POSITION PAPER

Against the Practice of MSP/MSSP using non-FedRAMP services in support of CMMC Organizations Seeking Assessment (OSA)

April 2026

Executive Overview

Managed Service Providers and Managed Security Service Providers routinely operate multi-tenant platforms on behalf of defense contractors undergoing CMMC Level 2 assessment. These platforms — help desks, RMM tools, SIEM/SOC dashboards, ticketing systems, managed EDR consoles, backup management portals, and others — frequently provide operational or administrative access to endpoints, networks, or data stores containing Controlled Unclassified Information. This access exists by design through the service's functional capabilities, regardless of policies restricting CUI handling within the platform.

When these platforms are multi-tenant and provider-controlled, the Organization Seeking Assessment cannot implement CMMC controls within them. Frequently, the platform is hosted on FedRAMP-authorized infrastructure, but that authorization covers the infrastructure provider's boundary — not the MSP-operated application layer where CUI exposure occurs. The result is a CUI-capable service with no entity demonstrably responsible for application-layer controls.

This paper derives a conclusion from existing federal standards that resolves this ambiguity. NIST SP 800-145 defines cloud computing by architectural characteristics — not by provider self-classification. Multi-tenant, network-delivered, provider-managed SaaS platforms satisfy this definition regardless of whether the operator identifies as an MSP, MSSP, or CSP. DFARS 252.204-7012 requires cloud computing services handling CUI to meet FedRAMP Moderate equivalency. This obligation attaches to the service delivery model, not the provider's label.

An MSP operating a CUI-capable multi-tenant SaaS platform is functioning as a Cloud Service Provider for that service and is subject to FedRAMP equivalency as a contractual requirement. The paper provides a framework for Registered Practitioner Organizations and CMMC Third-Party Assessment Organizations to evaluate MSP/MSSP service delivery models, determine when CSP classification applies, and assess treatment adequacy within OSA environments.

BLUF: Logical Framework

Axioms (established by CMMC scoping guidance, NIST, and DFARS):

A1. A service that is *capable* of accessing CUI requires treatment, regardless of whether access is *intended*. (Section 2)

A2. Policy prohibiting CUI handling does not remove technical capability to access CUI. (Section 2.1)

A3. The entity that controls a service architecture is the entity responsible for implementing controls within it. (Section 3)

A4. An OSA cannot implement controls within a multi-tenant platform it does not control. (Section 3.1)

A5. Inherited infrastructure compliance (e.g., FedRAMP IaaS) does not extend to application-layer controls implemented independently by a third party. (Section 4.2)

A6. A Shared Responsibility Model requires attestation under a recognized framework to be authoritative for scoping decisions. (Section 3.2)

A7. NIST SP 800-145 defines cloud computing by service delivery characteristics, not by provider self-classification. (Section 5)

A8. DFARS 252.204-7012 requires cloud services used to store, process, or transmit CUI to meet FedRAMP Moderate equivalent. (Section 5.2)

Determinations (derived from axioms):

D1. MSP/MSSP-operated platforms that provide administrative, operational, or investigative access to systems, networks, or data stores containing CUI are *capable* of accessing CUI by design. [A1, A2] (Section 2)

D2. When such platforms are multi-tenant and provider-controlled, the OSA cannot treat them directly. [A3, A4] (Section 3.1)

D3. Hosting a multi-tenant application on FedRAMP-authorized infrastructure does not constitute treatment of the application layer. [A5] (Section 4.2)

D4. Exclusion of such a platform from the OSA boundary requires provider-implemented controls supported by attested compliance. [A4, A6] (Section 3.2)

D5. A multi-tenant MSP/MSSP platform capable of accessing CUI that lacks attested treatment cannot be defensibly descoped. [D2, D3, D4] (Section 4)

D6. A multi-tenant, network-delivered, provider-managed SaaS platform meets the NIST SP 800-145 definition of cloud computing regardless of provider self-classification. [A7] (Section 5)

D7. An MSP/MSSP operating such a platform is functioning as a Cloud Service Provider for that service. [D6] (Section 5.1)

