The CMMC Ecosystem

A Structural Reference for Practitioners

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

A practitioner entering the CMMC ecosystem encounters an unusually crowded landscape of entities, authorities, systems, and relationships. The entities include federal agencies whose roles are often misunderstood, an accreditation body with its own taxonomy of authorized organizations and individuals, a certification body that operates the practitioner credentialing function, operational systems that persist the compliance record, and enforcement pathways that operate independently of the scheduled assessment cycle. Every practitioner eventually builds a mental model of how these pieces relate, but the learning process is inefficient because the ecosystem documentation is distributed across multiple sources and the relationships among entities are rarely explained coherently in one place.

This paper is a structural reference for CMMC practitioners. It addresses what each entity in the ecosystem does, how the entities relate to one another, which authorities each entity derives its role from, and how the ecosystem behaves across the lifecycle of a contractor's engagement with CMMC obligations. The target audience is the RP, RPA, CCP, CCA, CCI, and the practitioners who work within C3PAOs and RPOs. The content assumes familiarity with CMMC at the conceptual level and builds the structural map that connects the conceptual understanding to the operational reality.

The ecosystem is best understood as four layers operating together. The policy layer establishes the framework that governs Controlled Unclassified Information and its protection. The DoD layer implements the framework within the defense contracting context. The accreditation and certification layer, which includes CyberAB and ISACA working in complementary roles, operates the assessment and practitioner ecosystem that delivers CMMC as a program. The enforcement layer operates across all three, providing the oversight and prosecutorial pathways that give the framework consequence. Practitioners who hold the four layers in mind simultaneously are positioned to advise clients coherently. Practitioners who know only the layer they work in most directly produce advice that works in limited contexts and fails when questions cross layer boundaries.

The taxonomy table below summarizes the entities this paper addresses. Each entity receives detailed treatment in the sections that follow.

Entity	Layer	Primary Role	Authority Source
NARA	Policy	Executive Agent for CUI Program	EO 13556
ISOO	Policy	CUI Program oversight within NARA	EO 13556, 32 CFR 2002
NIST	Policy	Authors SP 800-171 and related standards	FISMA, NDAA
OUSD(A&S)	DoD	Owns CMMC program	DoD organizational authority
CMMC PMO	DoD	Operates CMMC program	32 CFR Part 170
DoD CIO	DoD	Cybersecurity policy oversight	DoD organizational authority
DCSA	DoD	Conducts DIBCAC assessments	DFARS 252.204-7020
CyberAB	Accreditation	Accredits C3PAOs, registers RPOs, issues RP/RPA	Contract with DoD
ISACA (CAICO)	Certification	Operates CCP, CCA, CCI credentialing	CAICO appointment by CyberAB
C3PAO	Assessment	Performs Level 2 certification assessments	CyberAB accreditation
RPO	Consulting	Registered consulting organization	CyberAB registration
RP / RPA	Consulting	Individual consulting practitioner credentials	CyberAB registration
CCP	Assessment	Certified CMMC Professional (team	ISACA certification

Entity	Layer	Primary Role	Authority Source
		member role)	
CCA	Assessment	Certified CMMC Assessor (lead assessor role)	ISACA certification
CCI	Training	Certified CMMC Instructor	ISACA certification
LTP	Training	Licensed Training Provider	CyberAB license
LPP	Training	Licensed Publisher Partner	CyberAB license
SPRS	System	Supplier score submission in PIEE	DFARS 252.204-7019/7020
CMMC eMASS	System	CMMC assessment record system	32 CFR Part 170
DoJ Civil Division	Enforcement	False Claims Act prosecution	31 USC 3729-3733
DoD OIG	Enforcement	Inspector General investigations	Inspector General Act

The Policy Layer

The policy layer establishes what CUI is, how it must be handled, and what technical standards protect it. The three entities in this layer operate at the executive branch level and produce outputs that every other entity in the CMMC ecosystem ultimately references. Practitioners who understand the policy layer can trace any specific CMMC requirement back to its underlying authority, which is essential for defending implementation decisions during assessments and for answering client questions about why specific controls are required.

National Archives and Records Administration (NARA)

NARA is the Executive Agent for the Controlled Unclassified Information Program, a role established by Executive Order 13556 in November 2010. The selection of NARA for this role reflects the agency's institutional competence in information classification, marking conventions, records management, and oversight of sensitive information handling across the federal government. NARA had previously served as the Executive Agent for the classified national security information program through its Information Security Oversight Office, and the extension to CUI built on that established oversight capability.

NARA publishes the implementing regulation for the CUI Program at 32 CFR Part 2002, which became effective in November 2016. This regulation is the authoritative framework for CUI handling across all executive branch agencies and, by extension, for the contractors who handle CUI on behalf of those agencies. The regulation addresses designation, marking, safeguarding, dissemination, decontrolling, and destruction of CUI. A practitioner working on CMMC readiness needs to understand that the protection requirements CMMC assesses are a subset of the broader CUI handling obligations that 32 CFR Part 2002 establishes.

NARA also maintains the CUI Registry at archives.gov/cui, which is the authoritative public catalog of information categories that qualify as CUI. The Registry is organized by category family and includes categories like Controlled Technical Information, Export Controlled, Privacy, Procurement and Acquisition, Proprietary Business Information, and dozens of others. When a contractor or assessor needs to determine whether specific information qualifies as CUI, the answer is in the Registry. Many practitioners have never examined the Registry in detail, which is a gap worth closing because the Registry is the authoritative source on scope questions that arise during engagements.

Information Security Oversight Office (ISOO)

ISOO operates within NARA and serves as the specific office responsible for CUI Program implementation and oversight. The office publishes implementation guidance documents, conducts oversight activities, investigates complaints, and reports annually to the President and to Congress on the status of the CUI Program

across executive branch agencies. ISOO is a small office by federal government standards but carries substantial authority across the executive branch.

The oversight function ISOO performs operates through several mechanisms. Agency compliance reviews assess whether federal agencies are implementing the CUI Program consistently with 32 CFR Part 2002. The complaint investigation function addresses specific allegations of CUI mishandling from employees, contractors, or members of the public. The annual reports to the President and Congress document program status, identify areas of weakness, and influence policy attention. ISOO operates as an oversight body with escalation capability rather than as a direct enforcement authority. Findings and recommended corrective actions flow through agency heads, and serious violations are escalated to appropriate enforcement authorities including the Department of Justice.

