The MSP/ESP Paradox

Navigating External Service Provider Requirements in CMMC Level 2 Enablement

A White Paper for Defense Industrial Base Leadership

David W. Koran, CMMC Registered Practitioner
March 2026
dkoran@davidkoran.com

Executive Summary

The Department of Defense has redefined the compliance landscape for defense contractors, and the implications extend well beyond the contractor's own four walls. With the publication of 32 CFR Part 170 in October 2024 and the activation of Phase 1 on November 10, 2025, the Cybersecurity Maturity Model Certification (CMMC) program has become a contractual reality for the Defense Industrial Base (DIB). What many contractors have not yet internalized is that their eligibility for Department of Defense (DOD) contract awards is now directly tied to the compliance posture of the external organizations that manage, monitor, and secure their information technology environments.

This white paper examines a specific and consequential dimension of CMMC Level 2 enablement: the role, regulatory classification, and compliance obligations of Managed Service Providers (MSPs) and External Service Providers (ESPs). The analysis is anchored in the regulatory text of 32 CFR Part 170, the DOD FedRAMP Equivalency Memorandum dated December 21, 2023, the CMMC Level 2 Scoping Guide, and the CMMC Assessment Process (CAP) Guide version 2.0. The paper addresses the paradox that confronts many DIB contractors in 2026: the very providers hired to strengthen a contractor's cybersecurity posture may be the ones placing that contractor's CMMC certification at risk.

The intended audience for this paper is C-Suite executives, IT directors, compliance officers, and government contracts counsel within DIB organizations. The goal is to deliver a clear, evidence-based analysis to support informed decision-making on ESP selection, contract structuring, and pre-assessment readiness planning.

1. The Role of Managed Service Providers and External Service Providers in the Defense Industrial Base

The majority of small and mid-sized defense contractors do not maintain a fully staffed, internal information technology department. Instead, they rely on external organizations to provision, manage, and secure their IT infrastructure. These external organizations are most commonly referred to as Managed Service Providers (MSPs) or Managed Security Service Providers (MSSPs). In practice, an MSP is a third-party firm that assumes operational responsibility for some or all of a contractor's IT environment. The services delivered by an MSP typically include network monitoring, endpoint management, patch deployment, backup administration, user provisioning, and help desk support. Many MSPs also host or provide software platforms on behalf of the contractor, including email services such as Microsoft Exchange or hosted Exchange environments, file collaboration platforms, line-of-business application hosting, and enterprise resource planning (ERP) systems. In many engagements, the MSP functions as a Software-as-a-Service (SaaS) provider, delivering hosted applications that the contractor's workforce relies on daily to perform the contract. An MSSP extends the managed services model into the cybersecurity domain by providing services such as security information and event management (SIEM), intrusion detection and response, vulnerability scanning, and security operations center (SOC) monitoring.

Under 32 CFR Part 170, these providers are classified as External Service Providers (ESPs). The regulation defines an ESP as "external people, technology, or facilities that an organization utilizes for the provision and management of IT and/or cybersecurity services on behalf of the organization." The CMMC program applies an additional qualification: to be considered an ESP within the assessment scope, Controlled Unclassified Information (CUI) or Security Protection Data (SPD), such as log or configuration data, must be processed, stored, or transmitted on the ESP's assets.

1.1 Why Providers That Do Not See CUI Remain in Scope

A common misconception among both contractors and their service providers is that an MSP falls outside the CMMC assessment boundary if it does not directly handle CUI. This interpretation is incorrect because it is rooted in the concept of Security Protection Data (SPD). When an MSP deploys a Remote Monitoring and Management (RMM) tool on a contractor's endpoints, that tool collects configuration data, system logs, patch status information, and in many cases, authentication credentials. None of this data is CUI in the traditional sense. It is not a technical drawing, a controlled specification, or an export-controlled document. It is, however, SPD, and the presence of SPD on the MSP's infrastructure is what brings that provider into the CMMC assessment scope.