D8. When that service is capable of accessing CUI, DFARS 252.204-7012 requires FedRAMP Moderate equivalency. [D1, D7, A8] (Section 5.2)

Conclusions:

C1. MSP/MSSP-operated multi-tenant platforms capable of accessing CUI must be treated through one of: (a) provider-attested full-stack controls with FedRAMP or equivalent authorization, (b)

dedicated deployment under OSA control, or (c) provider assessment as an ESP under CMMC. Absent one of these, the platform remains within the CUI protection boundary. [D1–D5] (Section 6.1)

C2. Because such platforms constitute cloud computing by NIST definition, FedRAMP Moderate equivalency is not a best practice but a contractual requirement under DFARS 252.204-7012. The question is not whether treatment is needed, but whether an existing obligation is being enforced. [D6–D8] (Section 6.2)

1. Purpose

Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) deliver a broad range of operational and security services to Organizations Seeking Assessment (OSAs) under the CMMC framework. These services are commonly delivered through multi-tenant SaaS platforms that the provider operates across multiple clients: help desk and ticketing systems, Remote Monitoring and Management (RMM) tools, SIEM and SOC platforms, managed EDR consoles, backup and disaster recovery portals, identity management dashboards, vulnerability management platforms, and network monitoring systems.

When these platforms interact with environments containing Controlled Unclassified Information, questions arise regarding scoping, treatment, and responsibility boundaries. Current practice often classifies MSP/MSSP-delivered services as External Service Provider (ESP) relationships and evaluates treatment through Shared Responsibility Models of varying rigor. This paper examines whether that classification is consistently appropriate, or whether the service delivery architecture of many MSP/MSSP platforms triggers obligations that apply specifically to Cloud Service Providers.

This paper is intended for Registered Practitioner Organizations (RPOs) advising OSAs on scoping and architecture decisions, and for CMMC Third-Party Assessment Organizations (C3PAOs) making treatment determinations during assessment. It provides a framework for evaluating MSP/MSSP service delivery models against NIST definitions and DFARS requirements, and for determining when CSP classification — and its associated FedRAMP equivalency obligation — applies.

Throughout this paper, help desk and RMM platforms are used as representative examples. The principles apply to any MSP/MSSP-operated multi-tenant platform capable of accessing CUI.

2. Capability Determines Scope, Not Intent

2.1 The Capability Principle

CMMC Level 2 scoping is determined by whether systems store, process, transmit, or have access to CUI. The controlling factor is technical capability, not intended use or policy restriction.

MSP/MSSP platforms commonly provide one or more of the following capabilities against OSA environments:

- **Remote administrative access** to endpoints, servers, or network devices (RMM, help desk)
- **File transfer and artifact collection** from managed systems (RMM, backup, help desk)
- **Log and telemetry ingestion** from CUI-bearing systems (SIEM, EDR, monitoring)
- **Investigative access** including memory capture, process inspection, and command execution (EDR, SOC)
- **Configuration and policy management** over identity, access, or security controls (identity management, vulnerability management)
- **Screen viewing, clipboard interaction, and diagnostic capture** during support sessions (help desk, RMM)

Each of these capabilities enables access to CUI residing on managed systems, regardless of whether the platform is intended to store CUI within its own data layer. A policy prohibiting CUI submission through a ticketing system does not prevent a technician from viewing CUI on a user's screen. A policy restricting SIEM log content does not prevent CUI from appearing in application logs forwarded from a CUI-bearing system.

The distinction is between services that *do not* access CUI by policy and those that *cannot* access CUI by design. Services in the former category — where technical capability exists but is restricted only by procedural controls — are CUI-capable and require treatment. Services in the latter — such as monitoring tools that collect only abstracted metadata without access to user data or system content — may qualify as Security Protection Assets (SPA) generating Security Protection Data (SPD).