For CMMC practitioners, ISOO represents the oversight function that operates continuously and independently of the scheduled CMMC assessment cycle. A contractor who passes a CMMC assessment has demonstrated compliance with the specific protection requirements the C3PAO assessed. That contractor can still be the subject of an ISOO complaint investigation if their broader CUI handling practices depart from 32 CFR Part 2002 requirements. Practitioners who understand the ISOO oversight function can advise clients on the compliance scope that extends beyond CMMC.

National Institute of Standards and Technology (NIST)

NIST sits within the Department of Commerce and serves as the federal government's standards-setting body for cybersecurity, cryptography, and related technical domains. The Federal Information Security Management Act and subsequent legislation direct NIST to develop standards and guidelines for federal information systems, and the outputs of that work become the technical foundation for many federal cybersecurity requirements including CMMC.

NIST Special Publication 800-171 is the specific NIST document that CMMC directly assesses against. The publication addresses protection of CUI in nonfederal systems and organizations, and its 110 security requirements form the control set that CMMC Level 2 assessments evaluate. NIST SP 800-171 Revision 2 was published in

February 2020 and is the current assessment baseline for CMMC 2.0. NIST SP 800-171 Revision 3 was published in May 2024 with substantial structural changes, and the transition of CMMC to the Revision 3 baseline is pending policy decisions that have not yet been finalized.

NIST also authors SP 800-172, which extends SP 800-171 with enhanced security requirements for higher-risk CUI categories. CMMC Level 3, which applies to a small subset of defense contractors handling CUI of elevated sensitivity, references SP 800-172 requirements. NIST produces related publications including the Risk Management Framework in SP 800-37 and the Security and Privacy Controls catalog in SP 800-53, which provide the broader context within which SP 800-171 operates.

Practitioners preparing clients for CMMC assessment work directly with NIST publications as primary reference material. The assessment methodology in NIST SP 800-171A describes how each of the 110 requirements in SP 800-171 is assessed through specific objectives and assessment methods. A practitioner who treats the NIST publications as the authoritative source rather than secondary CMMC guidance documents produces more defensible assessment preparation.

The DoD Layer

The Department of Defense operationalizes the policy layer within the defense contracting context. CMMC is a DoD program, and the entities in the DoD layer define how the broader CUI Program framework applies to defense contractors specifically. Practitioners need to distinguish between CUI obligations generally, which apply to all contractors handling CUI for any federal agency, and the DoD-specific implementation that CMMC assesses.

Office of the Under Secretary of Defense for Acquisition and Sustainment

The Office of the Under Secretary of Defense for Acquisition and Sustainment, abbreviated OUSD(A&S), is the DoD organization that owns the CMMC program. The office has policy authority over acquisition-related cybersecurity

requirements, which positions it as the natural home for a program that conditions contract eligibility on cybersecurity compliance. OUSD(A&S) developed the CMMC program concept, drove the rulemaking process, and oversees implementation.

Within OUSD(A&S), cybersecurity acquisition policy responsibility sits in specific offices that have evolved over the development of CMMC. The specific organizational structure has been revised multiple times since CMMC was first announced in 2020. The current structure positions CMMC program management within an office responsible for defense industrial base cybersecurity generally, which includes CMMC alongside related programs addressing supply chain risk management and cyber incident reporting.

CMMC Program Management Office

The CMMC Program Management Office, commonly referred to as the CMMC PMO, is the specific DoD office that operates the CMMC program day-to-day. The PMO publishes program guidance, maintains program documentation, coordinates with CyberAB on ecosystem operations, oversees the rollout of CMMC requirements through the rulemaking and implementation process, and serves as the primary DoD point of contact for program stakeholders.

The PMO published the CMMC final rule at 32 CFR Part 170, which became effective in December 2024. The final rule establishes the regulatory framework for CMMC as a program, including the three assessment levels, the self-assessment requirements for Level 1, the third-party assessment requirements for Level 2 and certain Level 3 cases, and the government-led assessment for the highest sensitivity Level 3 requirements. The companion DFARS rule at 48 CFR was finalized separately and contains the contract-level flowdown language that puts CMMC requirements into defense contracts.

Practitioners working on CMMC engagements reference PMO-issued guidance regularly. The CMMC Assessment Guides for Level 1 and Level 2 are the operational documents that describe how assessors conduct assessments against the relevant control sets. The Scoping Guides address how the assessment boundary is defined. Practitioner awareness of which PMO documents are

authoritative and which are supplementary shapes how well practitioners can defend assessment preparation decisions.

> **In practice.** A practitioner preparing a client for Level 2 assessment encounters a disagreement with the client's internal IT director about whether a specific system falls within the assessment boundary. The practitioner references the CMMC Assessment Scoping Guide for Level 2, which was published by the PMO, to establish the authoritative boundary criteria. The IT director pushes back with a blog post from a consulting firm that offers a contrary interpretation. The practitioner's ability to distinguish PMO-issued guidance from third-party commentary determines whether the scoping decision survives the C3PAO's review. Client engagements regularly turn on these source-authority distinctions.

DoD Chief Information Officer

The DoD Chief Information Officer has broad cybersecurity policy authority within the department, independent of the acquisition-focused CMMC role that OUSD(A&S) holds. The DoD CIO issues cybersecurity instructions and standards that apply to DoD information systems and, through various mechanisms, to the contractor systems that process, store, or transmit DoD information. DoD Instruction 8500.01, DoD Instruction 8510.01, and the family of related cybersecurity instructions establish the policy baseline for DoD cybersecurity operations.

For CMMC practitioners, the DoD CIO role matters in specific contexts. The DoD CIO issues the guidance that governs how DoD treats compromised contractor systems, how incidents must be reported under DFARS 252.204-7012, and how classified and controlled information must be segregated. The interaction between CMMC requirements and the broader DoD cybersecurity policy regime sometimes surfaces in assessment contexts, particularly for contractors whose work extends into classified environments or involves specialized compartmented programs.