The logic is straightforward but important to articulate clearly: the MSP provides the security barrier protecting the contractor's CUI environment. If that barrier is compromised, the CUI is exposed. The DOD does not draw a distinction between a provider that touches CUI directly and a provider whose tools and infrastructure constitute the defensive perimeter around CUI. Both are in scope. The CMMC Level 2 Scoping Guide reinforces this position by classifying ESP tools and services as Security Protection Assets (SPAs) that "provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI."

The practical result is that a contractor's CMMC certification depends, in part, on the compliance posture of every ESP whose tools or services interact with the contractor's assessment boundary. This dependency is not theoretical. During a C3PAO assessment, the assessment team will examine ESP documentation, evaluate Customer Responsibility Matrices, and may extend the assessment to include a review of ESP-controlled assets. If the ESP cannot demonstrate conformance with the applicable NIST SP 800-171 requirements, the contractor's assessment outcome is directly affected.

2. Regulatory Foundation: 32 CFR Part 170 and the Phase 1 Rollout

The regulatory basis for the CMMC program is 32 CFR Part 170, published as a final rule in the Federal Register on October 15, 2024. The rule establishes the CMMC model, defines assessment levels and methodologies, codifies the roles of ecosystem participants, and sets the requirements for contractor self-assessments and third-party certification assessments. The rule became effective upon publication, and the phased implementation began with Phase 1 on November 10, 2025. Under Phase 1, contracting officers are required to include CMMC Level 1 and Level 2 self-assessment requirements in applicable solicitations and contracts. At the DOD's discretion, C3PAO-assessed Level 2 certification may also be required during Phase 1. Phase 2, scheduled for November 10, 2026, will formally require C3PAO-assessed Level 2 certification in applicable solicitations and contracts.

2.1 The ESP and CSP Distinction Under DFARS 252.204-7012

A critical regulatory distinction exists between an External Service Provider and a Cloud Service Provider under the CMMC framework, and this distinction carries different compliance obligations. DFARS 252.204-7012, the clause governing the safeguarding of Covered Defense Information and cyber incident reporting, requires that any cloud service provider used to process, store, or transmit CUI must meet security requirements equivalent to the FedRAMP Moderate baseline. This requirement has been in effect since 2017, though the definition of "equivalent" remained ambiguous until the DOD issued clarifying guidance in late 2023.

Under 32 CFR Part 170, a Cloud Service Provider (CSP) is defined according to NIST SP 800-145: a provider of cloud computing services (Software as a Service, Platform as a Service, or Infrastructure as a Service) exhibiting five essential characteristics, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. An ESP, by contrast, is a broader category that includes any external provider of IT or cybersecurity services. All CSPs are ESPs, but not all ESPs are CSPs. This distinction matters because the FedRAMP Moderate equivalency requirement under DFARS 252.204-7012 applies specifically to CSPs. A non-CSP ESP, such as a traditional MSP that provides on-premises network management, is not subject to FedRAMP requirements but is subject to CMMC requirements when its assets process, store, or transmit CUI or SPD.

The regulatory consequence is that contractors must perform a classification analysis for each external provider. If the provider delivers cloud-based services meeting the NIST SP 800-145 definition, FedRAMP Moderate authorization or equivalency is required. If the provider delivers non-cloud IT or cybersecurity services and its assets process, store,

or transmit CUI or SPD, the provider falls within the CMMC assessment scope as an ESP. In either case, the contractor is responsible for ensuring that the provider's compliance posture is adequate and documented.

3. The Security Protection Asset Logic

Understanding the Security Protection Asset (SPA) classification is essential to grasping why ESP infrastructure falls within the CMMC assessment boundary. Under the CMMC Level 2 Scoping Guide and 32 CFR § 170.19(c)(1), Table 3, the assessment scope for Level 2 is organized into five asset categories: CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets. Each category carries different assessment requirements, but the critical point for this analysis is the SPA category.