2.2 Illustrative Examples

Platform Type	CUI Access Mechanism	Commonly Recognized?
Managed EDR	File retrieval, memory capture, remote investigation on CUI endpoints	Yes — typically FedRAMP SaaS
Help Desk / RMM	Remote desktop, file transfer, screenshot capture, diagnostic collection	Often not — despite equivalent access
Managed SIEM / SOC	Log ingestion from CUI systems, alert investigation, incident response	Inconsistent
Backup / DR Portal	Full system image access, file-level restore from CUI systems	Inconsistent

Platform Type	CUI Access Mechanism	Commonly Recognized?
Identity Management	Policy authority over authentication and access to CUI systems	Inconsistent

The technical capability to access CUI is present across all of these service types. The inconsistency in treatment reflects assumptions about intended use rather than analysis of capability — a distinction this paper seeks to resolve.

3. The Multi-Tenant Provider Control Problem

3.1 OSA Cannot Treat What It Does Not Control

When an MSP/MSSP platform is multi-tenant and provider-operated, the OSA does not control tenant isolation, authentication architecture, logging infrastructure, data retention, administrative access, or personnel access. The OSA cannot independently implement CMMC controls within the platform and cannot reasonably bring the system into its own assessment boundary for direct treatment.

This distinguishes provider-operated tooling from contractor personnel operating within OSA-owned infrastructure. When external personnel use OSA-managed systems under OSA-defined access controls and logging, the OSA retains control and responsibility. When the MSP/MSSP provides and operates its own platform, responsibility for controls within that platform belongs to the provider.

3.2 Attestation Is Required, Not Optional

The only mechanism for excluding a CUI-capable, provider-controlled platform from the OSA boundary is reliance on a Shared Responsibility Model (SRM) provided by the service operator. For an SRM to be authoritative for scoping purposes, it must be supported by attestation under a recognized compliance framework. Without independent validation, an SRM is a self-asserted allocation of responsibility, not demonstrated implementation of controls.

The OSA cannot verify control implementation within a multi-tenant environment it does not control. Attestation — through FedRAMP authorization, CMMC assessment, or equivalent recognized framework — fills that gap. An unattested SRM from a provider operating a CUI-capable multi-tenant platform does not provide a defensible basis for scoping decisions.

4. Treatment Models

4.1 Provider-Implemented Full-Stack Treatment

The provider delivers a platform assessed and operated as a complete service capable of handling CUI. Controls are implemented across the full stack — application, infrastructure, administrative access, logging, data handling, and operations. The SRM is supported by independent attestation such as FedRAMP authorization. This is the standard model for EDR platforms serving CUI environments and represents complete, verifiable treatment.

4.2 Multi-Tenant Application on Treated Infrastructure (The Gap)

The underlying infrastructure may be FedRAMP-authorized, but the application layer is independently operated as a shared platform by the MSP/MSSP. This is the most common architecture for MSP-delivered services and introduces two problems:

Infrastructure inheritance does not cover the application layer. FedRAMP authorization applies to the infrastructure provider's boundary — compute, storage, networking, and provider-managed services. It does not extend to third-party applications deployed on that infrastructure. The mechanisms through which CUI is accessed — operator interaction, data ingestion, remote sessions, artifact collection — exist at the application and operator layers, outside the infrastructure authorization boundary.

An attestation gap results. The OSA cannot treat the application (no control). The infrastructure provider's authorization does not cover it. The MSP-operated application is typically not independently assessed. A CUI-capable platform exists with no entity demonstrably responsible for application-layer controls.

4.3 Dedicated Deployment Under OSA Control

The platform is deployed in a dedicated tenant or single-customer instance where the OSA retains authority over configuration, access, logging, and retention. MSP/MSSP personnel may operate the platform, but within an OSA-controlled environment — functioning as contractor support rather than an independent service operator. The OSA implements application-layer controls directly, with optional infrastructure inheritance from a compliant cloud provider.

4.4 Untreated Commercial SaaS

The platform operates as commercial SaaS without FedRAMP authorization, dedicated isolation, or CMMC-aligned treatment. Unlike the model in Section 4.2, which creates ambiguity through partial inheritance, this model is straightforwardly untreated and clearly unsuitable for CUI-capable services.

5. MSP/MSSP-Operated SaaS as Cloud Computing

5.1 NIST SP 800-145 Characteristic Analysis

NIST SP 800-145 defines cloud computing through five essential characteristics. The definition is characteristic-based — a service is cloud computing if it exhibits these properties, regardless of how the provider describes itself.

