for the assessment must be retained by the OSA for six (6) years from the CMMC Status Date." - 32 CFR § 170.16(a)(2)

Six years is a long time. Evidence that is scattered across laptops, held only in one person's email, or stored in draft folders will not survive staff turnover, system migrations, or a DCMA DIBCAC assessment three years after the fact. A small amount of retention discipline up front prevents a great deal of scrambling later.

Practical Retention Suggestions

- **Organize evidence by assessment objective.** A common approach is a central mapping document or workbook with an entry for each requirement, where the evidence supporting each assessment objective is listed (or linked) on that entry. Future reassessment becomes dramatically easier when the structure mirrors how the assessment itself is conducted.
- **Capture evidence in a stable format.** PDF exports of policies, screenshot captures of configurations with visible timestamps, and saved copies of logs are more durable than live links to systems that may change. (Hashing these artifacts is not required for self-assessments—the requirement applies only to C3PAO and DIBCAC assessments—but OSAs anticipating a future certification assessment may find it worthwhile to adopt the practice early. The DoW CIO publishes a CMMC Hashing Guide containing instructions.)
- **Record the CMMC Status Date prominently.** The six-year clock runs from that date. Every evidence artifact should be traceable to the assessment it supported.
- **Designate an owner.** Evidence retention without an owner decays. Assign responsibility, ideally to the same role that supports the annual affirmation.
- **Keep it accessible.** Evidence retained on a system that was later decommissioned, in a vendor tool that was replaced, or in a personal drive that left with an employee is effectively not retained.

6. Scoring and the POA&M

The CMMC scoring methodology at 32 CFR § 170.24 is deterministic. Each of the 110 Level 2 requirements carries a point value of 1, 3, or 5. A MET or NOT APPLICABLE finding contributes the full point value to your score. A NOT MET finding subtracts that point value from the maximum of 110. The result can be negative: the scoring range runs from a maximum of 110 to a theoretical minimum of -203. In practice, any score below 88 disqualifies the OSA from Conditional status.

How Points Are Weighted

POINT VALUE	WHAT IT MEANS	EXAMPLES
5 points	Basic and derived security requirements that, if not implemented, could lead to significant exploitation of the network or exfiltration of CUI.	AC.L2-3.1.1 (Authorized Access Control); IA.L2-3.5.1 (Identification); SC.L2-3.13.1 (Boundary Protection).
3 points	Requirements that, if not implemented, have a specific and confined effect on the security of the network and its data.	CM.L2-3.4.3 (Track and Review Changes); AU.L2-3.3.4 (Audit Failure Alerting).
1 point	Requirements that, if not implemented, have a limited or indirect effect on the security of the network and its data.	AT.L2-3.2.3 (Insider Threat Awareness); CA.L2-3.12.2 (Plan of Action).

Conditional vs. Final Status

A passing self-assessment results in one of two CMMC Statuses:

- **Final Level 2 (Self)** is achieved when all 110 requirements are MET. The score is 110 and no POA&M exists.
- **Conditional Level 2 (Self)** is achieved when the score is at least 88 (80% of 110), the remaining NOT MET items are eligible for a POA&M, and the POA&M complies with the rules below. Conditional status expires if the POA&M is not closed out within 180 days. Closing out the POA&M requires a POA&M closeout self-assessment and an updated SPRS submission.

POA&M Rules at a Glance

The rule that governs POA&M eligibility is straightforward, but it is often summarized in a way that obscures what actually controls the outcome. Of the 110 Level 2 requirements, **62 cannot be placed on a POA&M at all**—all 42 five-point requirements, all 14 three-point requirements, and six specific 1-point requirements, including CA.L2-3.12.4 (which has no point value but is a prerequisite for the assessment itself). Only the remaining 48 one-point requirements are POA&M-eligible by default.