Security Protection Assets are defined as assets that provide security functions or capabilities within the contractor's CMMC Assessment Scope, regardless of whether those assets process, store, or transmit CUI. The DOD Scoping Guide provides the following example: an ESP that provides a SIEM service may be logically separated from the CUI environment and may never directly process CUI, but the SIEM contributes to meeting the CMMC requirements within the contractor's assessment scope. As a result, that SIEM service and the ESP infrastructure supporting it are classified as Security Protection Assets and are subject to assessment against applicable CMMC practices.

3.1 How MSP Tooling Creates Scope Inclusion

The tools that MSPs deploy to manage contractor environments are the mechanism by which ESP infrastructure enters the CMMC assessment boundary. Consider the typical MSP engagement. The provider deploys an RMM agent on every managed endpoint and server. That agent reports system health, patch compliance, and security events to a centralized management console hosted on the MSP's infrastructure. The MSP may also deploy a Professional Services Automation (PSA) platform to track service tickets, some of which may include information on system configurations, user access issues, or incident details. The MSP's backup solution captures and stores copies of contractor data, which may include CUI. The MSP's identity management tools control user access to the contractor's systems. Furthermore, many MSPs host software platforms that contractors use for day-to-day operations, including email servers such as Exchange, file collaboration services, hosted databases, and line-of-business applications. When these hosted platforms process, store, or transmit CUI, the MSP is no longer operating solely as a Security Protection Asset provider. The MSP is operating as a CUI Asset provider, and potentially as a Cloud Service Provider subject to the FedRAMP Moderate equivalency requirements under DFARS 252.204-7012. This dual role is where the scoping analysis becomes particularly consequential.

Each of these tools processes or stores Security Protection Data. The RMM console holds configuration data. The PSA platform holds incident records. The backup system holds data copies. The identity management system holds authentication credentials

and access policies. Hosted software platforms, such as email servers, may process and store CUI directly. Under the CMMC scoping framework, every one of these tools is either a Security Protection Asset or a CUI Asset, and the ESP infrastructure supporting them is within the assessment boundary. The data flowing through these tools, the configuration settings, the log files, the access credentials, the email messages, and the stored documents constitute either Security Protection Data or CUI, depending on their nature. When the MSP's hosted platforms contain CUI itself, the scoping classification elevates from Security Protection Asset to CUI Asset, and the compliance obligations increase accordingly.

In practice, this means that the MSP's internal infrastructure, management consoles, data centers, employee access controls, and cybersecurity posture all become relevant to the contractor's CMMC assessment. If the MSP cannot demonstrate that its systems meet the applicable NIST SP 800-171 requirements, the contractor cannot claim that its own security controls are adequate, because the MSP is providing some of those controls on the contractor's behalf.

4. FedRAMP Equivalency and the December 2023 DOD Memorandum

For contractors that use cloud-based services to process, store, or transmit CUI, the DOD FedRAMP Equivalency Memorandum, dated December 21, 2023, establishes the evidentiary standard that Cloud Service Providers must meet. DFARS 252.204-7012 has required FedRAMP Moderate equivalency for cloud services hosting Covered Defense Information since 2017. However, the term "equivalent" was undefined until the DOD issued its December 2023 memorandum. Prior to this clarification, many CSPs made unsubstantiated claims about their compliance posture. Some asserted equivalency based on adherence to NIST SP 800-171, which covers only approximately 60 percent of the NIST SP 800-53 Moderate baseline required by FedRAMP. Others claimed equivalency by hosting their services on FedRAMP-authorized infrastructure, such as AWS GovCloud or Microsoft Azure Government, without demonstrating that their own service offerings met the FedRAMP Moderate controls.

4.1 The Evidentiary Requirements

The DOD memorandum eliminated ambiguity by establishing a specific set of requirements for CSPs claiming FedRAMP Moderate equivalency. To be considered equivalent, a Cloud Service Offering must achieve 100 percent compliance with the current FedRAMP Moderate security control baseline through an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization (3PAO). The memorandum does not permit self-attestation. The memorandum does not accept internal audits. The memorandum does not accept assessments performed by non-recognized organizations.