NIST 800-145 Characteristic	Typical MSP/MSSP Multi-Tenant SaaS Platform
On-demand self-service	Operators provision sessions, tickets, alerts, scans, or investigations without manual vendor intervention
Broad network access	Platform delivered over standard internet protocols, accessed via browser or client application
Resource pooling	Infrastructure and application resources shared across multiple customers in a multi-tenant architecture
Rapid elasticity	Capacity scales with customer count and usage without per-tenant infrastructure provisioning
Measured service	Usage metered by seat count, endpoint count, event volume, or storage consumption

Multi-tenant, network-delivered, provider-managed SaaS platforms — whether labeled as MSP tooling, MSSP services, or managed platforms — satisfy these characteristics. The provider's organizational identity does not alter the architectural reality. NIST SP 800-145 defines what cloud computing is, not what providers choose to call it.

An MSP/MSSP operating a platform that meets these characteristics is functioning as a Cloud Service Provider for that service, regardless of self-classification.

5.2 DFARS Consequence

DFARS 252.204-7012(b)(2)(ii) requires that cloud computing services used to store, process, or transmit Covered Defense Information meet security requirements equivalent to FedRAMP Moderate. This requirement attaches to the service delivery model, not to the provider's organizational label.

If an MSP/MSSP operates a multi-tenant SaaS platform that meets the NIST SP 800-145 definition of cloud computing, and that platform is capable of storing, processing, or transmitting CUI, then DFARS 252.204-7012 requires FedRAMP Moderate equivalency for that service. This is a contractual obligation flowing from the prime contract through DFARS clause flow-down — not an assessment recommendation or best practice.

The common practice of classifying MSP/MSSP-operated SaaS platforms as ESP services rather than cloud services does not withstand analysis against NIST SP 800-145. The DFARS obligation follows the architecture, not the label.

6. Position and Assessment Guidance

6.1 Acceptable Treatment Models

A multi-tenant MSP/MSSP platform capable of accessing CUI may be excluded from the OSA assessment boundary when treatment is implemented and attested:

- **Provider-attested full-stack SaaS** — controls at both infrastructure and application layers, supported by FedRAMP authorization or equivalent assessment demonstrating FedRAMP Moderate equivalency (Section 4.1)
- **Dedicated deployment under OSA control** — OSA implements application-layer controls directly, provider personnel operate within OSA-defined boundaries (Section 4.3)
- **Provider assessed as ESP under CMMC** — provider demonstrates implementation of controls governing CUI access through the service, supported by CMMC assessment

6.2 Non-Defensible Approaches

The following do not constitute adequate treatment:

- **Policy-only restriction** — prohibiting CUI handling does not prevent incidental access through the service's functional capabilities
- **Infrastructure inheritance alone** — FedRAMP IaaS authorization does not extend to MSP/MSSP-operated applications deployed on that infrastructure
- **Unattested provider assertions** — an SRM without independent assessment is self-certification, not verifiable treatment
- **ESP classification to avoid CSP obligations** — if the service meets NIST SP 800-145 cloud computing characteristics, classifying it as ESP does not remove the DFARS 252.204-7012 FedRAMP equivalency requirement

6.3 Assessment Framework

When evaluating MSP/MSSP-operated platforms during CMMC Level 2 assessment or advisory engagement, the following determination sequence applies:

Step 1 — Determine capability. Does the platform provide administrative, operational, or investigative access to systems, networks, or data stores containing CUI? If yes, the service is CUI-capable regardless of intended data flow.

Step 2 — Determine control ownership. Is the platform multi-tenant and provider-operated? If yes, the OSA cannot implement controls directly and the service requires provider-implemented treatment.

Step 3 — Determine service classification. Does the platform meet NIST SP 800-145 cloud computing characteristics (multi-tenant, network-delivered, provider-managed, resource-pooled, metered)? If yes, the service is cloud computing and DFARS 252.204-7012 FedRAMP Moderate equivalency applies.

