
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 comes next should verify security rather than restate it.

FOR

The CMMC Reform Task Force, DIB suppliers, and the people who assess them

POSITION

Keep the Level 2 security baseline. Change how it gets verified.

WHAT CHANGED

The certification stopped. The obligation did not.

On July 13, 2026, the Department suspended CMMC Phase II and held later implementation phases pending review. Everything a supplier already owed, it still owes.

PAUSED

Third-party certification

The Phase II milestone and later CMMC implementation phases are suspended until further notice.

STILL IN FORCE

The security obligation

Phase I self-assessment and affirmation, SPRS reporting, and safeguarding duties under DFARS 252.204-7012 remain.

The CMMC Reform Task Force is reviewing the program and can recommend changes. The Department retains policy, rulemaking, and contracting authority.

THE COST QUESTION

Three costs are being counted as one.

Build the security. Prove it. Verify it. Reform cannot remove the first cost. It can stop the second and third from repeating.

01	BUILD	Controls, architecture, technology, people, remediation, and security operations.
02	PROVE	Claims, evidence, scope, provenance, updates, and reconciliation.
03	VERIFY	Self-assessment, independent assessment, Government review, findings, and correction.

SBA · JULY 2026

\$388.6k / \$593.8k

Reported small-firm self-assessment and third-party certification costs.

CMMC FINAL RULE · 2024

\$34.3k / \$101.8k

Level 2 self-assessment and certification estimates under different assumptions.

THE POSITION

Keep the standard. Change five parts of the work.

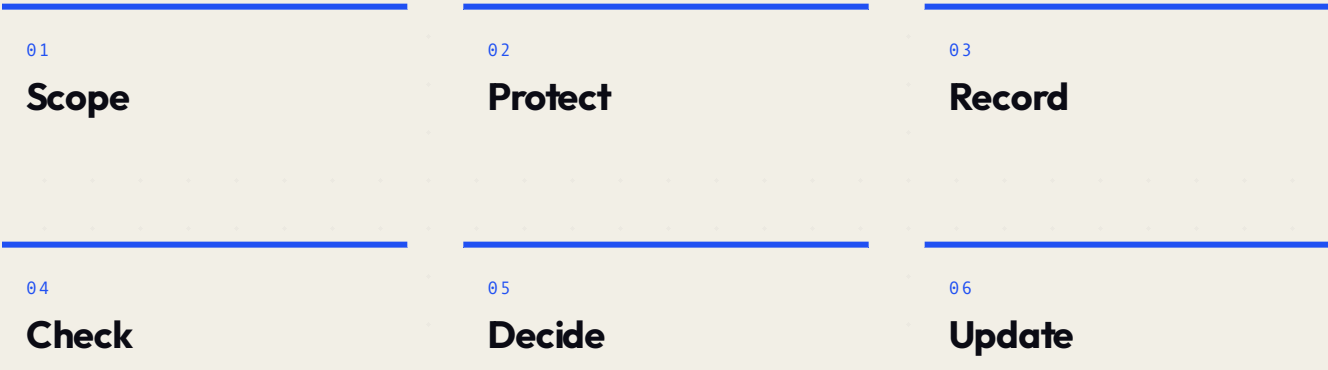
None lowers the baseline. Each changes where security facts come from, how often they get rechecked, and how many times someone has to re-enter them.

-
- 01 **Automation over documentation**
Collect security facts from the systems that produce them.
 - 02 **Continuous over point-in-time**
Recheck the claims a material change actually affects.
 - 03 **Assessment-ready over dashboard green**
Keep evidence a reviewer can trace, test, and challenge.
 - 04 **Accessible over enterprise-only**
Keep the same baseline within reach of small suppliers.
 - 05 **Ecosystem-wide over contractor-only**
Carry provider and partner responsibility in the same record.
-

THE BLUEPRINT

The security work should produce the proof.

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



Keep each claim with its evidence, source, collection date, scope, and stated limitations. Reopen only what a material change affects.

THE PROPOSAL

Let risk determine the verification route.

