Docket

DOCKET / RESEARCH & PRACTICAL GUIDANCE

CAGE Code CMMC Scope: A UID-First Check, Not Hierarchy

> Build a more reviewable acquisition pipeline with Docket. Our deal-origination software and managed research help private equity teams screen companies against a mandate and understand the evidence behind each finding.

Published by Docket · 2026-11-18 · cage code cmmc scope · cage hierarchy · cmmc uid · sprs cmmc status · cmmc assessment scope · cmmc level 2 scope · immediate owner highest level owner · defense contractor due diligence · private equity cmmc diligence

Original article: https://docket.capital/articles/cage-hierarchy-cmmc-scope-uid-first-check



In this article

1. Executive Summary
2. Introduction and Background
3. Definition and Taxonomy: Seven Evidence Objects
4. Walking the Evidence: What SPRS Shows, to Whom, and What Changed in 2026
5. Reading Status and Dates Without Calculating Eligibility
6. Policy Timeline: Separating Announcement, Assessment, Affirmation and Observation
7. Implementation Guidance: A UID-First Evidence Worksheet
8. Worked Fictional Cases (Hypothetical Example)
9. Data Analysis and Evidence
10. Implications and Future Directions
11. Frequently Asked Questions (FAQs)
12. Conclusion

Executive Summary

A **CAGE code** (Commercial and Government Entity code) identifies a facility or entity, and the **CAGE hierarchy** records who owns whom. Neither one tells a research team which information systems a CMMC (Cybersecurity Maturity Model Certification) assessment covered. The Supplier Performance Risk System (SPRS) FAQ states that CAGEs "are not used in the boundary definition" of a company's CMMC assessment (www.sprs.csd.disa.mil), that the Hierarchy button "DOES NOT represent entities covered by an assessment" (www.sprs.csd.disa.mil), and that the contracting officer verifies status only through the unique identifier (UID) supplied by the offeror (www.sprs.csd.disa.mil). The DoD CIO FAQ says the same thing about site-level codes (dodcio.defense.gov).

For a private equity (PE) origination team the practical consequence is a change of lookup key. The question "does this parent hold a CMMC status?" cannot be answered from a CAGE. The answerable question is "which assessment UID covers the operation named in the mandate, at what level and status, as of which date?" The UID is a **10-character alphanumeric** identifier assigned to a CMMC assessment (www.acquisition.gov), and the rule preamble says it is assigned to the scope the organization defined for itself (www.federalregister.gov). SPRS release 4.1.5, dated April 29, 2026, removed CAGE search from the government Criteria Search (www.sprs.csd.disa.mil), so older "search by CAGE" advice no longer describes the tool.

This report proposes a seven-object evidence crosswalk and a UID-to-scope ledger. The seven objects are identity, CAGE code, hierarchy, assessment boundary, assessment record, score and announcement. Each has a safe claim and an unsafe inference. The ledger returns one of six dispositions: supported for the defined claim, issuer-stated, wrong-scope, outdated, conflicting, or not accessible. Public evidence will often end at "issuer-stated" or "not accessible", because SPRS access is role-limited and a system boundary is documented in material a researcher should not seek without authorization.

Policy timing also needs care. Phase II of the CMMC rollout was originally scheduled for November 10, 2026 (www.war.gov), and the Department of War announced its suspension on July 13, 2026 (dodcio.defense.gov). Phase I self-assessment requirements remain in place (dodcio.defense.gov). As of November 18, 2026, this review found no official successor date. This is a research protocol, not contractor implementation advice, contract-eligibility advice or legal advice.

Introduction and Background

Defense-industrial and government-services origination work often starts with a public claim: "the company is CMMC Level 2 certified." The claim travels easily. It appears in press releases, capability statements and directory listings. What the claim covers is much less portable. A Level 2 assessment applies to a defined set of assets, and the company decides that set before the assessment begins (www.ecfr.gov).

Three identifiers are routinely blurred. The first is the entity identifier assigned in the System for Award Management (SAM), the 12-character Unique Entity ID (UEI) (open.gsa.gov). The second is the 5-character CAGE code, assigned by the Defense Logistics Agency (DLA) (www.dla.mil). The third is the CMMC UID, assigned to an assessment record. They answer different questions: who is the registrant, which location or entity is the code attached to, and which assessed scope does this record describe.

The blur matters more after April 2026. SPRS release 4.1.5 removed CAGE search from the government Criteria Search (www.sprs.csd.disa.mil), and the same release introduced a new subcontractor listing built from SAM subaward data (www.sprs.csd.disa.mil). That listing is a different object from a certificate registry. A reviewer who sees a subcontractor listed has learned about a subaward relationship, not about an assessment.

The policy backdrop is also moving. The CMMC acquisition rule was published in the Federal Register on September 10, 2025 and became effective November 10, 2025 (www.federalregister.gov). The July 2026 suspension of Phase II changed what many contracts will require, but it did not remove the assessment records or the verification mechanics described here (dodcio.defense.gov).

