A POSITION FROM DEEP FATHOM

Cybersecurity is not paperwork.

The Department paused third-party certification. It did not pause the obligation to protect defense information. What replaces Phase II should verify security rather than restate it.

FOR	The CMMC Reform Task Force, DIB suppliers, and the people who assess them
ARGUES	Keep the Level 2 security baseline. Change how it gets verified.
REVIEWED	August 2026 · v2.0

> This industry position and working system have no Government endorsement. Nothing here changes what a supplier owes today under DFARS 252.204-7012 or under CMMC Phase I.

WHAT CHANGED

The certification stopped. The obligation did not.

On July 13, 2026 the Department of War suspended CMMC Phase II, the third-party certification milestone set for November 10, 2026, and held the later phases pending its program review. Everything a supplier already owed, it still owes.

SUSPENDED	Phase II third-party certification, plus pending and future CMMC implementation milestones across Department solicitations and contracts.
STILL IN FORCE	Phase I self-assessment and affirmation, SPRS reporting, and safeguarding obligations under DFARS 252.204-7012.
IN CONTRACTS NOW	Contracting officers may include Level 1 (Self) or Level 2 (Self) assessment requirements only, until further notice.
UNDER REVIEW	The Department's CMMC Reform Task Force, its program review, and a public request for information on cost, burden, and reform.

THE SCALE BEHIND THE PAUSE

120k

SMALL BUSINESSES IN SCOPE

SBA's count of DIB small firms Phase II would have reached

~100

APPROVED ASSESSORS

The certification capacity available to meet that demand

The Task Force reviews the program and recommends changes. The Department retains authority over policy, rulemaking, and contract requirements.

Department suspension announcement SBA small-business statement

> Public statements from the Department and the SBA as of August 2026. The Task Force has not published findings, and nothing here predicts what it will recommend.

THE COST QUESTION

Three costs are being counted as one.

The public figures for CMMC cost measure different things. Folded into one number, they hide the part that reform can actually reach through better evidence and verification.

SBA · JULY 2026

$388,600
self-assessment

$593,800
third-party certification

Total small-firm compliance cost. The public release does not decompose the estimate.

CMMC FINAL RULE · 2024

$34,277
Level 2 self-assessment

$101,752
certification assessment

Each includes initial affirmation and assumes NIST SP 800-171 is already implemented.

1 · BUILD	Controls, architecture, technology, people, remediation, and security operations. Correct scope and commercial capability reduce it. Reform does not remove it.
2 · PROVE	SSP content, implementation statements, mappings, provenance, updates, and reconciliation. A common evidence profile and source-linked records cut the rewriting.
3 · VERIFY	Self-assessment, independent assessment, Government review, and every downstream request for facts that have not changed. Graduated verification, deterministic checks, and controlled reuse cut the repetition.

Dropping the C3PAO requirement does not touch Layer 1. Nearly everything reform can reach through program design sits in Layers 2 and 3.

SBA cost context CMMC final rule · 89 FR 83092

> These two estimates are not competing measurements of the same quantity and should not be subtracted from one another. The rule's model assumes NIST SP 800-171 is already implemented. The SBA figure does not.

THE POSITION

Keep the standard. Change five parts of the work.

None of these lowers the baseline. Each one changes where security facts come from, how often they get rechecked, and how many times a person has to re-enter them.

01 **Automation over documentation**

Collect security facts from the systems that produce them. A configuration export beats a paragraph describing the configuration.

02 **Continuous over point-in-time**

Recheck the claims a change actually affects, when it happens. A three-year cycle cannot see the two years in between.

03 **Assessment-ready over dashboard green**

Hold evidence a reviewer can trace to its source, date, and scope, and then challenge. A score without its basis is an assertion.

04 **Accessible over enterprise-only**

A twelve-person machine shop should reach the same baseline without an enterprise security program. The cost of proving security should not decide who stays in the DIB.

05 **Ecosystem-wide over contractor-only**

Providers, advisors, assessors, and primes each hold part of the record. Publish responsibility once instead of re-deriving it for every customer.

> The Department sets verification tiers, evidence requirements, and acceptable error limits. CMMC 20X supplies an implementable proposal for that decision.

THE BLUEPRINT

The security work should produce the proof.

Six steps run continuously. Assessment tests a maintained record, and suppliers update it between reviews.

01 · SCOPE

Name the data, the systems, the people, the providers, and the owners. Establish the boundary before anyone spends against the wrong one.

02 · PROTECT

Implement the safeguards. Close what is missing, and say plainly what is not closed yet.

03 · RECORD

Keep each claim with its evidence, source, collection date, scope, and stated limitations.

04 · CHECK

Run repeatable tests. Surface conflicts and keep them open for review.

05 · DECIDE

Record the human finding, the reviewer, and the authority behind the decision.

06 · UPDATE

Reopen only the claims affected by a change.

Maintain once. Recheck what changes. Each assessment tests the current source-linked record. The supplier updates affected claims.