RULE	PRACTICAL IMPLICATION
Minimum score of 88 / 110 (80%)	You cannot achieve Conditional status with a score below 88. A single 5-point NOT MET combined with a handful of 3-point NOT METs puts you at the edge quickly. Treat high-value requirements as priority-one for implementation.
No requirement with a point value greater than 1 may be on a POA&M	Every 5-point and 3-point requirement must be MET or N/A at the time of the self-assessment. This is the dominant rule and the one most likely to disqualify a contractor from Conditional status. There is one narrow exception: SC.L2-3.13.11 (CUI Encryption) may be on a POA&M if encryption is employed but not FIPS-validated (3 points deducted). If encryption is not employed at all, the requirement is fully non-POA&M-able (5 points deducted).
Six additional 1-point requirements are also carved out and cannot be on a POA&M	The following 1-point requirements must all be MET at the time of the self-assessment: • **AC.L2-3.1.20** (External Connections) • **AC.L2-3.1.22** (Control Public Information) • **CA.L2-3.12.4** (System Security Plan) • **PE.L2-3.10.3** (Escort Visitors) • **PE.L2-3.10.4** (Physical Access Logs) • **PE.L2-3.10.5** (Manage Physical Access)
Partial credit can apply to two requirements	• **IA.L2-3.5.3** (MFA): 3 points deducted if MFA is implemented only for remote and privileged users; 5 points if not implemented for any users. • **SC.L2-3.13.11** (CUI Encryption): 3 points deducted if encryption is employed but not FIPS-validated; 5 points if encryption is not employed. Only SC.L2-3.13.11 in its 3-point (non-FIPS) state may be placed on a POA&M. IA.L2-3.5.3 is not POA&M-eligible in either partial state.
CA.L2-3.12.4 (System Security Plan) is treated specially	Per 32 CFR § 170.24, **CA.L2-3.12.4** has no associated point value. A missing or incomplete SSP does not deduct points; instead, the assessment cannot be completed. The finding is "an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012." An up-to-date SSP is a prerequisite for any CMMC assessment to proceed.
180-day closeout	A POA&M closeout self-assessment must be completed and submitted to SPRS within 180 days of the Conditional CMMC Status Date. If the POA&M is not closed out in time, the Conditional status expires and the OSA becomes ineligible for awards with a Level 2 (Self) or higher requirement until a new status is achieved.

7. Reporting Your Results: SPRS and the Affirmation

"Clicking the buttons in SPRS is not the same as performing a self-assessment. It is how you report the results of one."

The self-assessment results are reported in the Supplier Performance Risk System (SPRS) at **https://www.sprs.csd.disa.mil**. The submission is not the assessment; the submission is how the Government receives the result of your assessment and relies on it for contract eligibility.

What You Submit

32 CFR § 170.16(a)(1)(i) specifies the minimum information an OSA must submit when recording a Level 2 self-assessment in SPRS:

CMMC Level
The assessment level being reported (Level 2 Self).

CMMC Status Date
The date of the assessment. This date anchors the three-year validity period and the six-year evidence retention clock.

CMMC Assessment Scope
The defined boundary of the information system(s) assessed (i.e., Enterprise, Enclave).

CAGE Code(s)
All industry CAGE codes associated with the information systems within the CMMC Assessment Scope.

Overall Score
The numeric score, expressed out of 110.

POA&M Usage and Compliance Status
If applicable, whether a POA&M is in place and whether it is currently compliant with CMMC POA&M rules.

FURTHER GUIDANCE: SPRS SCORE SUBMISSION WALKTHROUGH

For a step-by-step walkthrough of SPRS score submission mechanics—including how the system presents each requirement, how to record assessment objective findings, and how to submit the affirmation—see this training deck: **Overview: Supplier Performance Risk System.**

7. Reporting Your Results: SPRS and the Affirmation

The Annual Affirmation

After each self-assessment, a senior Affirming Official within the OSA submits an affirmation in SPRS. The affirmation states that the organization has implemented and will maintain the applicable CMMC security requirements within the defined Assessment Scope. Affirmations are required:

- **Upon achieving Conditional Level 2 (Self) status.**
- **Annually following the Final CMMC Status Date.**
- **Upon achieving Final Level 2 (Self) status.**
- **After a POA&M closeout self-assessment**

THE AFFIRMING OFFICIAL

The Affirming Official is defined in 32 CFR § 170.4 as “the senior level representative from within each Organization Seeking Assessment who is responsible for ensuring the OSA’s compliance with the CMMC Program requirements and has the authority to affirm the OSA’s continuing compliance.”

In practice, this is typically an executive. What they are signing is an attestation—a statement of fact—submitted to the United States Government. That attestation carries legal weight under the False Claims Act. The affirmation is not a routing step; it is a personal commitment. The person signing should have reviewed the assessment results and understand what they are certifying.

8. Accountability After the Fact

It is worth remembering why CMMC exists. For years, defense contractors self-attested to NIST SP 800-171 compliance under DFARS clause 252.204-7012 on a trust basis, and the results were uneven. CMMC introduces structure: an assessment methodology, third-party verification for most contractors, and—critically for self-assessors—an **investigation right** the Government can exercise at any time.

A self-assessment is not self-governed. The framework that makes a self-assessment credible is the Government's ability to verify it after the fact, and the OSA's ongoing obligation to maintain the implementation they attested to.

What This Means in Practice

- **Your self-assessment score is not the final word.** A DCMA DIBCAC finding supersedes it. If DIBCAC assesses your program and reaches different conclusions, their assessment controls.
- **A DCMA DIBCAC assessment can be triggered at any time.** The investigation right does not expire with the contract. This is why evidence must be retained for six years from the CMMC Status Date.
- **The annual affirmation is an ongoing attestation.** It is the Affirming Official's yearly statement that the program remains in the state it was assessed in. Material changes to the system require a new self-assessment and a new affirmation.
- **False Claims Act exposure follows the attestation.** A score submitted to SPRS is a statement of fact to the United States Government. An unsubstantiated score is a misrepresentation. The mechanism that makes this actionable is the DCMA DIBCAC investigation right described above.