This report treats research as evidence organization: it preserves dates and flags what is unknown. It cannot audit a target's systems, and neither a CMMC status label nor a NIST (National Institute of Standards and Technology) assessment score is a security audit performed by the researcher. The emphasis is a narrow decision, not a directory of certified companies: generic "CMMC certified companies" queries are an adjacent audience.

Definition and Taxonomy: Seven Evidence Objects

Table 1 below separates the objects that public coverage tends to merge. Each row names the key that identifies it, what it is for, who can read it, the claim it safely supports and the inference it does not support. The "current source" column points to the document that fixes the definition, and each source carries its own date, which matters because the SPRS guides were written at different times.

Evidence object	Identity key and purpose	Authorised reader	Safe claim	Unsafe inference	Current source and date
Company identity	UEI in SAM, a 12-character entity identifier (open.gsa.gov)	Public (SAM)	This registrant exists and holds a registration	That its subsidiaries or sites share an assessment	GSA data dictionary (June 2023)
CAGE code	5-character code for a facility or entity at a location (www.dla.mil)	Public (CAGE and SAM)	A code is attached to this name and address	That the code is "certified" or in scope	DLA pages; FAR 52.204-16
Corporate hierarchy	Immediate owner and highest level owner (HLO) fields entered by the registrant (open.gsa.gov)	SAM and role-limited SPRS views	This is the ownership structure the registrant reported	That every CAGE in the tree is covered by one assessment	SPRS FAQ; SPRS manual, May 2026
Assessment boundary	The set of assets the organization chose to assess (www.ecfr.gov)	The organization, its assessor, and authorised government users	The issuer's stated scope, if a scope statement is produced	That an enterprise tree equals an information-system boundary	32 CFR Part 170 (eCFR, current)
Assessment record	CMMC UID, level, type, status, affirmation and status dates	Role-limited in SPRS	A record with this UID shows this status on this date	That the status applies to systems the UID does not represent (dodcio.defense.gov)	SPRS manual V4.1.5; DoD CIO FAQ v2.4
NIST score	Summary score out of 110 in a NIST SP 800-171 DoD Assessment (www.acq.osd.mil)	Role-limited; scores are not releasable under FOIA (www.sprs.csd.disa.mil)	A score was posted for a system security plan	That a score equals a CMMC status or a security guarantee	DoD Assessment Methodology v1.2.1
Announcement	A press release or web badge	Public	The issuer made a statement on a date	That an assessment exists, is current or covers the mandate	Issuer page, retrieved date

The interpretive point is that only the fourth and fifth rows describe the thing a mandate cares about, and the fifth row is not public in the way the first three are. The first three rows are identity and access metadata. The SPRS FAQ puts it directly: the HLO CAGE is "only used to manage access in SPRS and often has no other connection to a particular assessment" (www.sprs.csd.disa.mil), and CAGE codes, including the HLO, serve metrics, access enforcement and annual affirmations.

Identity: UEI and CAGE

SAM generates the UEI when an entity registers, and GSA stated that the UEI transition did not change CAGE codes (www.gsa.gov). The two identifiers are independent. FAR 52.204-16 explains that DLA assigns a CAGE code as part of SAM registration (www.acquisition.gov), and that a code is required before award

(www.acquisition.gov). A CAGE code attaches to a location: the SAM data dictionary says CAGE codes are assigned at the Entity EFT (electronic funds transfer) Indicator level (open.gsa.gov), so one registration can carry several codes.

Hierarchy: Immediate Owner and Highest Level Owner

FAR 52.204-17 defines an immediate owner as an entity, other than the offeror, that has direct control of the offeror (www.acquisition.gov), with indicators of control that are explicitly non-exhaustive (www.acquisition.gov). The highest level owner sits at the top, where "no entity owns or exercises control" of it (www.acquisition.gov). The owner CAGE fields in SAM are "selected by the entity" (open.gsa.gov), so the hierarchy is a registrant-reported structure. SPRS imports it from SAM via DLA, and ownership changes in SAM typically reach SPRS within 48 hours (www.sprs.csd.disa.mil). A supplier-community presentation by the SPRS program office, dated August 25, 2026, says updates flow "within hours" (www.jhuapl.edu). The two timing statements differ, and neither is a service guarantee.

For parent and subsidiary reasoning, the slides describe the top CAGE as the HLO (www.jhuapl.edu) and a division CAGE as an immediate owner (www.jhuapl.edu). That is a map of control reported by registrants, and nothing in it describes an assessed network.