The memorandum requires the CSP to produce and present the following body of evidence to the contractor and to the DOD for review: a System Security Plan (SSP) documenting the implementation of all FedRAMP Moderate baseline security controls; a Security Assessment Plan (SAP) documenting the assessment methodology and scope; a Security Assessment Report (SAR) prepared by a FedRAMP-recognized 3PAO with detailed findings, scan results, and penetration test results; and a Plan of Action and Milestones (POA&M) documenting any controls not fully implemented, with the requirement that all POA&M items must be fully closed before equivalency is recognized.

This last requirement is particularly significant. Under standard FedRAMP authorization, an agency Authorizing Official may grant an Authority to Operate even with open POA&M items, accepting residual risk through an informed decision. The DOD equivalency standard does not allow this flexibility. The memorandum requires

100 percent compliance, with zero open findings from the 3PAO assessment. This is, in practical terms, a higher bar than standard FedRAMP authorization for many CSPs.

4.2 GRC Platforms as Cloud Service Providers

One category of cloud-based tools frequently overlooked in FedRAMP analysis is the Governance, Risk, and Compliance (GRC) platform. Many contractors adopt cloud-hosted GRC tools to manage their CMMC compliance program, including their System Security Plan (SSP), Plan of Action and Milestones (POA&M), evidence of control implementation, and assessment artifacts. These platforms are marketed as compliance enablement tools, and contractors understandably view them as part of the solution rather than part of the compliance problem. That perception does not align with the regulatory framework. A GRC platform that processes, stores, or transmits Covered Defense Information (CDI) is a Cloud Service Provider, and DFARS 252.204-7012 requires that any CSP handling CDI meet security requirements equivalent to the FedRAMP Moderate baseline. CDI, as defined in DFARS 252.204-7012, includes CUI and any other information that requires safeguarding or dissemination controls pursuant to law, regulation, or government-wide policy. The analysis that follows demonstrates why the data residing in a GRC platform used for CMMC Level 2 compliance almost certainly meets that definition.

The most direct basis for this classification is the evidence artifacts that GRC platforms are specifically designed to collect and retain. To demonstrate compliance with the 110 NIST SP 800-171 Revision 2 security requirements and their 320 assessment objectives, contractors must produce verifiable evidence of control implementation. In practice, this evidence frequently includes screenshots of CUI-handling systems with actual CUI visible on screen, Active Directory and group policy exports showing which personnel have access to CUI repositories, configuration exports from firewalls, endpoints, and servers within the CUI boundary, vulnerability scan results identifying specific weaknesses in CUI-processing systems, penetration test findings documenting exploitable paths to CUI data stores, and audit log samples from systems that process or transmit CUI. Each of these evidence types either contains CUI directly or contains information that would enable an adversary to identify and exploit the contractor's CUI environment. When this evidence is uploaded to a cloud-hosted GRC platform, the platform stores CDI. The FedRAMP Moderate equivalency requirement attaches at that point, regardless of how the GRC vendor characterizes its service.

The System Security Plan itself reinforces this conclusion. The SSP for a CMMC Level 2 environment is not a generic policy document. It is a detailed technical description of the contractor's security architecture, including network topology diagrams with IP addressing, hardware and software asset inventories for every in-scope system, data flow diagrams showing how CUI enters, moves through, and exits the environment,

identification of every user role with CUI access, and the specific implementation details for each of the 110 security requirements. The DOD has recognized the sensitivity of this information. Contractors subject to DFARS 252.204-7019 are required to report their NIST SP 800-171 assessment results through SPRS, a controlled government system, precisely because the details of a contractor's security posture are sensitive. An SSP that describes in granular detail how a contractor protects CUI, including which controls are fully implemented and which are not, constitutes information that requires safeguarding. Disclosing an SSP to an unauthorized party would provide a roadmap for compromising the contractor's CUI environment. Treating the SSP as something other than CDI requires ignoring the operational reality of what the document contains.