Defense Counterintelligence and Security Agency (DCSA)

The Defense Counterintelligence and Security Agency is a DoD agency with several related missions including industrial security, personnel security, counterintelligence, and insider threat programs. For CMMC practitioners, DCSA matters because it operates the Defense Industrial Base Cybersecurity Assessment Center, commonly known as DIBCAC, which conducts NIST SP 800-171 assessments of DoD contractors.

DIBCAC assessments predate CMMC and served as the DoD mechanism for verifying contractor cybersecurity posture before CMMC's assessment ecosystem became operational. A DIBCAC high assessment score has been recognized under interim DoD policy as equivalent to CMMC Level 2 certification, though the exact terms of this recognition have evolved as CMMC has been implemented. Practitioners supporting clients who have received DIBCAC assessments need to understand how the DIBCAC findings translate into CMMC context and how the historical assessment results affect current obligations.

DCSA's broader industrial security mission also touches CMMC indirectly. Facility clearances under the National Industrial Security Program, personnel clearance investigations, and the handling of classified information at contractor facilities all interact with CMMC-scoped environments when contractors hold both CUI and classified information. Practitioners working with contractors whose scope includes classified work need to understand where DCSA's industrial security role meets the CMMC assessment process.

> **In practice.** A defense contractor with a prior DIBCAC high assessment engages a practitioner for CMMC readiness support. The contractor's leadership believes that the DIBCAC score protects them from needing additional work. The practitioner reviews the DIBCAC findings, identifies which control deficiencies were noted, and maps those to current CMMC assessment objectives. The practitioner discovers that DIBCAC was assessed against a subset of the environment that no longer matches the contractor's current operating state because the contractor acquired another facility after the DIBCAC engagement. The DIBCAC equivalency does not cover the acquired

> facility, which means the practitioner has to scope and remediate a meaningful portion of the environment as if no prior assessment had occurred.

The Accreditation and Certification Layer

The accreditation and certification layer is where the CMMC program operationalizes practitioner and organizational credentials. Two entities operate this layer in complementary roles. CyberAB holds the accreditation function, which covers C3PAO accreditation, RPO registration, and the issuance of RP and RPA credentials. ISACA serves as the Cybersecurity Assessor and Instructor Certification Organization, commonly referred to as CAICO, which operates the certification function for CCP, CCA, and CCI credentials. The division of roles between CyberAB and ISACA is recent and requires specific explanation because earlier ecosystem documentation treated CyberAB as the sole operator of the practitioner credentialing function.

CyberAB

The Cyber Accreditation Body, commonly referred to as CyberAB, is the private organization authorized by DoD to operate the accreditation function for the CMMC program. CyberAB is not a government agency. The organization operates under a contract with DoD and is recognized in the CMMC rulemaking ecosystem through 32 CFR Part 170. The combination of contractual authorization and regulatory recognition produces operational authority that functions like regulation in practice, even though sovereign regulatory authority remains with DoD. Practitioners often misunderstand this relationship, treating CyberAB as if it were a government regulator rather than a contracted accreditation body operating under DoD oversight. The distinction matters because CyberAB's authority is bounded by its contract with DoD and the rulemaking that DoD has completed.

CyberAB accredits C3PAOs, registers RPOs, issues RP and RPA credentials for individual consulting practitioners, licenses training providers and publishers, and maintains program infrastructure including the CyberAB Marketplace and the

Code of Professional Conduct. The organization also retains responsibility for Tier 3 investigations of credentialed practitioners even where the underlying credential was issued by ISACA under the CAICO role.

The CyberAB Marketplace, accessible at cyberab.org, is the public registry of authorized organizations and individuals. Every C3PAO, every RPO, every RP and RPA in current good standing appears in the Marketplace. Contractors selecting assessment organizations or consulting organizations can verify credentials through the Marketplace. The Marketplace is the authoritative source for verifying claims of CMMC credentials in the categories CyberAB operates, and practitioners who help clients evaluate vendors should be familiar with how to use it. CCP, CCA, and CCI credentials are verified through ISACA rather than through the CyberAB Marketplace, reflecting the CAICO role transfer.

CyberAB's retention of the Tier 3 investigation function matters for practitioner ethics. When allegations arise that a credentialed practitioner has violated the CMMC Code of Professional Conduct in ways that warrant formal investigation, CyberAB handles the Tier 3 process regardless of whether the underlying credential is issued by CyberAB directly or by ISACA as CAICO. This continuity of the investigation function ensures that enforcement of professional conduct standards remains consistent across the credential types.

> **In practice.** A practitioner preparing a client for Level 2 assessment needs to recommend candidate C3PAOs for the engagement. The practitioner visits the CyberAB Marketplace to evaluate accredited C3PAOs by geography, size, and industry focus. The Marketplace shows which C3PAOs are currently accredited and in good standing, which matters because the accreditation list changes as organizations join, withdraw, or have their accreditations suspended. The practitioner who recommends a C3PAO without verifying current Marketplace status risks recommending an organization that cannot perform the assessment. The Marketplace is also the practitioner's own professional record. A prospect evaluating the practitioner will verify the claimed credentials there before engaging.

ISACA as Cybersecurity Assessor and Instructor Certification Organization (CAICO)

ISACA is a global professional association in governance, risk, cybersecurity, audit, and related disciplines. The organization administers several widely recognized certifications including the Certified Information Systems Auditor, the Certified Information Security Manager, the Certified in Risk and Information Systems Control, and the Certified Data Privacy Solutions Engineer. In December 2025, ISACA was appointed by CyberAB as the CAICO for the CMMC program, with the transition becoming fully operational by April 1, 2026.

As CAICO, ISACA operates the certification function for three CMMC credentials. The Certified CMMC Professional credential, commonly referred to as CCP, qualifies an individual to participate in CMMC assessments as a team member under the direction of a Lead Assessor. The Certified CMMC Assessor credential, commonly referred to as CCA, qualifies an individual to serve as a Lead Assessor on CMMC Level 2 assessments. The Certified CMMC Instructor credential, commonly referred to as CCI, qualifies an individual to deliver CMMC training through Licensed Training Providers.