Assessment Boundary: Scope and Asset Categories

The rule defines the CMMC Assessment Scope as the set of all assets in the organization's environment that will be assessed (www.ecfr.gov). The DoD CIO scoping guide sorts Level 2 assets into five categories (dodcio.defense.gov). CUI Assets are assets that process, store or transmit controlled unclassified information (CUI) (www.ecfr.gov). Security Protection Assets provide security functions within the scope (dodcio.defense.gov). Contractor Risk Managed Assets (dodcio.defense.gov) and Specialized Assets (dodcio.defense.gov) are also part of the scope, while Out-of-Scope Assets cannot process, store or transmit CUI (dodcio.defense.gov). The guide adds that enterprise-wide security tools do not make all enterprise assets part of the scope (dodcio.defense.gov).

The term "Enterprise" is therefore easy to misread. The rule defines an enterprise as an organization with a defined mission and a defined boundary (www.ecfr.gov). SPRS asks for one of two scope values, Enterprise or Enclave, and defines an enclave as a set of system resources operating in the same security domain (www.sprs.csd.disa.mil). Neither term is a statement about a corporate entity tree.

Assessment Record: UID, Level, Type, Status

The DFARS (Defense Federal Acquisition Regulation Supplement) subpart defines the UID as 10 alphanumeric characters assigned to each CMMC assessment (www.acquisition.gov), and says UIDs apply to each contractor information system that will process, store or transmit federal contract information (FCI) or CUI (www.acquisition.gov). The SPRS manual states that Level 1 and Level 2 self-assessment UIDs, assigned after initial affirmation, carry the prefix S1 or S2 respectively, and that eMASS-assigned UIDs for Level 2 certification and Level 3 assessments carry the prefix L2 or L3 (www.sprs.csd.disa.mil). The Federal Register preamble adds that a new assessment submitted to SPRS yields a new UID for that scope (www.federalregister.gov). A target with two UIDs therefore has two assessment records, and each needs its own row in the ledger.

Score: A Different Object

A NIST SP 800-171 DoD Assessment produces a summary score out of 110, and the posted record is the summary rather than the individual requirement values (www.acq.osd.mil). The DoD CIO alignment deck gives the score range as -203 to 110 (dodcio.defense.gov). A Basic Assessment is a contractor self-assessment that yields a Low confidence level because the score is self-generated (www.acquisition.gov). The CMMC Level 2 conditional threshold uses a different test, a score of at least 0.8 of the Level 2 requirements (www.ecfr.gov). The two schemes should not be merged in a ledger column.

Walking the Evidence: What SPRS Shows, to Whom, and What Changed in 2026

Role limits and access

SPRS records are role-limited. The FAQ says a "SPRS Cyber Vendor User" role is needed for at least one CAGE in each HLO hierarchy (www.sprs.csd.disa.mil). The May 2026 manual describes that role as privileged access to the authorized CAGE and other CAGEs sharing the same HLO hierarchy. Government users see only affirmed Conditional and Final status types (www.sprs.csd.disa.mil), and the manual says assessments without a UID, such as Incomplete or Pending Affirmation records, are not visible to authorized government users (www.sprs.csd.disa.mil). An outside research team has none of these roles. No public PE lookup exists, so a missing public badge says nothing about a missing record.

The April 2026 search change

Release 4.1.5, published April 29, 2026, lists the removal of CAGE search from the government Criteria Search. The FAQ's contracting-officer answer was already firm: "Users cannot search by CAGE" and verifying an individual CAGE's CMMC status is "neither required nor possible" (www.sprs.csd.disa.mil). The November 2025 government viewing guide (version 4.12) still describes Criteria Search results as organized by the Corporate CAGE Hierarchy HLO (www.sprs.csd.disa.mil). That guide predates release 4.1.5, and it also warns that "Not all CAGEs listed may be associated with the assessment". A reviewer who finds screenshots or third-party advice built on the older display should date the document before using it. The later releases keep changing the surface: version 4.2 added the Reported HLO to the CMMC Vendor view (www.sprs.csd.disa.mil), and version 4.2.1 on October 7, 2026 improved the criteria search response for government administrators.

Included CAGEs are metadata, not a certificate of the tree

The manual's Level 1 table has an "Included CAGE(s)" column listing the CAGE codes included in the assessment, and the Level 2 tables carry "Last Entered or Affirmed CAGE(s) in Scope" or CAGEs "in scope when the assessment" was first affirmed. The rule itself requires Level 2 self-assessment results to include all industry CAGE codes associated with the information systems addressed by the scope (www.ecfr.gov), and the preamble describes CAGE codes as SPRS inputs (www.federalregister.gov). So a CAGE can be a field attached to a record. The training transcript shows the mechanism: the user opens the hierarchy and selects

which CAGEs are included (www.sprs.csd.disa.mil), and the manual says the selected CAGEs must be in the hierarchy. The tree is the picker. The selection is the metadata. Neither is the boundary, which the rule places in the assets (www.ecfr.gov).