Even under the most generous interpretation, in which a contractor argues that neither its evidence artifacts nor its SSP constitutes CUI, the data stored in a GRC platform still falls within the CMMC scope as Security Protection Data (SPD). Under 32 CFR § 170.19 and the CMMC Level 2 Scoping Guide, SPD is defined as data stored or processed by Security Protection Assets to protect an assessed environment. SPD is security-relevant information that, if disclosed, could aid an adversary in compromising the system. Vulnerability scan outputs, configuration baselines, access control matrices, incident response procedures, and security architecture diagrams all meet this definition. A cloud-based platform that processes SPD is, at a minimum, an External Service Provider whose assets are within the contractor's CMMC assessment scope as Security Protection Assets. If the platform meets the NIST SP 800-145 definition of cloud computing, which virtually all modern SaaS GRC tools do, it is a CSP processing SPD. Under the scoping requirements of 32 CFR § 170.19(c)(2)(i), a CSP processing SPD must meet FedRAMP Moderate equivalency requirements. The result is the same whether the analysis proceeds under the CUI classification or the SPD classification: the GRC platform requires FedRAMP Moderate authorization or equivalency.

A GRC vendor's claim that its platform is "built on AWS" or "hosted in Azure Government" does not satisfy this requirement. The underlying infrastructure may hold FedRAMP authorization, but the application layer, the vendor's proprietary code, the vendor's access controls, the vendor's employee screening practices, the vendor's data handling and retention policies, must independently meet the FedRAMP Moderate baseline. FedRAMP authorization is granted to a specific Cloud Service Offering, not to every application that runs on an authorized infrastructure. A GRC application hosted on AWS GovCloud inherits certain physical and infrastructure controls from AWS, but application-level controls, access management, encryption implementation, audit logging, and incident response capabilities remain the responsibility of the GRC vendor. Without an independent FedRAMP authorization or a 3PAO-assessed equivalency determination for the GRC application itself, the contractor cannot rely on the platform to meet its DFARS 252.204-7012 obligations. Contractors that store their SSP,

assessment artifacts, and compliance evidence in a non-FedRAMP cloud environment are introducing a compliance gap that a C3PAO assessment team will identify, and that gap will be reflected in the contractor's assessment outcome.

4.3 The Contractor's Obligation

A critical dimension of the FedRAMP Equivalency Memorandum is the allocation of verification responsibility. The memorandum places the burden of verifying CSP compliance on the contractor, not on the CSP or the DOD. The contractor is responsible for obtaining and reviewing the CSP's body of evidence. The contractor is responsible for ensuring that the CSP has an incident response plan, follows that plan, and can notify the contractor following a cyber incident. The contractor, not the CSP, is responsible for reporting cloud-related incidents to the DOD in accordance with DFARS 252.204-7012 paragraphs (c) through (g).

During a CMMC Level 2 certification assessment, the C3PAO assessment team will evaluate whether the contractor's cloud environment meets the FedRAMP Moderate equivalency standard as defined by the December 2023 memorandum. The assessment team will review the CSP's body of evidence. If the contractor cannot produce adequate documentation, or if the documentation reveals gaps in the CSP's compliance posture, the contractor's assessment outcome is directly affected. Vendor marketing materials and general claims of "government-grade security" are not acceptable evidence.

5. The Responsibility Matrix: From Shared Responsibility to Formal Documentation

The concept of shared responsibility is familiar to most IT professionals, but the CMMC program demands a more specific and rigorous approach than the informal shared-responsibility models that have historically governed MSP and contractor relationships. In a traditional MSP engagement, the division of labor is typically described in a Master Services Agreement (MSA) or Statement of Work (SOW). The MSP manages the infrastructure; the contractor manages the data. The MSP handles patching; the contractor handles user training. These divisions are often described in general terms and may not map directly to specific security controls.

5.1 What Is a Customer Responsibility Matrix

A Customer Responsibility Matrix (CRM) is a formal document that maps each applicable security control to the party responsible for its implementation and maintenance. In the context of CMMC Level 2, the CRM maps each of the 110 NIST SP 800-171 Revision 2 security requirements to one of three designations: the control is implemented and maintained by the ESP, the control is implemented and maintained by the contractor, or the control is implemented through a shared arrangement where both parties have defined responsibilities. For shared controls, the CRM must specify which aspect of the control each party owns.