Replace the binary choice between self-assessment and C3PAO certification with graduated routes. Risk sets the route; evidence quality governs scrutiny inside it.

ROUTE BY

Data sensitivity

Mission consequence

Threat exposure

Supplier criticality

Material change

EVIDENCE QUALITY

Weak evidence triggers correction, sampling, or escalation within the assigned route. Risk still determines the route.

Conditional medians from 100 paired runs per policy option · exposure date begins 12 months ≤ 0.35 · no forecast

Reopen unchanged

97%

CURRENT ASSURANCE
IN 2049

36%

CUMULATIVE SUPPLIER
ATTRITION

Feb. 2031 EXPOSURE TARGET SUSTAINED

Graduated verification

90%

CURRENT ASSURANCE
IN 2049

3%

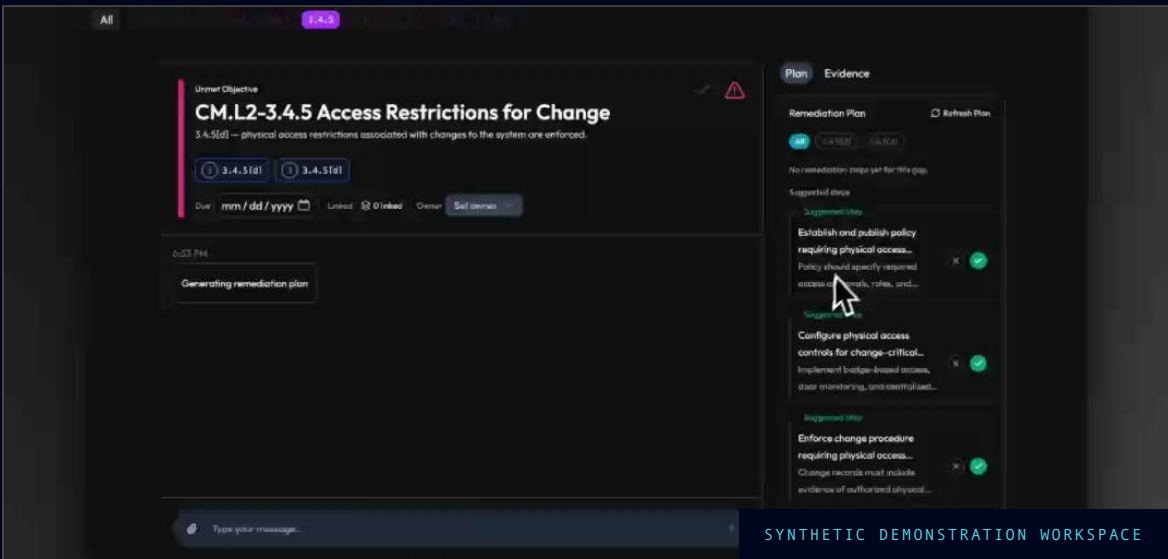
CUMULATIVE SUPPLIER
ATTRITION

Feb. 2034 EXPOSURE TARGET SUSTAINED

WORKING SOFTWARE · SYNTHETIC DATA

Working software, ready for evaluation.

Deep Fathom already represents the Level 2 model, links claims to evidence, keeps conflicts open, and separates machine analysis from human findings.



110

Level 2 requirements represented

320

Assessment objectives connected

1

Source-linked operating record

THE NEXT MOVE

Four recommendations for Department action.

01 Define the graduated verification model

Set the routes, risk criteria, reviewers, decision owners, permitted uses, correction, and appeal.

02 Define a vendor-neutral evidence profile

Generate human-readable and machine-readable views from one source record, with public conformance tests.

03 Clarify scope, inheritance, and commercial services

Publish worked examples for boundaries, provider classification, inherited responsibility, and required proof.

04 Charter an independent evaluation

Test multiple implementations against Government reference findings before operational reliance.

Read the complete argument

cmmc20x.com/briefing
cmmc20x.com/blueprint
cmmc20x.com/analysis

Examine or challenge it

cmmc20x.com/evaluation
deepfathom.ai
cmmc20x@deepfathom.ai