Two further details affect acquisitions. After affirmation, the list of in-scope CAGEs cannot be changed by the vendor or the assessor (www.jhuapl.edu), and at annual affirmation a CAGE removed from scope cannot be re-added in SPRS (www.sprs.csd.disa.mil). For NIST assessment entries, records made under a previous HLO are not visible to users of the current hierarchy (www.sprs.csd.disa.mil). A change of ownership can therefore change who sees a record without changing what was assessed.

Where the documents conflict

The sources do not agree everywhere, and the ledger should preserve the disagreement. *Table 2* lists the conflicts found and how this report treats them.

Topic	Source A	Source B	Handling in the ledger
Hierarchy timing	SPRS FAQ: ownership changes "typically" flow within 48 hours	SPRS program slides (August 25, 2026): updates flow "within hours" (www.jhuapl.edu)	Record both; do not rely on either for a date
Enclave meaning	SPRS manual, CMMC definition: system resources in the same security domain	SPRS manual, legacy NIST table: "Standalone under Enterprise CAGE as business unit" (www.sprs.csd.disa.mil)	Use the CMMC definition for CMMC records; flag the NIST wording as CAGE-flavoured
Pending-affirmation visibility	Manual: not visible to government users	Training transcript: government sees only affirmed Conditional and Final; the viewing training transcript says a Level 2 Conditional record shown as "Pending Affirmation" stays current until the affirmation is completed	Treat as not visible; mark any outside description of that state as unverified
Hierarchy display	Government viewing guide v4.12 (Nov 2025): results organized by HLO hierarchy	Release 4.1.5 (April 2026): CAGE search removed	Date every screenshot; newer release governs

The CIO memo's separate bar on designating Level 2 (C3PAO) or Level 3 (DIBCAC) assessments in contracts (dodcio.defense.gov) is a different matter from the DoW release's statement that select government-led assessments continue during the suspension. Reconciling those two points is an analyst reading, not a statement by either source.

Reading Status and Dates Without Calculating Eligibility

Type, status and the date fields

The SPRS manual lists four CMMC assessment types: Level 1 self, Level 2 self, Level 2 by a certified third-party assessment organization (C3PAO), and Level 3 conducted by DoD/DOW through DIBCAC (SPRS manual). DIBCAC is a Defense Contract Management Agency unit (cyberab.org). A Level 2 Conditional status

requires a score of at least 0.8 of the Level 2 requirements (www.ecfr.gov). The DFARS definition of "current" sets a three-year limit for Final Level 2 status (www.acquisition.gov) and a 180-day limit for Conditional status (www.acquisition.gov), and the rule requires an annual affirmation after a Final status date (www.ecfr.gov).

Two practical details change how a ledger reads. The affirmation window opens 60 days before expiry (www.sprs.csd.disa.mil), and the manual says users track expiration themselves. Expired and canceled records can remain visible to authorized government users, so visibility does not mean currency.

Fields that are still moving

The manual describes version 29, dated May 2026, for SPRS V4.1.5 (www.sprs.csd.disa.mil). A later release, 4.1.6 on July 13, 2026, lists a CMMC self-assessment record expiration time update (www.sprs.csd.disa.mil), and release 4.2.1 on October 7, 2026 was the newest release listed on the release page at the time of retrieval (www.sprs.csd.disa.mil). Because the handling of expiration times for older records was updated after the manual, a screenshot or a calculated date from the May manual is not a safe basis for a current-status claim. The ledger should record the manual version, the release number and the retrieval date, and recheck all three on publication day.

A synthetic date illustration (Hypothetical Example)

Take a wholly synthetic Level 2 self-assessment with the invented identifier S2SYNTH001 and a status date of January 15, 2026. If its status were Conditional, the 180-day limit would end on July 14, 2026. If it reached Final on that same status date, the first annual affirmation would be due by January 15, 2027, with the window opening 60 days earlier on November 16, 2026, and the three-year status would end January 15, 2029. These dates are arithmetic on the documented intervals. The system-calculated dates in a real record govern, and the exact SPRS timestamp rules should be read from the current manual rather than recomputed.

Policy Timeline: Separating Announcement, Assessment, Affirmation and Observation

A timeline is a protection against the most common error in this area: treating a policy date as an assessment date. *Table 3* keeps five date types apart. The dates come from official or issuer documents, and the final column says what the date can and cannot show.

