Before You Hire a CMMC Consultant

A Contractor's Guide to Verifying CMMC Practitioner Credentials

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

Introduction

The CMMC ecosystem has created a new category of professional services for the defense industrial base. Contractors pursuing Level 2 certification need practitioners who can guide them through readiness, build their documentation, configure their technical controls, and prepare them for a C3PAO assessment. The demand for these services is growing faster than the supply of credentialed practitioners, and that imbalance has created an environment where it is difficult for a contractor to distinguish between a qualified consultant and one who is not what they claim to be.

The consequences of selecting the wrong consultant are not limited to wasted fees. An engagement with an unqualified or conflicted practitioner can result in documentation that does not survive assessment scrutiny, technical configurations that must be reworked, delayed contract eligibility while the organization starts over with a credible practitioner, or in the most serious cases, an assessment that is later invalidated due to conflict of interest violations. These are business risks, not just compliance inconveniences.

This paper is written for contractors who are evaluating CMMC consultants. It explains the credentialed roles within the CMMC ecosystem, describes the regulatory separation between enablement and assessment, identifies the single authoritative source for verifying practitioner credentials, summarizes the Code of Professional Conduct that governs credentialed practitioners, and provides a practical set of verification steps and red flags that any contractor can use before signing an engagement.

The goal is not to tell you who to hire. The goal is to give you the tools to verify that the person you are considering is who they say they are and is authorized to do what they are offering to do.

The Credentialed Roles in the CMMC Ecosystem

The Cyber AB (formerly the CMMC Accreditation Body) is the sole organization authorized by the Department of Defense to credential individuals and accredit organizations within the CMMC ecosystem.[1] Every legitimate CMMC credential traces back to the Cyber AB. Understanding the roles and their boundaries is the first step in evaluating whether a consultant is operating within their authorized scope.

Registered Practitioner (RP)

The Registered Practitioner is the entry-level CyberAB credential for individuals providing CMMC consulting services. RPs have completed the required training and background check and are authorized to assist organizations with CMMC readiness, enablement, and implementation. They work on the enablement side of the ecosystem, meaning they help contractors prepare for assessment. They do not conduct assessments and they do not issue certifications.

Registered Practitioner Advanced (RPA)

The Registered Practitioner Advanced holds the same enablement authorization as the RP but has demonstrated additional competency through an advanced credentialing process. The RPA is still on the enablement side of the ecosystem. The distinction between RP and RPA reflects depth of demonstrated knowledge, not a change in the type of work the practitioner is authorized to perform.

Certified CMMC Assessor (CCA)

The Certified CMMC Assessor is credentialed to participate on a C3PAO assessment team.[2] CCAs conduct the formal assessments that determine whether an

[1] 32 CFR 170.8(a). The Accreditation Body is responsible for authorizing and ensuring the accreditation of C3PAOs and credentialing individuals within the CMMC ecosystem.

[2] 32 CFR 170.11(a). CCAs conduct Level 2 certification assessments of OSCs in accordance with NIST SP 800-171A and the assessment processes defined in 32 CFR 170.17.

organization meets the requirements for CMMC certification. They operate on the assessment side of the ecosystem. A CCA working independently as a readiness consultant would need to manage conflicts of interest carefully, because the Code of Professional Conduct places restrictions on practitioners who operate on both sides of the enablement and assessment boundary.

Certified CMMC Professional (CCP)

The Certified CMMC Professional credential indicates foundational knowledge of the CMMC framework. CCPs may serve in support roles on assessment teams or in advisory capacities.[3] Like all CyberAB credentials, the CCP is verifiable through the Marketplace.

CMMC Third-Party Assessment Organization (C3PAO)

C3PAOs are the organizations accredited by the CyberAB to conduct official CMMC assessments.[4] A C3PAO is not an individual; it is an organization that employs or contracts with credentialed assessors. Only a C3PAO can issue assessment results that lead to CMMC certification. No individual practitioner, regardless of their credential, can certify an organization on their own.

[3] 32 CFR 170.13(a). A CCP completes rigorous training on CMMC and the assessment process to provide advice, consulting, and recommendations to their OSA clients.

[4] 32 CFR 170.9(a). C3PAOs are organizations responsible for conducting Level 2 certification assessments and issuing Certificates of CMMC Status to OSCs.

The Bright Line Between Enablement and Assessment

The CMMC ecosystem is designed with a structural separation between the practitioners who help organizations prepare for certification and the organizations that conduct assessments. This separation exists to protect the integrity of the certification process. A practitioner who builds an organization's SSP and configures its controls should not be the same person who evaluates whether those controls are adequate.