The transition from CyberAB to ISACA for these credentials preserves the substantive credential requirements while changing the operational infrastructure that supports them. Existing CCP and CCA credential holders did not need to recertify when the transition occurred. ISACA automatically created accounts for existing credential holders using the email addresses registered with CyberAB, which allowed continuity of service without interruption. Current credential holders access renewal, continuing education tracking, and related services through the ISACA platform rather than through the CyberAB site.

The examination infrastructure for CCP and CCA certifications has moved to the PSI testing platform under ISACA's administration. Candidates pursuing the credentials for the first time register through ISACA, complete the required training through Licensed Training Providers, and schedule examinations through PSI. Background checks, which are required as part of the certification process, are initiated after a candidate passes the training and examination requirements.

ISACA validates the experience requirements and coordinates with CyberAB on credentialing decisions.

The CCI credential is distinct from the traditional training credentials in the CMMC ecosystem. While Licensed Training Providers are organizations licensed by CyberAB to deliver CMMC courseware, CCI is the individual credential held by qualified instructors who teach CMMC content within LTP programs. The CCI credential ensures that individuals delivering CMMC training have met specific standards for subject matter competence and instructional capability. ISACA operates this credential alongside CCP and CCA under the CAICO role.

For practitioners, the practical effect of the CAICO transition is that credential-related interactions split between two entities. Questions about RP and RPA credentials, RPO registration, or C3PAO accreditation go to CyberAB. Questions about CCP, CCA, and CCI credentials go to ISACA. Tier 3 investigations of alleged professional conduct violations go to CyberAB regardless of credential type. Practitioners holding multiple credentials across both organizations maintain accounts in both systems.

> **In practice.** A CCA who holds the credential from the pre-transition CyberAB era needs to complete continuing professional education to maintain good standing. Before the transition, continuing education tracking ran through the CyberAB platform. After the transition, the same practitioner logs into an ISACA account that was automatically created using the email address registered with CyberAB. The practitioner submits CPE documentation through ISACA. The experience feels different because ISACA's platform is designed around the organization's broader certification portfolio rather than around CMMC specifically. Practitioners who renewed credentials under CyberAB now navigate a different user interface, different renewal timing, and different verification processes. The credentials themselves carry the same recognition as before, but the administrative experience is genuinely different.

Certified Third-Party Assessment Organizations (C3PAOs)

C3PAOs are the organizations accredited by CyberAB to perform CMMC Level 2 certification assessments. Accreditation as a C3PAO requires the organization itself

to undergo an assessment of its own cybersecurity posture, which is a foundational integrity requirement. An organization that cannot meet the security standards it would assess others against cannot credibly serve as an assessor.

C3PAOs operate under strict conflict of interest rules that separate their assessment role from other roles they might play. A C3PAO cannot perform both consulting work and assessment work for the same client. The organizational structure of a C3PAO may include separate divisions or affiliated entities that perform consulting for different clients while the C3PAO performs assessments for others, but the conflict rules prohibit the same C3PAO entity from consulting and assessing the same client organization.

C3PAOs employ Certified CMMC Assessors and Certified CMMC Professionals to staff assessment engagements. The C3PAO is responsible for the assessment output and carries the professional liability for assessment decisions. The individual practitioners staffing the assessment hold credentials issued by ISACA under the CAICO role, but they work through the C3PAO's organizational structure and under the C3PAO's processes. Practitioners who work as CCA or CCP within a C3PAO are bound by both the C3PAO's processes and the CyberAB Code of Professional Conduct that applies across the ecosystem.

> **In practice.** A manufacturer engages an RPA for readiness support and, separately, engages a C3PAO for the Level 2 assessment. The RPA realizes midway through the engagement that the C3PAO is owned by a parent firm that also operates a consulting arm. The consulting arm contacted the manufacturer directly to offer assessment preparation services, which the manufacturer declined because the RPA was already engaged. The RPA verifies through the C3PAO that the assessment and consulting functions are organized in separate legal entities with documented separation of personnel, which satisfies the conflict of interest rules. The practitioner understanding of these structural separations is what allows the practitioner to recognize when an arrangement is legitimate and when a conflict concern needs to be raised directly with the C3PAO.

Registered Practitioner Organizations (RPOs)

RPOs are consulting organizations registered with CyberAB to provide CMMC-related advisory services. Registration as an RPO signals that the organization has committed to the CyberAB Code of Professional Conduct and typically employs practitioners with CyberAB-registered credentials. RPO registration is distinct from C3PAO accreditation. RPOs do not perform assessments. RPOs provide consulting, readiness, implementation, and related advisory services to contractors preparing for or responding to CMMC assessments.

RPO registration is one valid structural arrangement for providing CMMC consulting services, but it is not the only one. Independent practitioners holding RP or RPA credentials can provide consulting services directly without RPO registration, either as sole proprietors or through firms they operate. The choice between RPO registration and independent practice reflects business model decisions rather than credential requirements. Some clients and engagement types benefit from the RPO organizational structure. Others are well served by independent practitioners operating under their individual credentials. The ecosystem accommodates both arrangements.

> **In practice.** A defense manufacturer has seventeen employees and a single facility. The manufacturer needs CMMC Level 2 readiness support and evaluates two candidate consultants. One is an independent RPA who operates as a sole proprietor without RPO registration. The other is an RPO with twelve staff and a national client base. Both are qualified. The manufacturer chooses the independent RPA because the engagement economics work better at that scale, the communication is direct with the credentialed practitioner rather than routed through account management, and the engagement fits a timeline that the RPO could not accommodate for six months. A year later, the manufacturer refers another small contractor to the same RPA. The ecosystem accommodates both structural arrangements because clients have genuinely different preferences and requirements.

The distinction between the consulting function that RPOs perform and the assessment function that C3PAOs perform is foundational to the CMMC ecosystem's integrity. The separation is analogous to the separation between financial auditors and financial consultants that has been enforced in accounting practice since the

Sarbanes-Oxley Act. A single organization cannot both advise a client on how to meet a standard and then assess whether the client has met it, because the conflict of interest would undermine the credibility of the assessment.

Organizations can hold both C3PAO accreditation and RPO registration, but the conflict rules require that the same organizational entity not perform both roles for the same client. Some firms maintain legally separate consulting and assessment entities to operate in both roles while preserving the separation. Others choose to operate only in one role to avoid the structural complexity.