Date	Event	Date type	What it supports
September 10, 2025	DFARS final rule published; effective November 10, 2025 (www.federalregister.gov)	Policy	The acquisition clause framework, not any company's status
November 2025	SPRS government viewing guide v4.12	Document	A display as of its screenshots; predates the April 2026 search change
April 29, 2026	SPRS release 4.1.5: CAGE search removed from government Criteria Search	Observation (tool)	That CAGE-based lookup advice is outdated

Date	Event	Date type	What it supports
May 2026	SPRS manual v29 for V4.1.5	Document	Field names and definitions as of May 2026
July 13, 2026	DoW announces suspension of Phase II, originally November 10, 2026 (dodcio.defense.gov)	Policy	Rollout timing; Phase I self-assessments remain
July 13, 2026	SPRS release 4.1.6: expiration time update	Observation (tool)	That expiry fields changed after the manual
August 25, 2026	SPRS program supplier presentation (www.jhuapl.edu)	Document	Program office explanations; not a regulation
September to October 2026	Task Force report reported as not public; press reports a possible narrower Phase 2 restart (www.insidegovernmentcontracts.com) (federalnewsnetwork.com)	Press report	An option under discussion, not an adopted rule
October 7, 2026	SPRS release 4.2.1	Observation (tool)	The newest listed release as of retrieval

Table 3 shows why a single "as of" date is not enough. A company announcement dated June 2026 might refer to an assessment dated months earlier, an affirmation dated later, and a policy that was then in force and has since been suspended. The ledger's date columns should hold each of these separately.

On policy, the Department said that during the suspension it would continue to enforce baseline requirements through self-assessments and select government-led assessments (www.war.gov), and that Phase II was scheduled for November 10, 2026 (www.war.gov). The CIO implementing memo bars requiring activities from designating Level 2 (C3PAO) or Level 3 (DIBCAC) assessments and permits Level 1 and Level 2 self designations (dodcio.defense.gov), with further guidance promised after the 60-day review (dodcio.defense.gov). The Small Business Administration (SBA) said a comprehensive review would follow (legacy.sba.gov). An official successor was not located in this review as of November 18, 2026 (readers can re-check the DoW release, the DoD CIO CMMC page and the DoD CIO FAQ). The contract-level effect of the CIO implementing memo is a question for an authorized specialist. Nothing here implies that cyber obligations stopped: DoW stated that contractors remain obligated to safeguard covered defense information (www.war.gov).

Implementation Guidance: A UID-First Evidence Worksheet

Step 1: Write the exact claim and decision

Before looking at any source, write one sentence with the operation, the system or capability, the relevant date, the requested assessment level and type, and whether certification is mandatory or preferred under the mandate. Keep contract eligibility out of it. The sentence is the test the evidence must pass.

Step 2: Resolve the legal entity and operating unit

Record the UEI, legal name and address, and the CAGE code or codes. Treat these as identity and access metadata only. The CAGE code attaches to a name and location (www.acquisition.gov), and the owner fields are what the registrant entered (open.gsa.gov).

Step 3: Assign each piece of evidence to an object

Use the seven objects from *Table 1*. List what would count as each: a company identity record, a CAGE code, the corporate hierarchy, a scope statement, a UID with its status record, a NIST score and an announcement, and keep any assessor's accreditation as a separate item about the assessor. Draw only documented links between them. For example, an assessor's accreditation says something about the assessor. The Cyber AB (the CMMC Accreditation Body) describes C3PAOs as organizations that employ assessors (cyberab.org), and says only Cyber-AB recognized assessors used by a C3PAO may conduct authorized assessments (cyberab.org). It also describes the C3PAO as acknowledged to be objective and competent to assess organizations seeking certification (cyberab.org). An assessor badge on a vendor's website is therefore evidence about the assessor, not about the target's assessed systems.

Step 4: Build the UID and scope ledger

The ledger has one row per claim per UID. Suggested columns:

- **Claim and operation:** the sentence from Step 1.
- **Legal entity and identity metadata:** UEI, CAGE and owner fields, each labelled as metadata.
- **UID:** the 10-character identifier (www.acquisition.gov), or "not supplied".
- **Assessment type and status:** Level 1 self, Level 2 self, Level 2 C3PAO or Level 3; Conditional, Final, expired, retracted or pending.
- **Date set:** assessment or status date, affirmation date, affirmation expiration, status expiration.
- **Scope evidence:** the issuer's scope description, Enterprise or Enclave, and which asset categories it names.
- **Document version and retrieval date:** manual version, release number, FAQ date, retrieval date.
- **Provenance:** who supplied the extract, when, and how it can be authenticated.
- **Disposition:** one of the six outcomes below.

Step 5: Ask whether the evidence covers the operation

Enterprise and Enclave refer to information-system boundaries, not to a corporate entity tree (www.ecfr.gov). If the available statement says "company-wide" or names a business unit without naming systems that handle the mandate's data, the relationship is unresolved. Where a scope statement exists, compare it with the five asset categories. If it is missing, keep the material relationship unresolved and do not fill the gap from the hierarchy. The scoping guide notes that a Level 2 self-assessment and a Level 2 certification assessment use the same requirements and that a self-assessment cannot result in a certification (dodcio.defense.gov). A claim of "certified" that rests on a self-assessment should be returned as issuer-stated, because the record type does not support the certification claim.

