RESEARCH PAPER

Why CMMC 20X Separates Three Policy Layers

A design case for keeping required safeguards, proof structure, and review depth as three separate policy decisions.

STATUS	LAST REVIEWED	RESEARCH LANES	CLAIM REGISTER
Current	**August 13, 2026**	**Principles · Mechanism · Evidence · Evaluation**	**C-01 · C-02 · C-03 · C-04 · C-05**

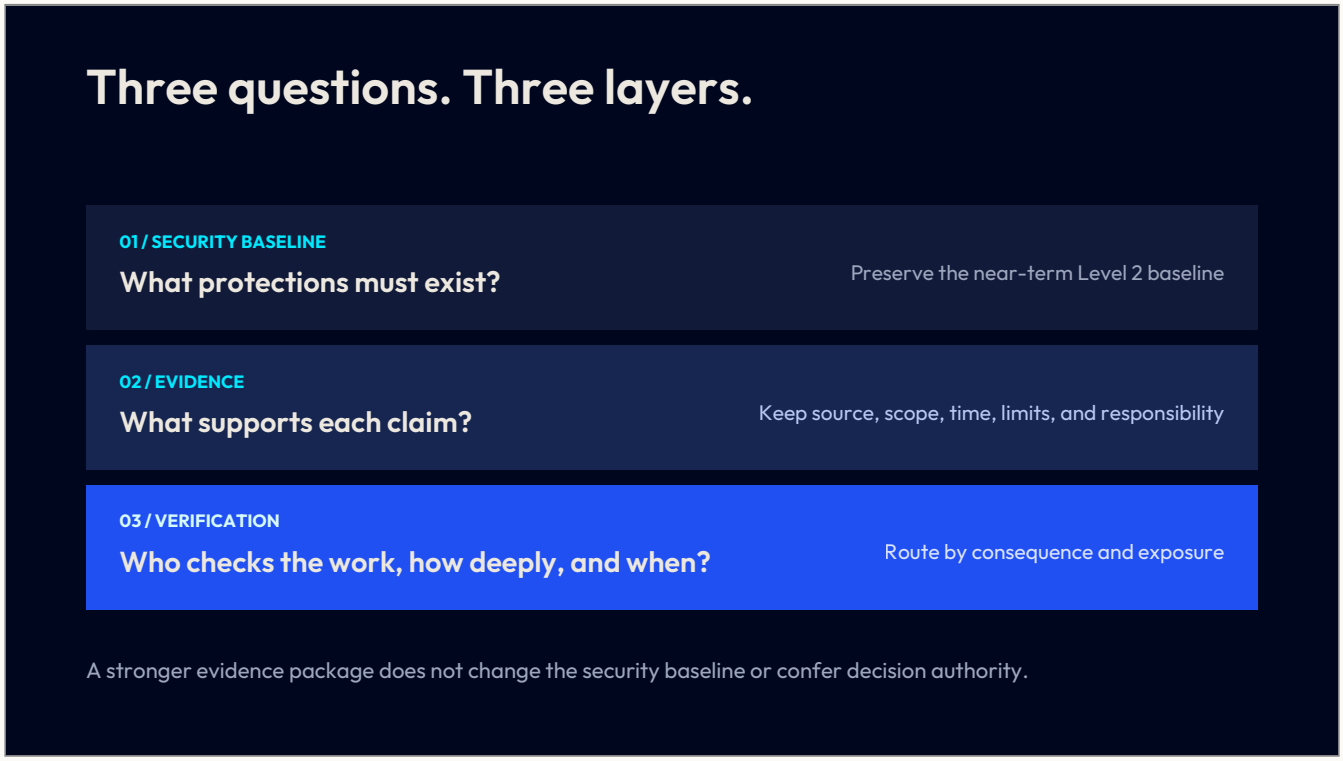
Current CMMC 20X design proposal as of August 13, 2026. It describes a policy architecture for evaluation and does not state a Government standard, measured program result, or legal conclusion.