Registered Practitioner (RP) and Registered Practitioner Advanced (RPA)

RP and RPA are individual practitioner credentials issued by CyberAB for consulting work. The RP credential requires completion of CyberAB-approved training and examination. The RPA credential requires additional training and examination beyond the RP baseline, typically focused on deeper technical content and assessment support skills. Both credentials are held by the individual practitioner and travel with that individual across employment or business structure changes.

RP and RPA credentials can be held by individuals in multiple structural arrangements. Many practitioners work as employees of RPOs, which provides the organizational infrastructure that supports consulting engagements at scale. Other practitioners operate as independent consultants, either as sole proprietors or through their own firms, without RPO affiliation. The credential itself does not require RPO affiliation. Independent RP and RPA practitioners are a legitimate and recognized part of the ecosystem, and they appear in the CyberAB Marketplace under their individual credentials. Some independent practitioners register their own firms as RPOs, which combines independent practice with the RPO structural recognition. The choice among these arrangements depends on the practitioner's business model, client base, and professional preferences rather than on credential requirements.

The RP and RPA credentials signal that the individual has met CyberAB's educational requirements and has committed to the Code of Professional Conduct.

The credentials do not authorize the holder to perform assessments. They authorize consulting work only. Practitioners with RP or RPA credentials who wish to perform assessment work must additionally obtain CCP or CCA credentials through ISACA's CAICO function, which is a separate pathway with distinct training, examination, and experience requirements.

In practice, the RP and RPA credentials are held by cybersecurity consultants across a range of practice structures, by IT service provider personnel, and by internal compliance staff at contractor organizations. The credential is recognized across the ecosystem as a baseline signal of CMMC subject matter competence, though the specific depth varies substantially across individuals holding the credential. The RP and RPA credentials remain under CyberAB administration following the CAICO transition, distinct from the CCP, CCA, and CCI credentials that transferred to ISACA.

> **In practice.** An RPA is asked by a prospective client whether the credential authorizes the practitioner to conduct the Level 2 assessment for the client's company. The practitioner explains that the RPA credential authorizes consulting and readiness work but does not authorize assessment work, and that the Level 2 certification assessment must be conducted by a C3PAO with CCA and CCP practitioners on the engagement team. The client then asks whether the practitioner can prepare the company for assessment, and the practitioner confirms that is exactly the scope the RPA credential covers. Clients regularly mix the consulting and assessment functions conceptually, and the practitioner who can draw the distinction clearly earns credibility as someone who understands the ecosystem boundaries.

Certified CMMC Professional (CCP), Certified CMMC Assessor (CCA), and Certified CMMC Instructor (CCI)

CCP, CCA, and CCI are individual practitioner credentials issued by ISACA under the CAICO role. The CCP credential is the entry-level assessment credential and authorizes the holder to participate in assessments as a team member under the direction of a Lead Assessor. The CCA credential authorizes the holder to serve as a

Lead Assessor on CMMC Level 2 assessments. The CCI credential authorizes the holder to deliver CMMC training through Licensed Training Providers.

Each credential requires substantial training, examination, and documented qualifying experience. The progression from CCP to CCA requires meaningful additional work and reflects the elevated responsibility of the Lead Assessor role. A Lead Assessor makes the professional judgment calls during an assessment that determine the assessment outcome, and the credential structure ensures that Lead Assessors have the experience base to exercise that judgment responsibly. The CCI credential operates on a parallel track, validating instructional capability alongside subject matter competence.

Individuals holding CCP or CCA credentials are typically employed by C3PAOs, though the credential travels with the individual rather than the employing organization. A CCA who changes employers from one C3PAO to another retains the credential and can perform assessment work through the new employer, subject to the credential's good-standing requirements. CCI holders are typically affiliated with Licensed Training Providers, whether as employees or as contracted instructors.

Practitioners pursuing these credentials interact with ISACA for registration, training provider identification, examination scheduling through PSI, background check processing, and credential issuance. Renewal and continuing education tracking also occur through ISACA. CyberAB retains authority over Tier 3 investigations of alleged professional conduct violations, which means that the most serious disciplinary processes involve both organizations in coordinated roles.

> **In practice.** A cybersecurity consultant decides to pursue assessment work and registers for the CCP credential through ISACA. The consultant identifies a Licensed Training Provider that offers CCP courseware, completes the training over several weeks, and schedules the CCP examination through PSI. After passing the examination, the background check process begins, with ISACA validating the consultant's experience against CCP requirements and coordinating any needed verification with CyberAB. The credential is issued months after the initial registration decision, reflecting the deliberate pace of

> the full certification process. Practitioners considering the CCP or CCA path should plan on the full sequence rather than expecting rapid credentialing.

Licensed Training Providers (LTPs) and Licensed Publisher Partners (LPPs)

LTPs are organizations licensed by CyberAB to deliver the training courseware that prepares candidates for practitioner examinations. LTP licensing ensures that training content aligns with established curricula and that training organizations meet quality standards for instruction. Candidates preparing for RP, RPA, CCP, CCA, or CCI examinations typically train through LTPs, though self-study options exist for experienced practitioners for some credentials.

LPPs are organizations licensed by CyberAB to publish the curriculum materials that LTPs use. The separation between course delivery and courseware publishing maintains quality control over the training ecosystem. A small number of LPPs produce the authoritative training materials, and LTPs across the ecosystem deliver those materials through live instruction, on-demand video, or blended formats.

The LTP and LPP functions remain under CyberAB licensing following the CAICO transition, even where the individual credentials earned through LTP-delivered training are issued by ISACA. This arrangement reflects the division of responsibility where CyberAB oversees the content delivery infrastructure and ISACA operates the individual certification function that uses that infrastructure.

> **In practice.** A practitioner preparing to pursue the CCA credential evaluates training options. Multiple LTPs offer CCA preparation courseware, with different formats (live instructor-led, on-demand video, blended) and different price points. The practitioner considers that the underlying curriculum is published by one of the LPPs, which means that different LTPs delivering that LPP's content are teaching from the same source material. The differentiation among LTPs is in delivery quality, instructor expertise, class schedule, and support services rather than in content coverage. The practitioner selects an

> LTP based on factors matching the practitioner's learning preferences and schedule rather than on content differences, because the content baseline is controlled at the LPP level.