Step 6: Separate public-only evidence from later diligence evidence

Public evidence is what the issuer has published and what official sources define. Later, authorised diligence may supply an extract from the target's own SPRS view or a scope statement. Handle each kind as follows:

- **Minimal excerpt:** retain only the relevant lines, with who provided them and when.
- **Provenance and currency:** confirm both with a qualified specialist before relying on an extract.
- **No out-of-role access:** do not seek access outside authorised roles, and do not collect a system security plan during public research.
- **No outreach:** none is part of this protocol.
- **Retention context:** the rule requires assessment artifacts to be retained by the assessed organization for six years from the status date (www.ecfr.gov), so a request for supporting material belongs in a lawful diligence process, not in desk research.

Step 7: Return a disposition

- **Supported for the defined claim:** a UID, level, type, current status and a scope description that names the systems or operation in the claim, with provenance.
- **Issuer-stated:** the issuer asserts status but no UID or scope evidence has been inspected.
- **Wrong-scope:** the evidence is genuine but covers a different boundary or entity.
- **Outdated:** the evidence is genuine, but its dates or document version are stale for the claim date.
- **Conflicting:** two sources disagree on level, UID, status or scope.
- **Not accessible:** the record sits behind a role the team does not hold.

None of these dispositions declares a company legally ineligible. High-consequence decisions go to specialist review.

Worked Fictional Cases (Hypothetical Example)

Every name, UID and date below is invented. The cases show how the ledger turns a claim into a disposition.

Table 4 summarises five synthetic cases and the disposition each would receive on public evidence alone.

Synthetic case	What the public record shows	Ledger reading	Disposition
A. Parent hierarchy, no scope evidence	"Northgate Synthetic Holdings" lists a subsidiary, "Harbor Synthetic Systems," under its HLO; a press release says the group is "CMMC Level 2 ready"	A hierarchy shows ownership only; no UID or scope statement	**Issuer-stated**
B. Expired affirmation	UID S2SYNTH001 shown in a screenshot with a Final status whose status date is 14 months before the claim date and no affirmation shown	The annual affirmation due 12 months after the status date is not shown; expired records remain visible	**Outdated**
C. Self-assessment called certification	A web page says "third-party certified" and cites a UID beginning S2	Prefix S2 denotes a self-assessment record, while L2 and L3 are assigned by eMASS	**Issuer-stated** (record type does not support the certification claim); escalate

Synthetic case	What the public record shows	Ledger reading	Disposition
D. Two different UIDs	Target lists S2SYNTH001 on one capability page and L2SYNTH002 on another, one for a corporate network and one for an enclave	Each UID represents its own assessed scope (www.federalregister.gov); the mandate's operation sits in neither description	**Conflicting** until reconciled
E. Date-mismatched announcement	An announcement dated before the Phase II suspension describes "required Phase II compliance"	Policy date differs from assessment date; Phase II was suspended	**Outdated** policy framing; record both dates

Case A is the central one for this report. A parent's CAGE hierarchy lists subsidiaries because SAM owner fields are entered by registrants (open.gsa.gov), and the SPRS display of that hierarchy does not represent entities covered by an assessment. The mandate cannot rely on it. In Case B the risk is the opposite: a genuine record presented without its dates. Case C turns on a type distinction that the scoping guide states plainly. Case D shows why the unit of analysis is the UID, since the DFARS subpart ties UIDs to each contractor information system in use (www.acquisition.gov). Case E is a reminder that the DFARS clause structure refers to UIDs supplied in proposals (acquisition.gov), so a policy statement and a status record are different objects.

Data Analysis and Evidence

This topic has no market-size or performance benchmark. The quantitative material is regulatory: counts, intervals and field definitions. The numbers are listed here so a reviewer can check a ledger against them.

- **Identifier lengths:** a UEI has 12 characters (open.gsa.gov), a CAGE code has 5 (www.dla.mil), and a CMMC UID has 10 (www.acquisition.gov).
- **Level 2 requirement count:** 110 security requirements across 14 families (dodcio.defense.gov), drawn from NIST SP 800-171 Revision 2, which NIST lists as withdrawn on May 14, 2024 (csrc.nist.gov) while the DoD materials continue to cite it.
- **Score range:** -203 to 110 for the NIST SP 800-171 DoD Assessment, and a Level 2 Conditional test of at least 0.8 of the Level 2 requirements (www.ecfr.gov).
- **Validity intervals:** Conditional status 180 days (www.acquisition.gov), Final status three years (www.acquisition.gov), annual affirmation (www.ecfr.gov).
- **Affirmation window:** opens 60 days before expiry.
- **Self-assessment cadence:** Level 2 self-assessment every three years (www.ecfr.gov).
- **Phase timing:** Phase I began November 10, 2025 (dodcio.defense.gov); Phase II was set for November 10, 2026 (legacy.sba.gov).
- **Assessor capacity context:** SBA's statement describes a system "supported by only about 100 approved assessors" (legacy.sba.gov), and gives an estimated certification cost of approximately $593,800 for small firms where a third-party assessment is required (legacy.sba.gov). These are SBA's framing of the program, not measurements of any company.
- **Release cadence:** the SPRS release page lists releases 4.1.5, 4.1.6, 4.2 and 4.2.1 between April 29 and October 7, 2026 (www.sprs.csd.disa.mil).