The central design question is simple: **which parts of CMMC must remain fixed, and which parts can change when policy learns?**

CMMC discussions often compress three decisions into one. The first decision is the cybersecurity baseline: which safeguards an organization must implement. The second is the evidence contract: which facts must accompany a claim so that another person can examine it. The third is verification: who reviews the claim, with what independence and depth, under which authority.

Treating these as one object creates unnecessary policy risk. A proposal to improve evidence exchange can sound like a proposal to weaken safeguards. A proposal to reserve full independent assessment for higher-consequence work can sound like permission to skip implementation. A change to a template can appear to change the requirement itself.

CMMC 20X separates the three so each can be debated, tested, and governed on its own terms.



A stronger evidence package does not lower the baseline or confer decision authority.

Three policy objects, three questions

POLICY OBJECT	QUESTION IT ANSWERS	WHAT CMMC 20X HOLDS OR CHANGES
Security baseline	What must the contractor implement?	Preserve the complete near-term Level 2 baseline.
Evidence profile	What must travel with a security claim?	Propose common fields for source, scope, time, coverage, responsibility, conflicts, and review history.
Verification route	How deeply and independently is the claim examined?	Propose graduated review based primarily on consequence, sensitivity, exposure, criticality, and material change.

The separation is substantive. NIST SP 800-171 states security requirements for protecting controlled unclassified information in nonfederal systems. NIST SP 800-171A supplies assessment procedures for examining those requirements. The CMMC rule adds program roles, levels, assessment types, affirmation, status, and other legal and operational effects. Those materials already distinguish a required condition from the method used to assess it, even though program implementation connects them closely.

CMMC 20X extends that distinction to the evidence exchange layer. The profile is a proposed way to preserve what a reviewer needs to understand a claim. It does not declare the claim true. A record can be structurally valid while its source is incomplete, its population is wrong, or its implementation fails.

Why the baseline should stand on its own

The baseline is the security commitment. If policy changes verification, a supplier still has to implement every requirement applicable to its level. If policy standardizes evidence fields, a contractor still owns the accuracy of its system description and affirmation. If software reduces repeated handling, the underlying safeguard still has to operate.

That independence matters for at least four reasons.

First, it prevents burden reduction from becoming an informal control waiver. The strongest case for reducing repeated evidence work is that time and money can return to implementation, remediation, and skilled review. That case fails if the proposal quietly removes required protections.

Second, it makes failures diagnosable. When an organization lacks multifactor authentication for an access path, the failure concerns implementation. When the organization operates MFA yet supplies an export with unknown coverage, the failure concerns evidence. When a review samples too little to detect an exception, the failure concerns verification design. Different failures need different remedies.

Third, it protects comparability. Government can compare routes only if each route examines the same baseline. A lower finding rate under a lighter review could mean better preparation, weaker detection, or a different standard. A common baseline removes one source of ambiguity.

Fourth, it makes future baseline revision legible. NIST and the Department may change requirements through their own processes. An evidence exchange should be able to represent revised requirements without dictating their substance.

Evidence is an interface; a reviewer reaches the verdict

An evidence profile should function like an interface among contractors, providers, advisors, assessors, primes, and Government. It defines the minimum context needed to move a claim without stripping away its meaning.

For an identity claim, that context may include the source system, collection method, observation time, expected and observed population, exclusions, integrity information, responsible parties, linked objectives, known conflicts, and reviewer disposition. A screenshot can remain attached. The profile adds enough structure to reveal what the screenshot can and cannot support.

This layer deserves independent governance because it will evolve faster than the baseline. New source systems appear. Collection methods improve. Providers develop reusable exports. Conformance tests expose ambiguous fields. None of those events should silently revise what a Level 2 requirement means.

The evidence layer also deserves independent testing. A Government-led process could publish synthetic cases, expected structural results, and adversarial examples. Competing implementations could demonstrate that they preserve the same facts without producing identical software or identical reviewer judgments.

