RESEARCH PAPER

What a Common Evidence Profile Must Preserve

The minimum context a CMMC security claim needs to remain traceable, challengeable, and useful across tools and reviewers.

STATUS	LAST REVIEWED	RESEARCH LANES	CLAIM REGISTER
Current	**August 13, 2026**	**Evidence · Mechanism · Principles**	**V-03 · V-04 · C-05 · C-06 · C-07**

Current design note for the proposed CMMC 20X evidence profile as of August 13, 2026. The profile is a discussion draft and working implementation; it is not a Government standard, authorized assessment method, or measured performance result.

The useful question for an evidence standard is not “can two tools exchange a file?” It is: **after the exchange, can a qualified person still understand, test, and challenge the security claim?**

A common profile can reduce repeated assembly only if it preserves the facts that give evidence meaning. Otherwise it standardizes loss. A clean JSON file with missing population coverage is still a weak basis for judgment. A signed provider statement with unclear customer duties still leaves responsibility unresolved. A mapped artifact with no collection time may describe a system that no longer exists.

CMMC 20X proposes a public, vendor-neutral evidence profile for discussion and testing. Its draft implementation is evidence that the idea can be made concrete. It carries no Government authority. The Department would need to define fields, permissible uses, conformance, security requirements, and governance through an open process.

Preserve the complete chain around the artifact

An artifact is one part of a review record. The full chain begins with a claim about implementation, links that claim to requirements and assessment objectives, identifies source evidence, states coverage and limits, records conflicts, and preserves what machines and people each did.

The following minimum set keeps those layers distinguishable:

RECORD ELEMENT	QUESTION IT MUST ANSWER	FAILURE IF OMITTED
Claim	What exactly is asserted?	Reviewers infer different propositions from the same artifact.
Requirement mapping	Which requirement and objectives are implicated?	Coverage appears complete while objectives remain unexamined.
Implementation	Which people, process, technology, and configuration make the claim true?	A policy statement substitutes for operating reality.
Source and method	Where did the fact come from, and how was it collected?	Authenticity and reproducibility cannot be evaluated.
Scope and population	Which systems, assets, accounts, locations, and period are covered?	A partial sample is mistaken for universal coverage.
Responsibility	Which party performs, configures, reviews, and corrects each part?	Provider and contractor duties blur together.
Limits and conflicts	What is excluded, missing, stale, or contradictory?	Known weaknesses disappear during packaging.
Review history	Who examined the record, under which method and version, and what did they decide?	A machine output or prior opinion is treated as current authority.
Change triggers	Which events require reconsideration?	Old evidence continues to support a changed system.

These elements are deliberately broader than file metadata. Hashes, signatures, timestamps, and identifiers matter. They help establish integrity and lineage. They do not tell a reviewer whether the observed population matches the claim.

Claims need precise subjects

“MFA is enabled” leaves the subject undefined. A testable claim names the environment, account population, enforcement point, relevant exceptions, and period of observation. It may state that a specified conditional-access policy was assigned to all privileged interactive accounts in a tenant at a given time, with one local emergency account outside the source export.

Precision does not guarantee sufficiency. It lets reviewers identify the next question. They can compare the stated population with inventories, inspect the emergency path, sample sign-in behavior, and decide whether the implementation satisfies the applicable objectives.

The profile should allow a claim to be supported, partially supported, unsupported, disputed, or awaiting review. A binary green field collapses too much information. The reason for a state and the person or rule that assigned it must travel with the state.

Source records need coverage and limits

Evidence should say how it was produced. Useful provenance includes source system, collector, collection method, observation time, relevant query or configuration, original format, integrity value, transformation history, and access restrictions.

Coverage deserves first-class fields. A directory export may show 24 accounts while an asset inventory expects 25. A vulnerability report may cover managed endpoints while excluding operational technology. A ticket sample may represent one facility and no others. Counts alone are insufficient; the record should state how the expected population was determined and identify exclusions.

Limits must survive every transformation. If a human-readable report is generated from the machine-readable package, the report should display material limits. If an advisor filters a package for remediation, the underlying source and exclusion records should remain addressable. If an assessor exports a finding, the evidence relied upon and contrary evidence should remain linked.