Operational Systems

The CMMC ecosystem operates through specific government systems that persist the compliance record. Practitioners who understand the systems know where contractor data lives, how it moves between systems, and how the records persist across program cycles. The systems layer is less visible to practitioners than the entity layer but shapes the practical operation of compliance obligations in consequential ways.

Supplier Performance Risk System (SPRS)

SPRS is the Department of Defense system that receives contractor self-assessment scores against the NIST SP 800-171 control set. SPRS is accessed through the Procurement Integrated Enterprise Environment, the broader DoD procurement infrastructure commonly referred to as PIEE. Contractors register for SPRS access through PIEE and submit their scores through the SPRS interface.

The obligation to submit a SPRS score comes from DFARS 252.204-7019 for contractors under DFARS 252.204-7012 coverage, and the score submission is a precondition for being considered for contracts that contain the relevant flowdown language. SPRS scores range from 110 (full compliance) down to negative 203 (every control unimplemented), with the scoring methodology weighted to give heavier deductions for controls DoD considers more important to CUI protection.

Contractors have been submitting SPRS scores since late 2020 under the interim DFARS 7012 self-attestation regime. The submitted scores are the basis for several of the False Claims Act settlements that practitioners should be familiar with,

including Georgia Institute of Technology, MORSE Corp, and other cases. The persistence of the scoring record is important. A contractor who submitted a score in 2021 has that score retained for extended periods and subject to retrospective review, and the accuracy of the submission is a question that can be revisited at any time.

Under CMMC 2.0, SPRS continues to serve as the score submission system for contractors, but the certification decision for Level 2 assessments is captured separately. The SPRS score and the CMMC certification are related but distinct records.

> **In practice.** A practitioner engaged by a new client reviews the client's SPRS history as a first step in the engagement. The client submitted a score of 95 in 2021 and has not updated it since. The practitioner conducts a current-state assessment and concludes that the actual score based on implementation today would be 62. The gap between the submitted score and the current-reality score raises multiple questions. Was the 2021 submission accurate at the time? Has the environment degraded since then? Does the client have documentation of the 2021 state to defend the submission if it is later challenged? The practitioner's first-meeting questions often begin with SPRS review because the history there shapes everything that follows.

CMMC eMASS

CMMC eMASS is the specific deployment of the Enterprise Mission Assurance Support Service that captures CMMC assessment results. The CMMC PMO operates this system as the authoritative record of CMMC certifications. When a C3PAO completes a Level 2 assessment, the assessment results and certification decision are recorded in CMMC eMASS. This is the system that contract officers reference when verifying that a contractor holds the required CMMC certification for a particular contract.

The eMASS platform itself is broader than the CMMC-specific deployment. DoD uses eMASS as the system of record for Authority to Operate decisions across many DoD information systems. The CMMC deployment extends eMASS's functionality into the contractor certification context. Practitioners should understand that

CMMC eMASS is a specific deployment of a general platform, and that the underlying platform has broader uses that contractors and their internal personnel may encounter in other contexts.

The persistence of CMMC eMASS records has long-term implications for contractors. A certification decision, positive or negative, becomes part of the durable record that the program maintains. Updates, corrections, and re-certifications occur through defined processes, but the historical record of prior decisions remains accessible. Contractors whose certification lapses, whose assessments surface findings, or whose certifications are later challenged carry that history in the system. Practitioners advising contractors should recognize that the eMASS record is historically persistent and that changes to it occur through formal processes rather than through informal contractor-side modifications.

> **In practice.** A contractor's CMMC Level 2 certification expires because the triennial reassessment was not scheduled on time. The contractor engages an RPA to address the gap, and the engagement includes both technical remediation and re-certification planning. The RPA discovers that the original certification record in CMMC eMASS shows specific deficiencies noted during the initial assessment, some of which the contractor believed had been resolved through the POA&M process. The eMASS record documents what was actually addressed and what remained open at certification expiration. The practitioner's preparation for re-assessment has to begin from the documented state in eMASS rather than from the contractor's internal understanding, because the C3PAO conducting the new assessment will have access to the same record.

Oversight and Enforcement

The entities described in prior sections produce the framework, operate the assessments, and persist the records. The oversight and enforcement layer is what gives the framework consequence. Without enforcement mechanisms, compliance obligations would depend on voluntary commitment. The enforcement layer ensures that contractors who misrepresent their compliance posture face

meaningful consequences, which in turn motivates honest assessment preparation and accurate self-reporting.

ISOO Oversight

ISOO's oversight function was discussed in the policy layer section. The operational relevance of ISOO oversight for practitioners is that ISOO provides the mechanism through which CUI Program violations surface independently of the scheduled CMMC assessment cycle. Complaints filed with ISOO can trigger investigations that produce findings, corrective action requirements, and referrals to enforcement authorities. The ISOO complaint mechanism is accessible to employees, contractors, members of the public, and other interested parties, which means the surface area for complaint-driven exposure is broader than the surface area that a CMMC assessment covers.

Practitioners advising contractors on overall compliance posture should recognize that CMMC preparation addresses a specific subset of the obligations ISOO has authority over. A contractor who prepares thoroughly for CMMC but handles designation markings inconsistently, shares CUI through unauthorized channels, or fails to train personnel on CUI handling requirements from 32 CFR Part 2002 has residual exposure that the CMMC assessment does not address.

> **In practice.** A former employee of a defense contractor files a complaint with ISOO alleging that the contractor routinely shared CUI-marked documents through personal email accounts and cloud storage services outside the CUI-approved environment. The complaint names specific documents and specific incidents. ISOO reviews the complaint and forwards it to the contracting agency's CUI Senior Agency Official for investigation. The contractor is notified, produces documentation of its CUI handling procedures, and defends its practices. The practitioner supporting the contractor's CMMC readiness did not address the broader CUI dissemination practices because CMMC does not specifically assess them. The complaint investigation surfaces the gap, and the practitioner is brought back in to build a broader CUI handling program that addresses what CMMC preparation alone did not cover.

