

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.

THE POSITION

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

THE POLICY STATE

The certification stopped. The obligation did not.

Phase II and later milestones were suspended.
Existing safeguards, reporting, and current
contract duties remain.

~~Paused~~

Phase II third-party certification

Advancement to later implementation phases

Still in force

Phase I self-assessment and affirmation

SPRS reporting and DFARS safeguarding duties

WHO DECIDES

The Task Force reviews and recommends. The Department retains policy, rulemaking, and contract authority.

BUILD • PROVE • VERIFY

Three costs are being counted as one.

Security work remains. Reform can sharply reduce repeated proof and verification work.

WHERE REFORM CAN HELP MOST

01

Build

Controls, architecture, people, remediation, and security operations.

02

Prove

Implementation statements, mappings, sources, updates, and reconciliation.

03

Verify

Assessment, review, and repeated requests for facts that have not changed.

Removing a review step does not implement a safeguard.

Public cost estimates span different scopes; do not subtract them.

KEEP THE LEVEL 2 BASELINE

Keep the standard. **Change five parts** of the work.

Change where security facts come from, how often they are checked, and how often people must re-enter them.

- | | | |
|----|--|--|
| 01 | Automation over documentation | Collect security facts from the systems that produce them. |
| 02 | Continuous over point-in-time | Recheck what changed, when it changed. |
| 03 | Assessment-ready over dashboard green | Preserve source, date, scope, and limits. |
| 04 | Accessible over enterprise-only | Reach the same baseline without enterprise-scale overhead. |
| 05 | Ecosystem-wide over contractor-only | Make responsibility follow the work across organizations. |

THE BLUEPRINT

The security work should **produce the proof.**

In the proposed model, assessment tests evidence already current. Suppliers maintain the record between reviews.

01

Scope

Name the boundary and owners.

02

Protect

Implement the safeguards.

03

Record

Keep claims with their sources.

04

Check

Run repeatable tests.

05

Decide

Record the human finding.

06

Update

Reopen only affected claims.

Maintain once. Recheck what changes. ↻

Source + date + scope + limitations travel with every claim.

ONE CLAIM, THREE SOURCES

Use software for repetition.
Use people for judgment.

A contradiction stays open until an authorized person judges its scope and consequence.

IA.L2-3.5.3 MFA is enforced for privileged access.			
POLICY All admins The written rule requires MFA.	IDENTITY EXPORT 24 / 24 Every account in the export shows enforcement.	LOCAL ACCOUNT Outside export An emergency access path remains unseen.	Open Software preserves the conflict.

HUMAN FINDING A clean export cannot prove an unseen access path.

THE PROPOSAL

Let **risk** determine the verification route.

Keep the Level 2 safeguards. Replace the binary route with verification depth matched to consequence.

Risk sets the verification route.

Evidence quality triggers sampling, correction, or escalation inside it.

CUMULATIVE SUPPLIER ATTRITION	Reopen unchanged		Graduated verification	
	36%	97%	3%	90%
CURRENT ASSURANCE IN 2049	suppliers lost	current assurance	suppliers lost	current assurance

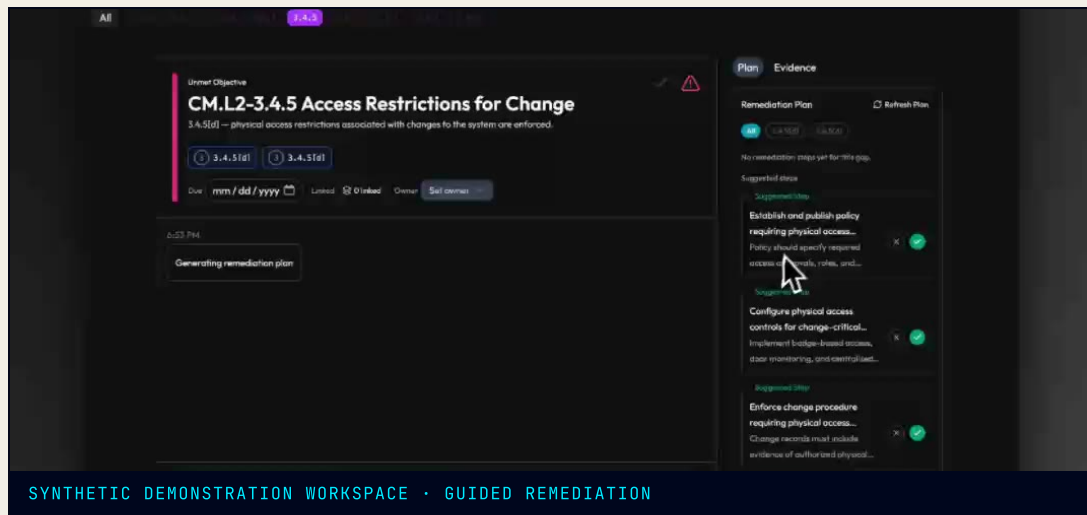
Exposure target sustained (12 months ≤ 0.35): Feb. 2031 · reopen unchanged / Feb. 2034 · graduated verification

Medians · 100 paired runs per path · model bf91444e3fcc · conditional results

DEEP FATHOM SOFTWARE

Working software, ready for evaluation.

A working, source-linked implementation spans the Level 2 requirement and assessment-objective set.



110

NIST SP 800-171 Rev. 2 requirements

320

CMMC Level 2 assessment objectives

01

source-linked record behind every generated view

READY FOR CONTROLLED
EVALUATION

Measure accuracy, disagreement, correction, and reviewer effort on Government-defined cases.

WHAT COMES NEXT

Four recommendations for Department action.

The Task Force can review and recommend.
The Department defines the policy, methods,
and acceptance conditions.

01 Define graduated verification

Set tiers, risk criteria, reviewers, decision owners, uses, correction, and appeal.

02 Define a vendor-neutral evidence profile

Produce human and machine views from one source, with public conformance tests.

03 Clarify scope and inheritance

Publish worked examples for boundaries, providers, shared responsibility, and services.

04 Charter an independent evaluation

Compare implementations on the same synthetic cases and reference findings.

Keep the baseline. Modernize how it is proved and verified.

cmmc20x.com · cmmc20x@deepfathom.ai