Responsibility cannot be flattened

CMMC evidence frequently crosses organizational boundaries. A cloud or managed service provider may operate infrastructure, produce logs, enforce part of a safeguard, and retain records. The contractor may choose configurations, manage users, monitor exceptions, and decide how CUI flows through the service.

A reusable provider record should identify the service, version, covered functions, applicable period, evidence offered, known limits, dependencies, and customer duties. The contractor then adds its own configuration and operating evidence. The two records can support one claim while keeping authorship and responsibility separate.

This design prevents two opposite errors. The contractor cannot imply that a provider performs customer-owned work. The provider does not have to recreate the same service-level facts for every customer when the facts and conditions are genuinely shared.

Machines and people need separate records

Rules can check required fields, references, identifiers, dates, counts, integrity values, and declared consistency conditions. AI can suggest mappings, summarize a conflict, or propose questions for review. These outputs can make work easier to inspect.

Neither output should silently become a finding. The profile should record the tool and version, input references, operation performed, result, confidence or limitations where relevant, and time. Human disposition should be a separate object with reviewer identity or role, authority, method, rationale, decision, and date.

Separation supports correction. A new model version can produce a different suggestion without rewriting the earlier human decision. A reviewer can reject a rule result while preserving the reason. An auditor can see whether a person examined the conflict or merely accepted a generated summary.

Privacy and security belong in the profile design

More structure can create more exposure. Evidence packages may contain system names, user identifiers, network details, vulnerabilities, security tooling, provider information, and CUI. Interoperability cannot mean indiscriminate distribution.

The profile should support data classification, handling restrictions, field-level or object-level access controls, minimization, redaction references, retention rules, and disclosure logs. It should permit evidence to remain in an authorized repository while reviewers exchange references and verified derivatives. Conformance tests should include unauthorized-field leakage and unsafe default-export cases.

Digital signatures and integrity checks should protect provenance without implying substantive truth. A valid signature says who signed a record and whether it changed after signing. It does not establish that the signed claim meets CMMC.

Versioning must preserve old meaning

Profiles, requirement catalogs, assessment guidance, provider services, and tools all change. Every record should identify the applicable versions. A mapping from an old requirement identifier to a new one should state who made the mapping, its status, and whether human review is required.

Updates should be append-oriented. Correct an error through a linked amendment that identifies what changed and why. Preserve the earlier record when policy and retention rules permit. Silent replacement makes it impossible to reconstruct what a reviewer knew at the time.

A public conformance suite

Government could evaluate the proposal without adopting any vendor's product. Publish a small suite of synthetic cases and expected structural outcomes:

01 A complete technical record with matching populations.

02 A valid file whose evidence covers only part of the claimed population.

03 Conflicting sources with different collection times.

04 Provider evidence with an unfulfilled customer responsibility.

05 A stale artifact after a material architecture change.

06 A malicious or misleading instruction embedded in source material.

07 A corrected record whose earlier review must remain reconstructable.

08 A package containing fields that the recipient is not authorized to see.

An implementation passes structural conformance only when it preserves required fields, relationships, versions, integrity, limits, and access rules. Substantive reviewers then test whether the cases support findings. Those are separate results.

The suite should be open to competing tools. Results should identify profile version, implementation version, test case, failures, and corrections. No single vendor should control field meaning or certify its own product as a Government-approved assessment method.

The standard of usefulness

A common evidence profile succeeds when a claim can move across tools and organizations without losing its subject, source, scope, limits, responsibility, conflict history, or authority boundary. It should make weak evidence easier to see. It should make corrections traceable. It should let a reviewer reproduce routine checks and spend judgment on the questions that remain.

That outcome requires more than a schema. It requires governance, reference cases, security rules, conformance testing, migration policy, and measured use with qualified reviewers. CMMC 20X offers a draft for that work. Government and the ecosystem should judge it by what it preserves under difficult cases.

TRACE THE CLAIM

Sources and revision history.

PRIMARY AND GOVERNING SOURCES

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

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

03 **OSCAL Frequently Asked Questions**
National Institute of Standards and Technology
↗

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

05 **CMMC 20X Common Evidence Profile**
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.