FROM THE RULE

"The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSA… If the investigative results of a subsequent DCMA DIBCAC assessment show that adherence to the provisions of this part have not been achieved or maintained, **these DCMA DIBCAC results will take precedence** over any pre-existing CMMC Status. At that time, **standard contractual remedies will be available** and **the OSA will be ineligible for additional awards** with CMMC Status requirement of Level 2 (Self), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved."

32 CFR § 170.16(a)(1)(iv) [emphasis added]

"The trust is extended at contract award. The verification right runs for six years behind it."

9. What "Good Enough" Looks Like

Below is a plain-language checklist you can apply to your own program before submitting a score. If you cannot answer "yes" to each item honestly, your self-assessment is not yet defensible. These tests are cumulative—each one matters, and none of them substitutes for the others.

1. **Your system is built and running.**
   Not planned, not mostly there. The controls are in place, operating, and generating the kind of evidence an assessor would expect to see.
2. **Your documentation is final, not draft.**
   Your System Security Plan, policies, and procedures are approved, signed where appropriate, and represent how the organization actually operates.
3. **You've looked at every assessment objective, not just every requirement.**
   The 110 requirements break down into 320 objectives. You have worked through each one and made a judgment about whether the evidence supports a MET finding.
4. **Your evidence covers the whole scope, not just one favorable example.**
   If you have 50 laptops in scope, your evidence reflects 50 laptops. Checking the IT director's laptop and calling it done is not coverage.
5. **You've used more than one method where it matters.**
   For many objectives, examining a document alone is insufficient. Where applicable, you interviewed the people doing the work and observed the control functioning.
6. **You can explain every MET determination.**
   If DCMA DIBCAC showed up next week and asked "how do you know this control is working?"—you have a clear answer and the evidence to back it up.
7. **Your POA&M is honest.**
   If something is not fully implemented, it is on the POA&M. You have not stretched a NOT MET into a MET to avoid a Conditional status or preserve a score.
8. **You've retained your evidence in final form.**
   Everything you relied on is organized, labeled, and set aside for six years. Not scattered across laptops, not only in someone's head, not only in draft folders.
9. **Your Affirming Official has actually reviewed the results.**
   The affirmation is a legal attestation. The person signing understands what they are attesting to and has seen the evidence that supports it.

10. Where Level 2 (Self) Fits in the CMMC Program

The CMMC Program defines four assessment statuses: Level 1 (Self), Level 2 (Self), Level 2 (C3PAO), and Level 3 (DIBCAC). Each is associated with a specific population of contractors based on the type of information the contract involves.

Level 2 (Self) applies to a defined, and relatively narrow, population: contractors handling Controlled Unclassified Information that falls outside the **CUI Registry**'s Defense Organizational Index Grouping. When CUI falls inside that grouping—which includes categories like Controlled Technical Information, Naval Nuclear Propulsion Information, DoD Critical Infrastructure Security Information, and Unclassified Controlled Nuclear Information—Level 2 (C3PAO) is the minimum assessment requirement. The DoW's January 2025 implementation guidance establishes this clearly.

One important caveat: during Phase 1 of the CMMC rollout, which began in November 2025 and runs through November 2026, program managers are directed to include Level 2 (Self) requirements in applicable DoW solicitations, with Level 2 (C3PAO) included only at the program manager's discretion.

That said, contractors handling Covered Defense Information under DFARS clause 252.204-7012 almost universally handle CUI in the Defense Organizational Index Grouping. For those contractors, Level 2 (Self) is the assessment status that applies today for a given contract—not necessarily the assessment status that will apply to every future DoW contract they pursue.

Level 2 (Self) is a permanent part of the CMMC Program. Contractors whose CUI exposure remains outside the Defense Organizational Index Grouping will continue to self-assess and reaffirm for as long as they hold those contracts. The triennial reassessment and annual affirmation cycles will apply in perpetuity.

How C3 Supports Level 2 Self-Assessments

C3 has guided hundreds of DIB contractors through CMMC Level 2 readiness. Our approach is deliberate: time- and cost-efficient engagements, high confidence in assessment outcomes, and a bias toward getting you to a defensible score without duplicated effort.

What We Do

- Implementation. We design, build, and document the information system that will be assessed—whether that is an enclave or the full enterprise environment. Our implementations are built against the 320 assessment objectives from the start, so the evidence you need for the assessment is generated by the system as it runs.
- Evidence organization and assessment preparation. We help organize the evidence required to substantiate each assessment objective, in a structure that supports both the initial self-assessment and the annual affirmations that follow.
- Pre-Assessment Readiness Review. A Pre-Assessment Readiness Review is a structured, project-based engagement that walks an OSA through the same objectives, methods, and determinations a C3PAO would apply. It identifies gaps before the SPRS submission locks the score in. A Pre-Assessment Readiness Review requires that the system is implemented, operational, and fully documented—the same preconditions as a real self-assessment.