A permitted-sample report, in three separate ratios

If a future, authorised sample of claims is inspected, report these as three independent figures. Do not blend them into a single "compliance rate".

1. **Scope-supported share:** scope-supported claims divided by inspected claims.
2. **Outdated-evidence share:** claims whose evidence is stale for the claim date divided by inspected claims.
3. **Unknown-access share:** claims the team could not inspect because of role limits divided by inspected claims.

For arithmetic only (Hypothetical Example), suppose 20 claims were inspected: 6 scope-supported, 5 outdated, 4 not accessible, 3 wrong-scope and 2 conflicting. The three ratios would be 30 percent, 25 percent and 20 percent, and the remaining 25 percent would be the wrong-scope and conflicting claims. These numbers are invented to show the method. No benchmark or target performance was measured in this research, and the total population of certified companies cannot be estimated from badges, CAGE counts or source availability. The SPRS FAQ also states that individual SPRS reports are not releasable under FOIA, so the unknown-access share is expected to be large for public-only work.

Implications and Future Directions

For origination and screening. Until a UID and scope statement are in hand, a public CMMC claim should be recorded as issuer-stated for the defined operation. That is a neutral disposition. It does not say the company lacks a status, and the SPRS manual is explicit that records without a UID are not visible to government users, which means a missing public record is expected.

For acquisitions. Ownership change is a data event in SPRS. Hierarchy updates flow from SAM, in-scope CAGE lists lock at affirmation (www.jhuapl.edu), and records entered under a previous HLO can drop out of a current hierarchy view. A diligence plan should ask for the UID and the scope statement, and ask whether the scope boundary or the owner fields changed after the last affirmation. The question of whether a status carries over to a restructured entity is a legal and regulatory one for specialist review.

For source hygiene. Rules, FAQs and screenshots change on different schedules. The DoD CIO FAQ version 2.4 was updated to reflect the suspension (dodcio.defense.gov), and the acquisition-site DFARS pages carry their own change numbers and clause dates. A research team should store the version and retrieval date next to every excerpt.

Open questions. The Task Force's report was due to the CIO in September and had not been made public in the coverage retrieved (www.insidegovernmentcontracts.com). A press report describes an option to restart Phase 2 over a 90-day period with a narrower population (federalnewsnetwork.com), but that is a reported option and not a decision. Future releases may alter the vendor and government views again, so the protocol is versioned: rerun the checks on publication day against the newest FAQ, release notes and manual.

Research role. A research team, whether in-house or supported by a sourced research provider, can preserve the ledger, dates and excerpts for a mandate and hold unsupported claims open until lawful diligence supplies a UID and scope statement. It does not audit systems or advise on contract eligibility.

Frequently Asked Questions (FAQs)

What does "CAGE code CMMC scope" mean in practice? CAGE codes are not used to define the scope of a CMMC assessment. The scope is the set of assets the organization chose to assess (www.ecfr.gov).

Does a parent's or subsidiary's place in a CAGE hierarchy show CMMC coverage? No. The Hierarchy view shows the company structure of a reported HLO and does not represent entities covered by an assessment.

What are the immediate owner and highest level owner? The immediate owner has direct control of the offeror (www.acquisition.gov), and the highest level owner is the top of the chain (www.acquisition.gov). Both are reported by the registrant in SAM (open.gsa.gov).

How is CMMC status verified, and what is the SPRS UID? Contracting officers verify status using the UID provided by the offeror, and the DFARS subpart tells them to check SPRS for each UID provided (www.acquisition.gov). The UID is 10 alphanumeric characters (www.acquisition.gov).

Is there an "SPRS CAGE code lookup" for CMMC status? Not for government users: CAGE search was removed from the government Criteria Search in release 4.1.5, and the FAQ says verification by CAGE is neither required nor possible. No public lookup for private equity researchers was found, and access depends on roles.

What does a Level 2 certification scope include? Level 2 scope covers CUI Assets and Security Protection Assets, plus Contractor Risk Managed Assets and Specialized Assets as the scoping guide describes. Out-of-Scope Assets are excluded.

What should private equity due diligence on a defense contractor's cybersecurity ask for? Ask for the UID, the level and type, the status and affirmation dates, and the scope statement, and route interpretation to a specialist. Record whether evidence is public or lawfully supplied, and treat a NIST score as a separate object (www.acq.osd.mil).

Does the Phase II suspension mean cyber obligations stopped? No. The Department stated that Phase I self-assessment requirements remain in place and that contractors remain obligated to safeguard covered defense information (www.war.gov). Contract applicability is for an authorised specialist.