Step 4 — Evaluate treatment. Request the SRM and supporting attestation. Does the attestation cover the application layer where CUI access occurs, or only underlying infrastructure? If only infrastructure, treatment is not demonstrated at the layer where exposure occurs.

Step 5 — Conclude. Where attested application-layer treatment exists and FedRAMP equivalency is demonstrated (or the service operates under an acceptable model from Section 6.1), the platform may be descoped from the OSA boundary. Where these conditions are not met, the platform remains within the CUI protection boundary.

6.4 RPO Advisory Implications

RPOs advising OSAs on architecture and scoping should evaluate the full inventory of MSP/MSSP-delivered services against this framework before assessment. Where services are identified as CUI-capable multi-tenant platforms meeting cloud computing characteristics, the RPO should advise the OSA that:

- The service likely constitutes cloud computing under NIST SP 800-145
- DFARS 252.204-7012 FedRAMP equivalency applies to the service
- The OSA should request attested SRMs from the provider or evaluate architectural alternatives (dedicated deployment, FedRAMP-authorized replacement, or provider CMMC assessment)
- Policy-only restrictions and infrastructure inheritance claims should be evaluated critically against the application-layer access mechanisms

Early identification of these conditions prevents scoping surprises during assessment and gives the OSA time to remediate architecture or negotiate provider compliance commitments.

6.5 Consistency Principle

Treatment expectations should be applied consistently across all CUI-capable multi-tenant services. EDR platforms are widely recognized as requiring FedRAMP-authorized deployment. Help desk, RMM, SIEM, backup, and identity management platforms with equivalent technical capability to access CUI should be evaluated under the same standard. The determining factor is the capability to access CUI and the service delivery architecture, not the service category or provider label.

7. Anticipated Objections and Responses

This section addresses foreseeable objections to the positions established in this paper, ranked by analytical strength. Each objection is stated in its strongest form, assessed for validity, and answered. The intent is not to dismiss legitimate concerns but to demonstrate that the core conclusions survive scrutiny and to identify where precision in application is warranted.

7.1 DFARS 7012 Cloud Computing Clause Does Not Reach MSP Tooling (Strong Objection)

Objection. DFARS 252.204-7012(b)(2)(ii) requires the contractor to use FedRAMP-equivalent cloud computing when storing, processing, or transmitting Covered Defense Information. The clause contemplates the contractor's direct procurement of cloud services — migrating email to GCC High, storing files in a FedRAMP-authorized platform. It does not contemplate a second-order relationship where the contractor's MSP independently selects and operates its own internal tooling. The contractor did not procure the MSP's platform as a cloud service; the MSP chose it as an operational tool. The DFARS cloud clause does not reach through to the MSP's architectural decisions.

Assessment. This is a structurally serious objection that challenges the mechanism by which Conclusion C2 operates. The text of 7012(b)(2)(ii) is directed at the contractor's use of cloud computing, and reasonable interpretation could limit "use" to direct procurement rather than indirect exposure through a service provider's tooling choices.

Response. The objection is correct that DFARS 7012's cloud clause is directed at the contractor. However, it does not follow that the contractor's obligations are satisfied by ignorance of the MSP's architecture. DFARS 7012(b)(1) requires the contractor to provide "adequate security" for all Covered Defense Information on all contractor information systems. When the contractor engages an MSP whose platform accesses CUI, the contractor must ensure adequate protection exists for that access — regardless of whether the cloud clause or the general safeguarding requirement is the operative mechanism.

Furthermore, DFARS flow-down requirements (252.204-7012(m)) require the contractor to include the substance of the clause in subcontracts where CDI performance is anticipated. If the MSP's service involves access to CUI, the contractor is obligated to flow down the safeguarding requirements. The MSP, as a subcontractor performing with access to CUI, then becomes subject to the same obligations — including the cloud computing clause for its own use of cloud services.

The precise mechanism may be flow-down rather than direct application, but the treatment outcome is identical: a multi-tenant platform capable of accessing CUI must meet FedRAMP equivalency when it constitutes cloud computing under the governing federal definition. The contractor cannot discharge its adequacy obligation by declining to examine the MSP's service delivery architecture.

