FOUNDATIONAL PAPER

Introducing CMMC 20X

Five changes to how CMMC evidence is collected, reviewed, reused, and updated.

STATUS	LAST REVIEWED	RESEARCH LANES	CLAIM REGISTER
Revised	**August 13, 2026**	**Vision · Principles · Mechanism**	**V-01 · V-02 · V-03 · V-04 · V-05 · V-06 · V-07 · C-06 · C-07 · C-15**

The original January thesis, revised to reflect Deep Fathom authorship, software boundaries, and the current claim register.

CMMC asks an important question: does a contractor protect controlled information well enough to support the mission?

Too much of the work required to answer that question happens after the fact. A contractor assembles screenshots, exports, policies, tickets, and explanations. An advisor reorganizes them. An assessor reconciles them before testing the system. A provider answers similar questions for many customers. Then the environment changes and much of the package begins to age.

CMMC 20X starts from a different premise: **the security work should produce the proof.**

An identity system knows which accounts use MFA. A ticket shows when a weakness was fixed. A backup test shows whether recovery worked. A provider knows what its service protects and what the customer must configure. Keep those facts with the CMMC claims they support. Generate documents from that record instead of rebuilding the record for every review.

Five changes to the work

1. Stop rewriting the same facts

Collect evidence from the system or person that knows it. Map it to CMMC once. Use that record to produce the SSP, evidence index, readiness review, provider statement, and assessment package.

Software is useful for collection, mapping, counts, dates, broken references, and known rules. A file that passes those checks can still contain weak evidence.

2. Check again when the system changes

An assessment begins aging as soon as accounts, software, providers, or boundaries change. Give each claim a review date. When a material change occurs, reopen the claims and findings that depended on the old state.

History remains visible. Old evidence simply stops pretending to describe the current system.

3. Prepare evidence someone else can test

A green dashboard is an internal opinion. An assessor needs to know what the claim covers, where the evidence came from, when it was collected, which population it covers, who owns the work, what conflicts with it, and what remains unresolved.

Readiness means another qualified person can trace and test the claim.

4. Make security achievable

A small manufacturer should spend its limited security budget on MFA, backups, logging, patching, recovery, and qualified help. Rebuilding the same evidence for every customer and reviewer does not add another safeguard.

The savings cannot be assumed. They have to be measured separately from the cost of implementing security and the cost of qualified review.

5. Give each party its part of the proof

A cloud provider proves what its service does. The contractor proves how it configured and uses the service. An advisor helps find and fix gaps. An assessor tests the combined implementation. Government defines the rules and makes the decisions assigned to it.

Sharing evidence does not transfer responsibility.

What CMMC 20X is

CMMC 20X is Deep Fathom's public position, research, software, and program analysis. It is not a coalition, an industry consensus, a certification, or a Government policy.

Deep Fathom has implemented all 110 Level 2 requirements and 320 assessment objectives in software. The graph connects a requirement to the contractor's implementation, evidence, conflicts, open work, and human finding. The software can flag a problem or draft a suggestion. It cannot certify a contractor.

The public evidence format and graduated verification proposal are not vendor standards. Government and the CMMC community would have to define the final fields, tests, review methods, authority, and license. Multiple tools must be able to create and use the record.

GSA's FedRAMP 20X and NIST's OSCAL show that machine-readable security evidence can be developed and tested in public. CMMC has different participants, rules, and decisions. The lesson is to test the method, not copy the program.

Read the five principles, see how the work changes, or compare seven CMMC policy options.

CMMC 20X is authored by Deep Fathom.

TRACE THE CLAIM

Sources and revision history.

PRIMARY AND GOVERNING SOURCES

01 **FedRAMP 20x**
General Services Administration
↗

02 **Open Security Controls Assessment Language**
National Institute of Standards and Technology
↗

CORRECTIONS AND MATERIAL REVISIONS

AUG 13, 2026

Removed early coalition language and unsupported comparisons; clarified Deep Fathom authorship, evidence fields, software boundaries, and measured-benefit requirements.

See an error or a source we missed? Send a correction. Material changes are recorded here rather than silently overwritten.