The CRM is not an optional supplement. 32 CFR § 170.19(c)(2)(ii) requires that the use of an ESP, its relationship to the contractor, and the services provided be documented in the contractor's SSP and described in the ESP's service description and Customer Responsibility Matrix. The CRM outlines the responsibilities of the contractor and the ESP regarding the services provided. During a C3PAO assessment, the assessment team will examine the CRM to determine whether each control has been assigned to a responsible party, whether the responsible party has actually implemented the control, and whether evidence supports the implementation claim.

5.2 Anatomy of a Customer Responsibility Matrix

To illustrate the structure and function of a CRM, the following table provides a representative sample of how control responsibilities might be allocated between a contractor and an ESP for selected NIST SP 800-171 Revision 2 requirements. This is not an exhaustive mapping but rather a demonstration of the required level of specificity.

Control ID	Control Title	Responsibility	Implementation Detail

AC.L2-3.1.1	Authorized Access Control	Shared	ESP manages Active Directory and MFA infrastructure. Contractor defines user access policies and approves provisioning requests.
AU.L2-3.3.1	System Auditing	ESP	ESP configures, collects, and retains audit logs through its SIEM service. Contractor reviews summary reports.
AT.L2-3.2.1	Role-Based Awareness	Contractor	Contractor develops and delivers security awareness training to all users with access to CUI systems.
IR.L2-3.6.1	Incident Handling	Shared	ESP provides initial detection and escalation through SOC monitoring. Contractor maintains incident response plan and coordinates DOD reporting.
SC.L2-3.13.11	CUI Encryption	Shared	ESP configures FIPS-validated encryption on managed endpoints. Contractor ensures encryption is enabled on all portable devices.

Table 1: Representative Customer Responsibility Matrix Allocation (Illustrative)

The transition from an informal, shared-responsibility understanding to a formal, control-level CRM is one of the most operationally significant requirements of the CMMC program for contractors that rely on ESPs. The CRM must be current, accurate, and supported by evidence. If the CRM assigns a control to the ESP and the ESP cannot produce evidence of implementation, the control is scored as not met in the contractor's assessment.

6. The ESP Certification Question

One of the most consequential changes between the proposed CMMC rule and the final rule published in October 2024 was the treatment of ESP certification. In earlier versions of the proposed rule, ESPs, such as MSPs, were required to obtain their own CMMC certification. The final rule removed this mandatory requirement. Under 32 CFR Part 170, ESPs are not required to obtain their own CMMC certification. This change was welcomed by many MSPs and their contractor clients, but its practical implications are more nuanced than the headline suggests.

The removal of mandatory ESP certification did not remove the ESP from the contractor's assessment scope. The final rule states that services provided by an ESP are within the contractor's assessment scope and shall be included in the contractor's assessment. If the ESP handles CUI, the ESP's assets shall be assessed as CUI Assets. If the ESP is involved in protecting CUI without directly handling it, the ESP's assets shall be assessed as Security Protection Assets. In either case, the C3PAO assessment team will evaluate the ESP's compliance posture as part of the contractor's assessment.

The regulation does note that an ESP may voluntarily undergo a CMMC certification assessment to reduce the effort required during the contractor's assessment. An ESP that holds its own CMMC Level 2 certification provides the contractor with a significant advantage: the C3PAO assessment team can accept the ESP's existing certification rather than conducting a separate evaluation of the ESP's assets during the contractor's assessment. This reduces assessment duration, reduces assessment cost, and reduces the risk that ESP deficiencies will delay or prevent the contractor's certification.

The strategic calculation for contractors is therefore as follows: selecting an ESP that has independently achieved CMMC certification simplifies the contractor's own certification path. Selecting an ESP that has not achieved certification means the contractor accepts the operational risk that the ESP's assets will be assessed during the contractor's own assessment, and any ESP deficiencies could result in findings against the contractor. The ESP's compliance posture is, in effect, an extension of the contractor's compliance posture.