The CyberAB created the Registered Practitioner and Registered Practitioner Advanced credentials specifically to fill the enablement role. The RP and RPA exist for the purpose of helping contractors with readiness, implementation, and preparation for assessment. That is what the credential was designed for. When a contractor engages an RP or RPA for consulting work, the practitioner is operating squarely within the role the ecosystem was built to support.

Certified CMMC Assessors and C3PAOs operate on the assessment side. Their role is to evaluate whether the organization meets the CMMC requirements and to produce the assessment results that the Department of Defense relies on for certification decisions.

This does not mean that a CCA or CCP is prohibited from providing consulting services. Many qualified professionals hold assessment-side credentials and also do enablement work. However, when a CCA provides readiness consulting to an organization, they are operating outside the specific role their credential was designed for, and they must manage the conflict of interest that arises if they or their affiliated C3PAO later assess that same organization. The Code of Professional Conduct places explicit restrictions on this scenario.[5]

For a contractor evaluating consultants, the practical takeaway is straightforward. An RP or RPA providing readiness services is operating in the role the CyberAB designed for that purpose. A CCA or CCP providing readiness services may be fully

[5]CyberAB Code of Professional Conduct v2.0, Consulting/Advisory Conflict section. The prohibition covers any preparatory, advisory, or consulting activities for any type of CMMC assessment.

competent to do so, but the contractor should ask how the enablement and assessment boundary will be maintained, and should verify that the practitioner's consulting engagement will not create a conflict when it comes time for the C3PAO assessment.

The C3PAO Consulting and Referral Question

Some contractors report being approached by C3PAOs that offer consulting services to prepare the organization for assessment, with the understanding that a different C3PAO, often described as a colleague or associate, will then conduct the formal assessment. This arrangement deserves careful scrutiny.

The Code of Professional Conduct v2.0 is explicit on the direct conflict. A C3PAO and all of its assessment team members are prohibited from participating in an assessment for an organization they previously served as a consultant to prepare for any CMMC assessment. This prohibition extends for three years.[6] It applies to the C3PAO as an organization as well as to every individual on the assessment team. A C3PAO that consults for a contractor and then assesses that same contractor is in direct violation.

The referral arrangement is one step removed from the direct prohibition, but it raises the same underlying concern. When C3PAO "A" consults for a contractor and then refers that contractor to C3PAO "B" for assessment, C3PAO "A" has a reputational and financial interest in the assessment going well. A failed assessment reflects on the quality of their consulting work. If the referral is reciprocal, meaning C3PAO "B" sends its own consulting clients to C3PAO "A" for assessment, the arrangement creates a mutual dependency that undermines the independence the ecosystem was designed to protect.

The Code of Professional Conduct addresses this through its conflict of interest disclosure requirements. C3PAO conflicts of interest, both organizational and individual, can be based on financial, business, or other relationships.[7] The code does not state that all conflicts are prohibited. It states that all conflicts must be

[6]CyberAB Code of Professional Conduct v2.0. This prohibition applies to the C3PAO as an organization as well as to all of its Assessment Team members, and extends for three years.

disclosed, and that depending on their nature, they must be either mitigated or avoided. A referral relationship between two C3PAOs is a business relationship. If it is not disclosed to the contractor and to the CyberAB, the failure to disclose is itself a violation of the code, regardless of whether the underlying arrangement would have been permissible if transparent.[8]

For a contractor, the practical guidance is this. If a C3PAO or any consultant tells you they can get you assessed faster through a relationship with another C3PAO, ask specific questions. What is the nature of the relationship between the two organizations? Is the referral reciprocal? Has the relationship been disclosed to the CyberAB? Will the assessing C3PAO be informed that the referring organization provided consulting services? A credible practitioner or organization will answer these questions directly. Evasiveness or vagueness in response to these questions is itself informative.

Contractors should also understand that assessment results do not exist in a vacuum. C3PAOs submit assessment results into the CMMC instantiation of eMASS, where the Department of Defense has direct visibility.[9] Under 32 CFR 170.8, the CMMC PMO retains the prerogative to review Accreditation Body decisions and evaluate any alleged conflicts of interest purported to influence the assessment process.[10] The Accreditation Body is required to investigate potential violations reported or identified by the DoD, notify the DoD of new investigations within 72 hours, and report the outcome within 15 business days.[11] C3PAOs are required to

---

[7]CyberAB Code of Professional Conduct v2.0; 32 CFR 170.8(b)(17)(i)(E). CMMC Ecosystem members must disclose to Accreditation Body leadership, in writing, any actual or potential conflict of interest as soon as it is known or reasonably should be known.