7.2 Not All MSP Platforms Meet All Five NIST 800-145 Characteristics (Strong Objection)

Objection. The paper maps NIST SP 800-145 characteristics against MSP platforms generically, but not every MSP platform exhibits all five characteristics. A small MSP running a dedicated ConnectWise instance on a single server for ten clients does not demonstrate rapid elasticity or measured service in the NIST sense. The paper treats all multi-tenant MSP tooling as enterprise-scale SaaS, which overstates the applicability of the cloud computing classification.

Assessment. This is a legitimate narrowing objection. The NIST 800-145 definition requires all five essential characteristics, and some MSP platforms — particularly smaller-scale or less automated deployments — may not satisfy all five. Applying the CSP classification categorically to all MSP tooling would overstate the paper's conclusion.

Response. The paper's framework requires that the five-characteristic test be applied to each service individually, not categorically to all MSP platforms. Where a platform does not satisfy all five characteristics, the CSP classification and associated DFARS FedRAMP equivalency requirement (Conclusion C2) would not apply to that specific service.

However, this does not affect Conclusion C1. A multi-tenant MSP platform that is capable of accessing CUI but does not meet the cloud computing definition still requires attested treatment — the obligation derives from CUI capability and the OSA's inability to implement controls within a provider-controlled platform (Sections 2 through 4). The treatment requirement exists independently of the CSP classification. The CSP derivation elevates the obligation to a specific contractual requirement where applicable; its inapplicability to a particular platform does not remove the underlying treatment need.

In practice, the majority of commercially operated multi-tenant SaaS platforms used by MSPs at meaningful scale will satisfy all five characteristics. The objection correctly identifies edge cases that should be evaluated individually rather than assumed.

7.3 Capability-Based Scoping Is Overbroad (Moderate Objection)

Objection. If any service with administrative access to any system that touches CUI is CUI-capable, then virtually every MSP tool, vendor support portal, and SaaS admin console becomes in-scope. The result is unworkable, inconsistent with how CMMC assessments are actually conducted, and would make compliance prohibitively expensive for most defense contractors relying on MSP services.

Assessment. This is a practical objection rather than a logical one. It does not challenge whether the analysis is correct, but whether its consistent application produces manageable results.

Response. The paper establishes a specific distinction between services that cannot access CUI by design and those that do not access CUI by policy (Section 2.1). Services that collect only abstracted metadata, operate without access to user data or system content, and have no mechanism for retrieving, viewing, or interacting with CUI-bearing data are excluded under the design-based restriction. The scoping standard is not "any administrative access" but rather "access that enables exposure to CUI through the service's functional capabilities."

The scope is broad because the problem is broad. MSP-operated platforms routinely provide remote desktop access, file transfer, diagnostic collection, and endpoint interaction across client environments. When those environments contain CUI, the platforms are CUI-capable by the functional definition established in CMMC scoping guidance. That this creates compliance obligations for a large number of services reflects the actual scope of the issue, not an analytical error.

The alternative — narrowing scope based on intended use or policy restrictions — has the practical effect of excluding services from treatment based on assertions that cannot be enforced or verified within platforms the OSA does not control. Convenience of scope does not override accuracy of classification.

7.4 NIST SP 800-145 Is Definitional, Not a Compliance Test (Moderate Objection)

Objection. NIST SP 800-145 was published in 2011 as a general-purpose definitional document to establish common cloud computing terminology. It was not designed as a classification test for triggering DFARS

obligations or determining compliance requirements. Using it as a bright-line rule for CSP classification stretches the document beyond its intended purpose.

Assessment. This objection correctly characterizes 800-145's origin but does not account for how the definition operates within the regulatory framework.

Response. DFARS 252.204-7012 uses the term "cloud computing" without providing its own definition. When a regulation references a technical concept without defining it, the authoritative federal definition governs. NIST SP 800-145 is that definition — it is the standard referenced across federal cloud policy, FedRAMP guidance, and DoD cloud strategy. The document's purpose is precisely to provide the definition that other frameworks apply.