7. Business Impact: The Affirmation, SPRS, and False Claims Act Exposure

The business consequences of ESP compliance gaps extend beyond assessment outcomes to personal executive liability and federal enforcement. Under 32 CFR § 170.22, every contractor participating in the CMMC program must designate an Affirming Official, a senior-level executive who submits an annual affirmation in the Supplier Performance Risk System (SPRS) attesting that the organization "has implemented and will maintain implementation of all applicable CMMC security requirements." This affirmation is required upon achieving CMMC status, annually thereafter, and at Plan of Action and Milestones closeout.

The affirmation is not a general statement of intent. It is a specific, recorded attestation tied to a CMMC Unique Identifier (UID) and a specific SPRS score. Contracting officers are required to verify SPRS assessment scores before making contract awards, exercising options, or extending periods of performance. A contractor without a current and validated SPRS entry may be deemed ineligible for new contracts, and existing awards may be delayed or suspended pending verification of compliance.

7.1 The False Claims Act Connection

The legal theory connecting SPRS affirmations to False Claims Act (FCA) liability is direct and well-established. When a contractor affirms compliance with CMMC requirements as a condition of contract eligibility, and that affirmation is false, the contractor has submitted a false claim or made a false statement material to a false claim under 31 U.S.C. § 3729. The FCA does not require specific intent to defraud. Under 31 U.S.C. § 3729(b)(1), "knowingly" includes actual knowledge, deliberate ignorance of the truth or falsity of information, or reckless disregard of the truth or falsity of information.

The Department of Justice has demonstrated that this enforcement theory is not hypothetical. In 2025, the DOJ settled seven cybersecurity-related FCA cases. These settlements included an $11.25 million resolution with a managed care provider for false cybersecurity certifications on a TRICARE contract, a $4.6 million settlement with a defense contractor for submitting a false SPRS score, and an $875,000 settlement with a university research institution for submitting a false SPRS score and failing to implement required security controls on systems handling CUI. In December 2025, the DOJ announced its first settlement targeting the defense supply chain, a qui tam action brought by a former employee against a precision machining subcontractor.

7.2 How ESP Deficiencies Create Affirmation Risk

The connection between ESP compliance and executive affirmation risk is the central business concern addressed in this paper. When an Affirming Official signs the SPRS affirmation, that official is attesting to the compliance of the entire system boundary, including all in-scope ESP assets. If the contractor's SSP documents an ESP as providing specific security controls through the CRM, and the ESP has not actually implemented those controls, the contractor's SPRS score does not accurately reflect its compliance posture. The affirmation, in that scenario, contains a misrepresentation.

The Affirming Official may not have direct visibility into the ESP's actual implementation of controls. This is precisely the risk. The regulation requires that the contractor verify ESP compliance, not merely accept the ESP's representations. If the contractor relies on an ESP's assurance that it meets CMMC requirements, and a subsequent C3PAO assessment or government investigation reveals that the ESP does not, in fact, meet those requirements, the contractor and its Affirming Official face FCA exposure. The qui tam provisions of the FCA create additional risk, as whistleblowers who report violations are entitled to between 15 percent and 25 percent of any recovery. IT staff, compliance officers, and security personnel at both the contractor and the ESP are well-positioned to identify gaps between stated affirmations and reality.

8. Practical Readiness: Questions for Contractor Leadership

The preceding analysis identifies a set of practical questions that contractor leadership should be prepared to answer before entering the CMMC assessment process. These questions are not theoretical. They represent the information a C3PAO assessment team will seek and the areas where ESP deficiencies most commonly lead to assessment findings.