[8]CyberAB Code of Professional Conduct v2.0. "It is the failure to disclose a COI that runs afoul of responsible ethical behavior. Most COIs can be mitigated in some manner or another, while other conflicts must simply be avoided."

[9]32 CFR 170.8(b). The CMMC PMO retains the prerogative to review decisions of the Accreditation Body and evaluate any alleged conflicts of interest purported to influence its objectivity.

[10]32 CFR 170.8(b)(17)(ii)(C)(D). The Accreditation Body must inform the DoD in writing of new investigations within 72 hours and report the outcome of completed investigations within 15 business days.

[11]32 CFR 170.9(a)(9). C3PAOs must maintain all assessment related records for a period of six years.

maintain all assessment-related records for six years.[12] If an assessment is later found to have been conducted under circumstances that violated the conflict of interest or Code of Professional Conduct provisions, the DoD has the authority and the audit trail to act on that finding. The consequences for the contractor could include the invalidation of the assessment and the loss of the certification that the contractor relied upon for contract eligibility.

The CyberAB Marketplace: The Single Source of Truth

The CyberAB maintains a public, searchable registry called the Marketplace. It is accessible at cyberab.org and it is the only authoritative source for verifying whether an individual holds a current CMMC credential. The Marketplace lists the practitioner's name, their credential type, and their current status.

Verification takes less than two minutes. Before entering into any engagement with a CMMC consultant, search the Marketplace for their name or their affiliated organization and confirm that their credential type and status match what they have represented. Individual practitioners may appear under their own name or under the profile of their affiliated Registered Provider Organization or C3PAO. This single step eliminates the most common form of credential misrepresentation.

Legitimate Processing Gaps

There are situations in which a practitioner may hold or be in the process of obtaining a credential and not yet appear in the Marketplace, or may appear without full standing. Understanding these situations helps a contractor distinguish between a processing delay and a credential that does not exist.

Tier 3 Background Investigation. CCPs and CCAs are required to complete a Tier 3 suitability investigation to be considered in good standing and eligible to

[12] 32 CFR 170.9(a)(8). C3PAOs must submit pre-assessment and planning material, final assessment reports, and CMMC certificates of assessment into the CMMC instantiation of eMASS.

participate on assessment teams.[13] This process has experienced significant delays, sometimes exceeding twelve months for individuals without an existing security clearance. A practitioner may appear in the Marketplace after passing their exam but without the suitability indicator until the Tier 3 process is complete. This is a known bottleneck in the ecosystem and does not, by itself, indicate a credential problem.

Delta Training Requirements. In December 2024, the CyberAB updated Marketplace listing requirements to reflect changes introduced by the CMMC Final Rule.[14] CCPs and CCAs who had not completed the required delta training and testing were suspended from the Marketplace until they fulfilled the updated requirements. Some previously credentialed individuals may have been temporarily removed during this period.

ISACA Transition. Effective April 1, 2026, ISACA assumed responsibility as the sole managing body for CCP, CCA, Lead CCA, and CCI credentials.[15] New applications now route through ISACA, which validates experience and coordinates with the CyberAB for background checks. The CyberAB retains authority over the Marketplace itself. Processing gaps during this transition period are possible, particularly for individuals who applied near the transition date.

Brief Processing Window After Exam Completion. Approved Training Providers submit training completion rosters to the credentialing body within days of course completion, and credentials are typically updated within the same week. A gap of a few business days between exam completion and Marketplace listing is normal.

What This Means for Verification

A brief, explainable processing delay is not a red flag. A credible practitioner who has recently completed their credentialing process will be able to describe exactly

[13]32 CFR 170.11(b)(3); 32 CFR 170.13(b)(3). CCAs and CCPs must complete a Tier 3 background investigation resulting in a determination of national security eligibility.

[14]CyberAB Town Hall, December 2025; ISACA CAICO announcement. ISACA assumed management of CCP, CCA, LCCA, and CCI credentials effective April 1, 2026.

[15]CAICO CMMC Ecosystem Notification, December 17, 2024. Marketplace listing requirements updated to reflect 32 CFR Final Rule changes; assessment team members not meeting updated requirements were suspended.

where they are in that process, name their training provider, and point to the specific step that has not yet been reflected in the Marketplace. What should concern a contractor is a practitioner who has claimed a credential for an extended period, cannot provide a specific explanation for their absence from the Marketplace, or becomes evasive when asked to verify. The Marketplace remains the definitive record. If a consultant cannot be found there and cannot explain why in specific, verifiable terms, the contractor should proceed with caution.