Verification is a risk-allocation decision

Verification answers a separate question: how much independent scrutiny is warranted for this work and this consequence?

CMMC 20X proposes three broad routes within Level 2: evidence-backed self-review, assisted human review, and independent C3PAO assessment. The names are design labels. They have no current regulatory effect. Government would have to define eligibility, independence, reviewer qualifications, sampling, appeal, oversight, and legal consequences before any route could operate.

The route should be driven primarily by mission consequence, CUI sensitivity, threat exposure, supplier criticality, and material change. Evidence quality should influence what a reviewer examines and whether a package is ready to proceed. It should not lower the consequence of failure. A polished package for a critical system still warrants the scrutiny assigned to that system.

Graduation also requires escalation. A lower-intensity route must be able to send a case upward when it encounters unresolved conflicts, suspicious provenance, material scope change, repeated failures, or conditions outside its authorized use. Random and risk-based Government sampling should test whether the routes are producing credible results.

Failure cases the separation must survive

The architecture is useful only if it holds under pressure.

A vendor markets schema validity as compliance. The remedy is an explicit authority field and conspicuous output language: structural validation records what was checked and leaves findings to qualified people.

A buyer treats thin evidence as low risk. The remedy is to keep route selection inputs distinct from evidence-quality indicators. Missing support can trigger correction or escalation. It cannot establish low mission consequence.

A provider record is copied across customers. The shared portion must carry service scope, version, dates, limits, and customer duties. Each contractor must connect that provider record to its own configuration and use.

A lighter route misses a recurring class of failure. Government sampling and comparative testing should identify the miss rate. The response may narrow eligibility, increase required procedures, improve evidence requirements, or retire the route.

A baseline revision breaks old mappings. Versioned identifiers and explicit mapping status should preserve the old record while requiring review before it supports the new baseline.

An inspectable policy test

Before changing program rules, Government could run a controlled comparison that freezes the baseline and varies the other two layers.

01 Select representative Level 2 cases, including technical, procedural, inherited, sparse, changed, and adversarial conditions.

02 Establish reference findings through qualified independent review and a documented process for resolving disagreement.

03 Encode each case in the proposed evidence profile while retaining original artifacts and gaps.

04 Assign qualified reviewers to conventional and structured-evidence methods.

05 Measure supported findings, missed conflicts, false conclusions, reviewer disagreement, correction behavior, labor, elapsed time, and results by case type.

06 Apply preset stop rules when a method produces unsafe reliance or loses traceability.

07 Publish the protocol, synthetic cases, conformance tests, aggregate results, limitations, and changes made in response.

The test should answer a narrow question: can a common evidence layer and specified review routes preserve or improve finding quality while reducing repeated handling? It cannot establish that the architecture will work across the Defense Industrial Base without further operational evaluation.

The discipline this separation creates

Every proposed change should declare which object it touches.

If a change alters a safeguard, treat it as a baseline decision. If it changes the facts attached to a claim, treat it as evidence-profile governance. If it changes who examines the claim or the consequence of the examination, treat it as verification policy.

That discipline makes disagreements sharper. It also makes experimentation safer. Government can test evidence formats and review methods while preserving the security baseline, human authority, and clear responsibility for each decision. CMMC 20X is a proposal for that architecture. Its value must be shown through inspectable tests and public rules before it earns operational trust.

TRACE THE CLAIM

Sources and revision history.

PRIMARY AND GOVERNING SOURCES

01 **Cybersecurity Maturity Model Certification Program, 32 CFR part 170**
Electronic Code of Federal Regulations
↗

02 **CMMC Assessment Guide — Level 2, Version 2.13**
Department of War Chief Information Officer
↗

03 **NIST SP 800-171 Revision 2**
National Institute of Standards and Technology
↗

04 **NIST SP 800-171A Revision 2**
National Institute of Standards and Technology
↗

05 **CMMC 20X Blueprint**
Deep Fathom
↗

CORRECTIONS AND MATERIAL REVISIONS

No material corrections recorded.

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