Area of Inquiry	Question for Leadership
ESP Classification	Has each external provider been classified as a CSP, a non-CSP ESP, or out of scope, with supporting documentation for each classification?
CRM Availability	Does the organization possess a current Customer Responsibility Matrix from each in-scope ESP that maps responsibilities at the individual control level?
FedRAMP Compliance	For each CSP hosting CUI, can the organization produce a current SSP, SAP, SAR from a FedRAMP-recognized 3PAO, and closed POA&M documentation?
ESP Certification Status	Has the ESP independently achieved CMMC certification, or will the ESP's assets need to be assessed during the contractor's own assessment?
Evidence Availability	Can the ESP produce evidence of implementation for every control assigned to it in the CRM, in a format acceptable to a C3PAO assessment team?
Contractual Protections	Do current service agreements include provisions requiring the ESP to maintain CMMC-aligned security practices, cooperate with assessments, and notify the contractor of material changes?
Incident Reporting	Is the ESP contractually obligated to notify the contractor of incidents in timeframes that support the contractor's 72-hour DOD reporting obligation under DFARS 252.204-7012?

Table 2: Pre-Assessment Readiness Questions for ESP Compliance

9. Conclusion: The Paradox Resolved

The paradox at the center of this paper is that the organizations' contractors hire to improve their cybersecurity posture may be the organizations that prevent them from achieving CMMC certification. This paradox is resolved not by avoiding ESPs, which is operationally impractical for most DIB contractors, but by approaching ESP selection and management as a compliance function rather than a procurement function.

The regulatory framework is clear. 32 CFR Part 170 places ESP assets within the contractor's assessment scope. The CMMC Scoping Guide classifies ESP tools and infrastructure as Security Protection Assets subject to assessment. The FedRAMP Equivalency Memorandum establishes specific evidentiary requirements for cloud service providers. The affirmation requirement under 32 CFR § 170.22 imposes personal executive accountability for the accuracy of the contractor's reported compliance posture, including that of its ESPs.

The path forward for contractor leadership requires three actions. First, perform a thorough classification of all external providers against the ESP and CSP definitions in 32 CFR Part 170 and DFARS 252.204-7012. Second, obtain and validate formal Customer Responsibility Matrices from every in-scope ESP, ensuring that each of the 110 NIST SP 800-171 Revision 2 requirements is assigned to a responsible party and supported by verifiable evidence. Third, evaluate the business risk of relying on ESPs that have not independently achieved CMMC certification, recognizing that uncertified ESP assets will be assessed during the contractor's own C3PAO assessment and that any ESP deficiencies will become the contractor's.

The 2026 CMMC landscape does not allow contractors to treat their service provider relationships as outside the compliance boundary. The DOD has made clear, through regulations, memoranda, and enforcement actions, that a contractor's eligibility for defense awards is directly and measurably tied to the compliance posture of its Managed Service Providers and External Service Providers. Contractors who internalize this reality and act on it will be positioned for successful certification. Those who do not will find that the providers they trusted to protect them have become the obstacle to the contracts they need.

References

1. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Federal Register, Vol. 89, No. 199 (October 15, 2024).

2. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

3. Department of Defense Chief Information Officer, "Federal Risk and Authorization Management Program (FedRAMP) Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings." Memorandum dated December 21, 2023.

4. Department of Defense Chief Information Officer, CMMC Level 2 Scoping Guide.

5. NIST Special Publication 800-171 Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

6. NIST Special Publication 800-145, "The NIST Definition of Cloud Computing."

7. CMMC Assessment Process (CAP) Guide, Version 2.0. CyberAB.

8. 48 CFR (DFARS), CMMC Acquisition Clauses. Federal Register (September 2025), effective November 10, 2025.

9. 31 U.S.C. § 3729, False Claims Act.

10. 32 CFR § 170.22, Affirmation Requirements.

About the Author

David W. Koran is a CMMC Registered Practitioner with over 30 years of experience in information technology and cybersecurity. He is the founder and principal consultant of a CMMC compliance consulting practice serving Defense Industrial Base contractors and their legal counsel. His practice focuses on CMMC readiness, enablement, and implementation for organizations navigating Level 2 certification requirements. He is an Associate Member of the American Bar Association Section of Public Contract Law.

Contact: dkoran@davidkoran.com