FACING A CONTRACTUAL LEVEL 2 (SELF) REQUIREMENT? CONSIDER THIS BEFORE YOU PROCEED.

Before committing to a self-assessment path, ask:

1. What CUI does this contract actually involve? Map the CUI categories to the Defense Organizational Index Grouping. If any of it falls inside that grouping, Level 2 (C3PAO) is the appropriate steady-state minimum. During Phase 1 of the CMMC rollout (November 2025 through November 2026), the program office may specify Level 2 (Self) even for applicable solicitations; it is worth asking the Contracting Officer if the contract is expected to require Level 2 (C3PAO) after Phase 1.
2. Is this requirement representative of your full DoW portfolio? A Level 2 (Self) requirement on one contract does not mean your next contract will specify the same. If your business plans to pursue work involving Defense Organizational Index CUI, your compliance program will eventually need to meet the C3PAO standard.
3. If a future contract requires Level 2 (C3PAO), will your self-assessment evidence substantiate that level? The work required for a high-integrity self-assessment and the work required for a C3PAO assessment are substantially the same. Preparing for certification while executing the self-assessment avoids duplicative effort.

Get in Touch

If you are facing a Level 2 (Self) requirement or preparing an annual affirmation and want to talk through your path, reach out. We can help you understand what is in front of you, what your realistic timeline looks like, and what a defensible self-assessment requires.

Visit c3isit.com or contact your C3 representative.

Sources and Further Reading

- **32 CFR Part 170—Cybersecurity Maturity Model Certification (CMMC) Program.** Published in the Federal Register, October 15, 2024. The authoritative regulatory text for the CMMC Program. [Link]
- **NIST SP 800-171 Revision 2—Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.** The 110 security requirements assessed at Level 2. [Link]
- **NIST SP 800-171A Jun2018—Assessing Security Requirements for Controlled Unclassified Information.** The 320 assessment objectives, the three assessment methods, and the depth / coverage framework. [Link]
- **CMMC Assessment Guide—Level 2.** Published by DoW CIO. Provides interpretive guidance for assessing each Level 2 security requirement. [Link]
- **CMMC Scoping Guide—Level 2.** Published by DoW CIO. Defines how to identify the CMMC Assessment Scope and categorize assets. [Link]
- **January 2025 OSD Memo—Implementing the CMMC Program: Guidance for Determining Appropriate CMMC Compliance Assessment Levels.** Policy guidance on how program managers determine the required CMMC level for a given contract. [Link]

A NOTE ON IMPARTIALITY

C3 does not perform formal assessments of systems C3 has implemented or operates. This is a requirement of the Cyber AB Code of Professional Conduct. When C3 provides a Pre-Assessment Readiness Review, it is a support engagement that helps the OSA prepare for and execute their own self-assessment—the OSA remains accountable for every MET / NOT MET determination, the SPRS submission, and the Affirming Official attestation.

Glossary

TERM	DEFINITION
Affirming Official	The senior representative within an OSA who is responsible for ensuring CMMC compliance and has the authority to affirm continuing compliance. Defined in 32 CFR § 170.4.
C3PAO	CMMC Third-Party Assessor Organization. Performs Level 2 certification assessments.
CAGE Code	Commercial And Government Entity code. A unique identifier assigned to suppliers of government agencies.
CMMC	Cybersecurity Maturity Model Certification.
CUI	Controlled Unclassified Information.
DCMA DIBCAC	Defense Contract Management Agency, Defense Industrial Base Cybersecurity Assessment Center. Conducts Level 3 certification assessments and has the right to conduct investigative assessments at Level 2.
DFARS	Defense Federal Acquisition Regulation Supplement.
DoW	Department of War. References to DoD (Department of Defense) in regulatory text refer to the same entity.
ESP	External Service Provider. May include MSPs, MSSPs, CSPs, and other vendors that support an OSA's information system.
FCI	Federal Contract Information.
MET / NOT MET / N/A	The three possible findings for each assessment objective in a Level 2 assessment.
OSA	Organization Seeking Assessment. The term for any organization undergoing a CMMC assessment, whether self or third-party.
POA&M	Plan of Action and Milestones. A remediation plan for NOT MET requirements, used to achieve Conditional status.
SPRS	Supplier Performance Risk System. The DoW system where CMMC self-assessment scores and affirmations are submitted.
SSP	System Security Plan. The document that describes how an organization meets each of the CMMC Level 2 requirements.

This document is provided for informational purposes only and does not constitute legal advice.