The Code of Professional Conduct

Every individual who holds a CyberAB credential is bound by the CyberAB Code of Professional Conduct. This code establishes the ethical and professional standards that govern how credentialed practitioners operate within the ecosystem. A contractor does not need to memorize the code, but understanding its key provisions helps in evaluating whether a consultant is operating within appropriate boundaries.

Conflict of Interest. Credentialed practitioners are required to identify and disclose conflicts of interest. A practitioner who has a financial interest in a product or service they are recommending, or who is offering both enablement and assessment services to the same organization, has a conflict that must be disclosed and managed. The code does not merely discourage conflicts of interest; it requires practitioners to actively avoid situations where their judgment could be compromised.

Scope of Practice. Practitioners are expected to operate within the scope of their credential. An RP or RPA is authorized to provide enablement services. They are not authorized to represent themselves as assessors, to conduct activities that constitute an assessment, or to represent that their work product will guarantee a specific assessment outcome.

Accuracy and Integrity. The code requires practitioners to be truthful and accurate in their representations, including their credentials, qualifications, and the scope of services they are authorized to provide.[16] Misrepresenting a credential, whether by claiming one that was never issued or by continuing to represent a lapsed credential as active, is a direct violation.

Confidentiality. Practitioners are required to protect the confidentiality of client information obtained during the course of an engagement. This includes

[16]CyberAB Code of Professional Conduct v2.0; 32 CFR 170.8(b)(17)(ii)(E). Ecosystem members must represent themselves and their companies accurately, including not misrepresenting any professional credentials or status.

assessment data, security posture information, and any proprietary business information shared during the readiness process.[17]

The CyberAB accepts complaints against credentialed practitioners who violate the Code of Professional Conduct. If a contractor believes that a practitioner has violated the code, a formal complaint can be filed through the CyberAB.

Verification Steps Before Engaging a Consultant

The following steps represent a practical due diligence process that any contractor can complete before entering into an engagement with a CMMC consultant. None of these steps require technical expertise or specialized knowledge.

Step 1: Search the CyberAB Marketplace. Go to cyberab.org and search for the individual by name. Confirm that they appear in the Marketplace, that their credential type matches what they have represented, and that their status is active. If they do not appear, ask them to explain. A legitimate practitioner will be able to point you to their listing.

Step 2: Confirm the credential type matches the service being offered. An RP or RPA should be offering readiness, enablement, and implementation services. If someone with an RP credential is offering to assess your organization or is representing that they can issue certification results, the service does not match the credential.

Step 3: Ask about organizational affiliation. Determine whether the practitioner is operating independently or is affiliated with a C3PAO, a Registered Provider Organization (RPO), or another firm. If they are affiliated with a C3PAO and are also offering readiness services to your organization, ask how the conflict of interest is managed. Under the Code of Professional Conduct, a practitioner who provides consulting or advisory services to prepare an organization for assessment is

[17] CyberAB Code of Professional Conduct v2.0; 32 CFR 170.13(b)(6); 32 CFR 170.11(b)(9). Information obtained during assessment activities must not be shared with persons not involved in the assessment.

prohibited from serving on the assessment team for that same organization for three years. This prohibition applies to the individual and to the C3PAO as an organization. A credible practitioner will have a clear answer about how this boundary is maintained.

Step 4: Ask for references from completed engagements. A practitioner with real experience will be able to provide references from contractors they have worked with, subject to the confidentiality provisions of the Code of Professional Conduct. The references do not need to disclose assessment details, but they should be able to confirm that the practitioner performed the work they are representing.

Step 5: Evaluate the depth of their knowledge. Ask the consultant a question specific to your environment. If you are a manufacturer with a shop floor, ask how they would approach scoping CUI assets in a production environment. If you use a managed service provider, ask how they would handle ESP classification. A practitioner with real implementation experience will give you a substantive answer. One who is operating beyond their depth will give you a general answer that could apply to any organization.

Step 6: Verify complementary credentials independently. If the consultant claims to hold credentials outside the CyberAB ecosystem, such as CISSP, CISA, or CISM, those credentials are independently verifiable. CISSP is verifiable through ISC2. CISA and CISM are verifiable through ISACA. A practitioner who holds legitimate credentials will not object to you verifying them.

Red Flags

The following observations, individually or in combination, should prompt additional scrutiny before engaging a CMMC consultant.