The objection amounts to arguing that the governing definition of cloud computing should not be used to determine what constitutes cloud computing. This is circular. If the DFARS clause applies to "cloud computing" and 800-145 defines "cloud computing," the definition governs regardless of whether 800-145 was originally written with DFARS in mind. Definitions do not require intent to be applied — they require accuracy.

7.5 The ESP Pathway Makes CSP Classification Unnecessary (Moderate Objection)

Objection. CMMC already provides for External Service Provider treatment. If the MSP obtains its own CMMC assessment as an ESP, controls are validated through a recognized framework. Reclassifying MSPs as CSPs adds FedRAMP overhead that duplicates the CMMC pathway and imposes unnecessary cost when the ESP model already achieves the same protective outcome.

Assessment. This objection is practical and partially valid. The paper acknowledges ESP assessment as an acceptable treatment model (Section 6.1).

Response. The ESP pathway and the CSP classification are not mutually exclusive — they address different aspects of the same problem. The ESP pathway provides a mechanism for the MSP to demonstrate implementation of controls. The CSP classification identifies a specific contractual obligation that exists when the service delivery model constitutes cloud computing.

Where an MSP's platform meets the NIST 800-145 definition, both obligations may apply simultaneously: the MSP is an ESP that is also operating as a CSP. In practice, an MSP that obtains CMMC assessment as an ESP delivering a platform that also meets FedRAMP Moderate equivalency satisfies both pathways. The CSP classification is not intended to replace the ESP model but to identify cases where FedRAMP equivalency is a contractual requirement rather than an optional treatment approach.

The distinction matters primarily when an MSP has neither FedRAMP authorization nor CMMC assessment. In that scenario, the CSP derivation establishes that the gap is not merely a best-practice shortfall but a failure to meet a contractual obligation — a materially different assessment finding.

7.6 Policy-Based Restrictions Combined with Contractual Obligations Are Accepted Practice (Weak Objection)

Objection. Every CMMC assessment accepts policy-based controls to some degree. Access control policies, acceptable use policies, data handling procedures, and personnel security requirements are all implemented through policy and accepted by assessors. Dismissing policy-based restrictions as insufficient for help desk scoping while accepting them everywhere else introduces an inconsistency.

Assessment. This objection conflates two distinct conditions: policy governing behavior within a controlled environment and policy governing behavior within a platform the OSA does not control.

Response. Policy-based controls are accepted within CMMC when the policy is implemented within an environment where the OSA can monitor compliance, enforce restrictions, and log violations. An acceptable use policy governing employee behavior on OSA-owned systems is enforceable because the OSA controls the logging, monitoring, and access mechanisms that detect and respond to violations.

A policy prohibiting CUI submission through an MSP-operated multi-tenant help desk platform is not enforceable by the OSA. The OSA does not control the platform's logging, cannot monitor technician behavior within the application, cannot restrict what data is collected during remote sessions, and cannot audit compliance with its own policy inside the provider's system. The policy exists in a vacuum — it restricts behavior within an environment where the restricting party has no enforcement capability.

This is not an inconsistency in the paper's analysis. It is a recognition that policy-based controls require an enforcement mechanism, and that enforcement mechanisms require control over the environment in which the policy operates. Where control is absent, policy alone is insufficient.

8. References

CMMC Program

- CMMC Model Overview, Version 2.0, U.S. Department of Defense
- CMMC Level 2 Assessment Guide, U.S. Department of Defense
- CMMC Scoping Guide for Level 2 Assessments, Cyber AB / DoD CIO

NIST Publications

- NIST SP 800-145, The NIST Definition of Cloud Computing
- NIST SP 800-171 Rev. 2, Protecting CUI in Nonfederal Systems and Organizations
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations

DoD Contractual Requirements

- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 252.204-7019/7020/7021, NIST SP 800-171 Assessment and CMMC Requirements

Cloud and External Service Requirements

- FedRAMP Authorization Act (FY23 NDAA, 44 U.S.C. §3607)
- FedRAMP Moderate Baseline Controls
- FedRAMP Boundary Guidance and Authorization Packages