DoD Office of Inspector General

The DoD Office of Inspector General conducts independent oversight of DoD programs including the defense contracting ecosystem. The DoD OIG has authority to audit, investigate, and evaluate DoD programs and the contractors participating in them. For CMMC practitioners, the DoD OIG matters because OIG audits and investigations can surface contractor compliance failures that did not become visible through the regular assessment cycle.

DoD OIG reports are public documents that often identify specific contractors by name when findings are serious. A contractor whose CMMC-related compliance fails an OIG audit faces reputational exposure independent of the contractual or prosecutorial consequences. Practitioners can strengthen client compliance posture by understanding the patterns DoD OIG has historically pursued and ensuring that client implementations address those patterns rather than treating CMMC preparation as the complete compliance picture.

> **In practice.** A DoD OIG report addresses cybersecurity weaknesses among defense contractors performing specific types of work. The report names several contractors and describes patterns of deficiency including inadequate incident reporting, weak access control implementations, and missing security monitoring. A practitioner working with clients in the affected segment reviews the report and identifies which client environments exhibit the patterns the OIG flagged. The practitioner uses the report as a concrete reference for conversations with client leadership about compliance priorities. OIG findings surface the specific failure modes that regulators consider important, which gives practitioners substantive material to ground advisory work.

Department of Justice Civil Division

The Department of Justice Civil Division is the federal enforcer of the False Claims Act and the primary prosecutorial authority for compliance-related contract fraud. The False Claims Act, codified at 31 USC sections 3729 through 3733, imposes treble damages plus civil penalties per false claim on contractors who knowingly make false statements in connection with federal contracts. The statute authorizes qui

tam relator actions, which allow private parties with knowledge of fraud to file suits on behalf of the United States and share in recoveries.

The DoJ Civil Division has pursued multiple cybersecurity-related False Claims Act actions in recent years, with settlements that practitioners should be familiar with. Georgia Institute of Technology settled for $875,000 in August 2024 over allegations including a false SPRS score and unauthorized CUI handling environment. MORSE Corp settled for $4.6 million in March 2025 over allegations of a reported SPRS score of 104 against an actual score of negative 142, with no SSP and the majority of required controls unimplemented. Raytheon Technologies settled for $8.4 million in October 2024 over cybersecurity compliance allegations. Each case involved qui tam relators who provided the initial allegations that triggered DoJ investigation.

For CMMC practitioners, the DoJ enforcement reality shapes how advisory work should be conducted. A practitioner who signs off on an SSP or assessment preparation work product that later proves materially inaccurate has both professional and potentially legal exposure. Documentation of the professional basis for the work product, the information the practitioner relied on, and the caveats that applied protects both the practitioner and the client. Practitioners should also counsel clients on the discovery risk that qui tam relators represent, which is greater than many clients appreciate.

> **In practice.** A practitioner receives a document request in connection with a DoJ investigation of a former client. The investigation concerns a SPRS submission the practitioner helped prepare three years earlier. The request asks for engagement documentation, communications with the client, draft versions of the SSP, and the practitioner's working papers. The practitioner who maintained disciplined documentation practices produces records showing the information the client provided, the assumptions the work product was based on, the caveats and limitations expressed to the client, and the recommendations the practitioner made that the client chose not to implement. The documentation allows the practitioner to establish that the work product reflected the client's representations at the time rather than any misrepresentation the practitioner knowingly endorsed. Practitioners who do

> not document carefully find themselves in a very different position when document requests arrive.

Qui Tam Relators

Qui tam relators are not entities in the organizational sense, but they represent a specific category of actor in the enforcement ecosystem that practitioners need to understand. The False Claims Act allows private individuals with knowledge of fraud against the government to file sealed complaints on the government's behalf. If the government intervenes and recovers damages, the relator receives a share of the recovery ranging from 15 to 30 percent. For major cybersecurity False Claims Act cases, relator shares can exceed a million dollars.

The incentive structure creates real discovery risk for contractors. Employees with knowledge of the contractor's actual compliance posture can become qui tam relators, particularly when they have been terminated, when they believe they have been retaliated against, or when they have ethical objections to practices they observe. Former employees carry the same discovery risk, often with less reason to hesitate before filing. The categories of individuals who can become relators includes current employees, former employees, contractors, consultants, and members of the public with relevant knowledge.

Practitioners who work across multiple client engagements have visibility into client compliance postures that most individuals never see. Ethical obligations under professional conduct frameworks, including the CyberAB Code of Professional Conduct, govern what practitioners do with that visibility. Practitioners who encounter material misrepresentations during client engagements face genuine ethical and legal considerations about their own obligations that warrant thoughtful handling.

> **In practice.** A practitioner conducting a readiness engagement discovers that the client's submitted SPRS score materially overstates the actual implementation. The practitioner explains the gap to the client's leadership and recommends a corrected submission. The client leadership declines to correct the submission, citing competitive concerns about losing eligibility for current contracts. The practitioner faces a decision about how to proceed.

> Continuing the engagement with full knowledge of the misrepresentation creates practitioner exposure. Withdrawing from the engagement leaves the client in the same position with a different consultant. The practitioner consults with legal counsel about the ethical and reporting considerations involved. These situations are rare but real, and the practitioner's documented approach to them matters substantially if a qui tam action later emerges around the same client and the same time period.

The Lifecycle View

The entities and systems described above interact with contractors across a predictable lifecycle that spans years. Understanding when each entity acts on a contractor allows practitioners to sequence their advisory work appropriately and to prepare clients for interactions they may not otherwise anticipate.

Pre-solicitation. Before a CMMC-applicable contract is solicited, the contractor should understand the CUI Program framework, have implemented the protection controls, have a documented SSP, and have submitted a SPRS score. The entities active at this stage include NARA and ISOO at the framework level, NIST as the source of the technical standards, OUSD(A&S) and the CMMC PMO as the DoD program owners, and potentially CyberAB through RPO and RP/RPA advisory support. The contractor's own leadership makes the strategic decisions about compliance investment and governance structure.

Solicitation. When a CMMC-applicable solicitation is issued, DoD applies the appropriate CMMC level requirement based on the contract's information sensitivity. Contractors who are eligible at that level compete for the award. The contract officer's office references SPRS to verify score submissions and, once CMMC certifications become common, references CMMC eMASS to verify certification status at the required level.