The practitioner does not appear in the CyberAB Marketplace and cannot explain why. As discussed earlier in this paper, there are legitimate processing scenarios in which a credentialed practitioner may not yet appear in the Marketplace or may appear without full standing. A brief, specific, verifiable explanation is reasonable. What is not reasonable is a practitioner who has represented a credential for months, cannot be found in the Marketplace, and either has no explanation or becomes vague when asked. The burden of providing a credible explanation falls on the practitioner, not on you.

The practitioner offers both readiness services and assessment services. The CMMC ecosystem is designed to separate these functions. A practitioner who offers to prepare your organization and then assess it, or who implies that they can arrange a favorable assessment outcome, is describing a process that does not align with how the ecosystem operates.

The practitioner guarantees certification. No practitioner on the enablement side can guarantee a certification outcome. Certification is determined by a C3PAO assessment team based on their independent evaluation. A consultant who guarantees certification is either misrepresenting the process or does not understand it.

The consultant claims they can get you assessed faster through a relationship with a C3PAO. As discussed earlier in this paper, a consulting organization that refers clients to a specific C3PAO for assessment has a business relationship that the Code of Professional Conduct requires to be disclosed. If the consultant cannot clearly explain the nature of the referral relationship, whether it is reciprocal, and whether it has been disclosed, the arrangement may compromise the independence of the assessment.

The practitioner is vague about their credential type. The CyberAB credentials are specific: RP, RPA, CCA, CCP. If a consultant describes themselves as "CMMC

certified," "CMMC qualified," "CMMC expert," or "CMMC advisor" without specifying which credential they hold, ask for the specific credential type and verify it. None of these descriptions correspond to an actual CyberAB credential.

The practitioner lists credentials on their profile that cannot be independently verified. Legitimate professional credentials have public verification mechanisms. If a consultant lists multiple certifications and none of them can be confirmed through the issuing organization's public registry, that pattern warrants caution.

The practitioner recommends a specific product or vendor without disclosure. If a consultant steers you toward a specific GRC platform, managed security provider, or technology solution without disclosing any financial relationship with that vendor, the recommendation may not be in your best interest. The Code of Professional Conduct requires disclosure of conflicts of interest, including financial relationships with product vendors.

The practitioner cannot describe implementation specifics for your environment. CMMC readiness is not generic. Every organization has a different network architecture, different CUI flows, different asset inventory, and different operational constraints. A consultant who provides only high-level guidance without engaging with the specifics of your environment may not have the implementation experience necessary to prepare you for assessment.

What a Credible Engagement Looks Like

For comparison, the following characteristics are typical of a legitimate CMMC readiness engagement led by a credentialed practitioner.

The practitioner's credential is verifiable in the CyberAB Marketplace and matches the services being offered. The engagement begins with a scoping discussion to understand the organization's CUI flows, asset inventory, and network architecture before any work begins. The practitioner explains the separation between enablement and assessment and does not represent that their involvement will guarantee a specific outcome. The engagement produces tangible

deliverables, including a System Security Plan, a Plan of Action and Milestones, supporting policies, and evidence artifacts, rather than general advice. The practitioner is transparent about their fee structure, their organizational affiliation, and any relationships with product vendors. The practitioner is willing to explain their approach to specific controls and can demonstrate familiarity with the assessment process, including what assessors will look for and how evidence should be organized.

None of these characteristics require the contractor to have technical expertise to evaluate. They are observable through normal business due diligence, and a credible practitioner will welcome the scrutiny.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced (RPA) and the founder of David Koran & Associates, a CMMC consulting practice serving Defense Industrial Base contractors and their legal counsel. The firm provides readiness, enablement, and implementation services for organizations pursuing CMMC certification. He is an Associate Member of the ABA Section of Public Contract Law. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

Cyber AB. (2026). CyberAB Marketplace: Public Registry of Credentialed Practitioners and Accredited Organizations. https://cyberab.org/marketplace

Cyber AB. (2025). Code of Professional Conduct for Credentialed Practitioners. https://cyberab.org/

Cyber AB. (2025). CMMC Assessment Guide Level 2, Version 2.13. https://cyberab.org/

Department of Defense. (2024). Cybersecurity Maturity Model Certification (CMMC) Program Final Rule, 32 CFR Part 170. https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

ISC2. (2026). Member Directory: CISSP Credential Verification. https://www.isc2.org/

ISACA. (2026). Credential Verification: CISA, CISM, CRISC. https://www.isaca.org/