Conclusion

A CAGE code and a CAGE hierarchy answer questions about identity and ownership. A CMMC UID answers a question about an assessment record, and the scope statement behind it answers the question the mandate actually asks: which systems were assessed. The SPRS FAQ, the DoD CIO FAQ and the rule text point the same way. The hierarchy is not the boundary, and the UID must contain the scope that covers the assessment (www.sprs.csd.disa.mil).

For research acceptance, the protocol is short. Define the claim. Resolve the entity. Sort the evidence into objects. Record the UID, type, status and dates with document versions. Compare the scope description with the operation in the mandate. Return one of six dispositions, and hold the claim open where public evidence stops. Because SPRS releases, FAQ text and policy guidance changed repeatedly in 2026, every ledger row

should carry its retrieval date, and the checks should be rerun against current sources before a decision relies on them. What remains unknown, including restricted records and the effect of any successor policy, should be recorded as unknown.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.sprs.csd.disa.mil/faqs.htm
2. https://dodcio.defense.gov/Portals/0/Documents/CMMC/FAQsv6.pdf
3. https://www.acquisition.gov/dfars/subpart-204.75-cybersecurity-maturity-model-certification
4. https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
5. https://www.sprs.csd.disa.mil/pdf/release/RelHist_4_1_5.pdf
6. https://www.war.gov/News/Releases/Release/Article/4542329/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require
7. https://dodcio.defense.gov/CMMC
8. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
9. https://open.gsa.gov/api/entity-api/v1/SAM%20Functional%20Data%20Dictionary.pdf
10. https://www.dla.mil/Working-With-DLA/Applications/Details/Article/3606127/registration-renewal-and-cage-creation-in-system-for-award-management-sam
11. https://www.dla.mil/Working-With-DLA/Applications/Details/Article/2920893/cage-code-commercial-and-government-entity-code
12. https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf
13. https://www.gsa.gov/system/files/UEI_External_Fact_Sheet.pdf
14. https://www.acquisition.gov/far/52.204-16
15. https://www.acquisition.gov/far/52.204-17
16. https://www.jhuapl.edu/sites/default/files/2026-08/APL-CMMC-Supplier-Webinar-SPRS-Updates-082526.pdf
17. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf
18. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2v2.pdf
19. https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf
20. https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC-AlignmentNIST-Standards.pdf
21. https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171-dod-assessment-requirements.
22. https://www.sprs.csd.disa.mil/pdf/training/CMMCL2SelfAssessment-Transcript.pdf
23. https://www.sprs.csd.disa.mil/pdf/CMMCAssessmentViewingGuide-Gov.pdf
24. https://www.sprs.csd.disa.mil/release.htm
25. https://dodcio.defense.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf
26. https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/Assessing-and-Certification
27. https://www.insidegovernmentcontracts.com/2026/09/cmmc-reform-task-force-updates-september-2026

28. https://federalnewsnetwork.com/defense-main/2026/10/rfi-offers-path-forward-for-dod-with-cmmc
29. https://legacy.sba.gov/article/2026/07/13/sba-commends-us-department-wars-suspension-cmmc-phase-ii-small-defense-contractors
30. https://acquisition.gov/dfars/252.204-7025-notice-cybersecurity-maturity-model-certification-level-requirements.
31. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

THE PUBLISHER

About Docket

Docket provides deal-origination research software and managed research for private equity firms. We help investment teams investigate acquisition targets using structured screening criteria, retained sources and reviewable company evidence. Teams can work through a self-serve platform or use managed research, depending on how they want research delivered.

Research against a defined mandate

A useful target list needs more than company names. Docket focuses on the questions that determine whether a company fits an investment mandate, including the evidence needed to support or qualify each answer. Our research approach makes the connection between screening criteria, source material and conclusions visible to the team reviewing the work.

Triage, Scout and Audit

Docket's three named research agents perform complementary tasks. Triage resolves company identity and screens fit. Scout collects sourced answers against the mandate. Audit checks retained evidence, addresses contradictions and leaves unsupported answers visibly unresolved. This structure helps reviewers distinguish established findings from missing information and questions requiring further investigation.

Evidence that supports investment-team judgment

Our research library covers market mapping, screening criteria, private-company data, succession and ownership, source evaluation and evidence standards. These resources explain the methods and limitations behind origination research. Findings support a team's judgment; they do not establish that a company is for sale or guarantee a transaction or investment outcome.

Work with Docket

Visit Docket to explore the platform, managed research and the current contact path. Read about screening criteria, evidence standards, AI research agents and market mapping.

Public examples are illustrative unless explicitly identified otherwise. Research preparation and authorized outreach are separate activities; confidential target lists and customer outcomes should never be inferred from an educational example.

Website: https://docket.capital

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.