The safeguards and decision authority remain. Repeated reconstruction ends.

WORKED EXAMPLE

Use software for repetition. Use people for judgment.

One synthetic Level 2 claim, carried from source to finding. The interesting part is what happens when the sources disagree.

SYNTHETIC | IA.L2-3.5.3

MFA is enforced for privileged access.

POLICY	All administrators require MFA. Access control policy section 4.2, revision dated 2026-06-04.
OBSERVED	The identity provider export shows MFA for all 24 accounts it can see. Collected 2026-08-02; scope limited to the production tenant.
CONFLICT	A local emergency account sits outside that export. Its MFA coverage is unknown. The policy statement does not close the gap.

SOURCE

Says what was observed, where, when, and at what scope.

SOFTWARE

Tests the rules it knows, holds the conflict open, and refuses to close it.

HUMAN

Judges scope and consequence. An authorized person records the finding.

A clean export cannot prove an unseen access path.

A synthetic record shown for illustration. It touches objectives 3.5.3[a] through [c] only. A real determination needs the full objective set, the assessment scope, and an authorized assessor's finding.

THE PROPOSAL

Let risk determine the verification route.

Replace the binary choice between self-assessment and C3PAO certification with graduated tiers. Risk sets the tier. Evidence quality decides how hard you look inside it.

TIER BY	Data sensitivity, mission consequence, threat exposure, supplier criticality, and material change.
EVIDENCE QUALITY	Weak or incomplete evidence triggers sampling, correction, or escalation within the assigned tier. Risk still determines the tier.
METHODS	Evidence-backed self-assessment. AI-assisted review with accountable human validation. C3PAO assessment. Targeted Government review.
EACH DEFINES	Who produces the evidence, who reviews it, who owns the decision, what the result may be used for, and how it gets corrected or appealed.

TWO OF SEVEN MODELED PATHS

REOPEN UNCHANGED

97%
CURRENT ASSURANCE IN 2049

36%
CUMULATIVE SUPPLIER ATTRITION

EXPOSURE TARGET SUSTAINED · FEB. 2031

The modeled backlog falls because suppliers exit while the delay remains.

GRADUATED VERIFICATION

90%
CURRENT ASSURANCE IN 2049

3%
CUMULATIVE SUPPLIER ATTRITION

EXPOSURE TARGET SUSTAINED · FEB. 2034

87% of conditional-policy runs land inside the modeled outcome envelope.

`model bf91444e3fcc  conditional systems analysis  medians · 100 paired runs per path  analysis methodology`

> The exposure date begins 12 consecutive months at or below 0.35. These are conditional model results under stated assumptions. They are not forecasts. Seven paths were modeled and two are shown. The model says nothing about what the Department will decide, or what any single supplier will experience.

THE WORKING SYSTEM

The software is ready for evaluation.

Deep Fathom runs a working implementation of this blueprint. The system is ready for independent evaluation against Government-defined cases, reference findings, and acceptance thresholds.

110
NIST SP 800-171 REV 2 REQUIREMENTS
represented in the working compliance graph

320
CMMC LEVEL 2 ASSESSMENT OBJECTIVES
each carrying source, evidence, and review state

01
SOURCE RECORD
behind the SSP, assessment, and POA&M views

01 Every requirement maps to its assessment objectives.

02 Implementation statements connect directly to their evidence.

03 Deterministic checks run first. AI-assisted review handles what needs interpretation.

04 Conflicts stay visible. Open remediation stays open.

05 Source links, collection dates, ownership, and review state survive the next change.

06 The finding belongs to a person, and so does every consequential decision after it.

Examine the working implementation ↗

> The working system is ready for independent evaluation. The Government defines the cases, thresholds, authorized uses, and stop rules.

THE NEXT MOVE

Four recommendations for Department action.

01 **Define the graduated verification model**

The tiers, the risk criteria, and for each method the evidence producer, the reviewer, the decision owner, the permitted uses, and the appeal path.

02 **Define a vendor-neutral evidence profile**

Drafted on OSCAL. Human-readable and machine-readable views generated from one source record. Conformance tests published so no vendor owns the standard.

03 **Clarify scope, inheritance, and commercial service rules**

Worked examples for CUI boundaries, provider classification, inherited responsibility, and what a commercial component actually has to prove.

04 **Charter an independent evaluation**

Several implementations review the same synthetic Level 2 packages against Government reference findings. Measure accuracy, disagreement, correction, and failure. No effect on CMMC status, SPRS, award, or enforcement until the Department sets error limits.

READ THE ARGUMENT

cmmc20x.com/blueprint
cmmc20x.com/analysis
cmmc20x.com/product
cmmc20x.com/evaluation

CHALLENGE THE MODEL

Bring a real or synthetic evidence package, conflict, or responsibility boundary this system has to handle. The disagreements are the useful part.

deepfathom.ai
cmmc20x@deepfathom.ai