Award. Upon contract award, the flowdown requirements in the contract establish the specific obligations the contractor must meet. DFARS 252.204-7012 requires NIST SP 800-171 implementation and incident reporting. DFARS 252.204-7019 requires SPRS score submission. DFARS 252.204-7020 gives DoD the right to verify

contractor assertions. DFARS 252.204-7021 contains the CMMC-specific flowdown language. The contractor becomes legally obligated to the commitments made in the SPRS score and any CMMC certification.

Performance. During contract performance, the contractor handles CUI consistent with the framework. CUI received from DoD retains its designation and must be protected accordingly. Cyber incidents must be reported within 72 hours under DFARS 7012. Changes to the contractor's environment that affect the compliance posture must be reflected in updated documentation and, potentially, updated SPRS scores. Subcontracts that flow down CMMC requirements must be managed with appropriate oversight of subcontractor compliance. ISOO complaints, if filed, can trigger investigations during performance. DoD OIG or other oversight bodies can conduct audits.

Assessment. For Level 2 certification, the contractor engages a C3PAO when certification is required. The C3PAO conducts the assessment, staffed by ISACA-credentialed CCP and CCA practitioners, produces the assessment result, and records the certification decision in CMMC eMASS. Assessment preparation typically begins months before the assessment engagement, with RPO and RP or RPA support under CyberAB credentials. The assessment itself typically takes several days to several weeks depending on the scope and size of the environment.

Post-certification. After certification, the contractor is subject to surveillance reviews, triennial reassessment, and continuous obligation to maintain compliance. The SPRS score remains on record and must be updated annually or when material changes occur. The CMMC certification becomes a precondition for continued eligibility on CMMC-applicable contracts. Changes in the regulatory environment, including potential transition to NIST SP 800-171 Revision 3, may require additional preparation work.

Enforcement. At any point in the lifecycle, the enforcement layer can become active. ISOO complaints, OIG audits, and qui tam relator filings can trigger investigations that produce findings, corrective action requirements, and in serious cases DoJ enforcement actions. The enforcement layer operates continuously rather than on a scheduled cycle, which means contractors and their

advisors cannot simply prepare for scheduled events and consider their compliance exposure managed.

Practitioner Implications

A practitioner working in the CMMC ecosystem interacts with a subset of the entities described in this paper directly and the remainder indirectly. An RP or RPA working on readiness engagements interacts primarily with CyberAB through the credential and through the Marketplace, with RPOs through employment or affiliation, and with NIST publications through primary reference material. A CCP, CCA, or CCI interacts with ISACA through the CAICO function for credential issuance and renewal, with CyberAB for professional conduct standards and Tier 3 investigations, and with C3PAOs or LTPs through employment. Every practitioner ultimately references the policy layer through 32 CFR Part 2002 and the related framework documents, even when the direct interaction is with downstream implementations.

Competent practice requires holding the full ecosystem map in mind even when daily work touches only a portion of it. Client questions surface across the full ecosystem. A readiness client may ask about ISOO oversight. An assessment client may ask about SPRS score history. A compliance officer at a prime contractor may ask about DCSA and CMMC eMASS interaction. An assessment team member may ask about the split between CyberAB and ISACA in credential administration. The practitioner who has built the structural mental model can answer these questions with accuracy and authority. The practitioner who has not done that work produces advice that is accurate in its narrow focus but incomplete when questions cross boundaries.

The ecosystem will continue to evolve. NIST SP 800-171 Revision 3 is pending eventual integration into CMMC. The CAICO role held by ISACA will refine its operations over time as the transition matures. DoD policy around enforcement priorities evolves with administration transitions. CyberAB practices refine as the ecosystem matures. The practitioner who understands the current structure is positioned to understand future changes as adjustments to a known framework

rather than as unintelligible developments. The investment in structural understanding pays forward across the full arc of a professional career in this domain.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced and the founder of David Koran & Associates Inc., a practice serving Defense Industrial Base contractors and their legal counsel. The firm focuses on CMMC readiness, enablement, and implementation consulting. David is an Associate Member of the American Bar Association Section of Public Contract Law and a professional member of ISACA. He is the author of The CMMC Decision, a strategic guide for CEOs and senior executives of small and mid-sized defense contractors.

David can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

Executive Order 13556, Controlled Unclassified Information, November 4, 2010. https://www.archives.gov/cui/about/executive-order-13556

32 CFR Part 2002, Controlled Unclassified Information, September 14, 2016. https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002

National Archives and Records Administration, CUI Registry. https://www.archives.gov/cui/registry/category-list

Information Security Oversight Office. https://www.archives.gov/isoo

NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information, June 2018. https://csrc.nist.gov/publications/detail/sp/800-171a/final

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting

DFARS 252.204-7019 and 7020, NIST SP 800-171 DoD Assessment Requirements. https://www.acquisition.gov/dfars/252.204-7019-notice-nist-sp-800-171-dod-assessment-requirements

DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements. https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements

32 CFR Part 170, Cybersecurity Maturity Model Certification Program, October 15, 2024. https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

CyberAB Marketplace. https://cyberab.org/Marketplace

CyberAB Code of Professional Conduct. https://cyberab.org/Catalog/CMMC-Code-of-Professional-Conduct

ISACA CMMC Certifications. https://www.isaca.org/credentialing/cmmc

CyberAB Announcement of ISACA as CAICO, December 2025. https://cyberab.org/News-Events

Supplier Performance Risk System. https://www.sprs.csd.disa.mil/

Procurement Integrated Enterprise Environment. https://piee.eb.mil/

Defense Counterintelligence and Security Agency, Defense Industrial Base Cybersecurity Assessment Center. https://www.dcsa.mil/Industrial-Security/Cybersecurity-for-DoD-Contractors/

Enterprise Mission Assurance Support Service (eMASS). https://www.dcsa.mil/Systems-Applications/Enterprise-Mission-Assurance-Support-Service-eMASS/

False Claims Act, 31 U.S.C. sections 3729 through 3733. https://www.justice.gov/civil/false-claims-act

Department of Justice Civil Cyber-Fraud Initiative. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

Department of Defense Office of Inspector General. https://www.dodig.mil/