MANAGED SERVICE PROVIDER COLLECTIVE

January 10, 2026

The Honorable Mike Rogers
Chairman, House Armed Services Committee
2216 Rayburn House Office Building
Washington, DC 20515

The Honorable Adam Smith
Ranking Member, House Armed Services Committee
2264 Rayburn Office Building
Washington, DC 20515

Subject: Regulatory Gaps Concerning Managed Service Providers and the Protection of Controlled Unclassified Information

Dear Chairman Rogers and Ranking Member Smith,

On behalf of Managed Service Providers for the Protection of Critical Infrastructure (the "MSP Collective"), we write to bring to your attention a significant gap in the Cybersecurity Maturity Model Certification (CMMC) regulatory framework that, unless addressed, will continue to create a blind spot and exploitable attack surface within the Defense Industrial Base (DIB). Our members support the Department of War's (DoW) objective to strengthen protection of Controlled Unclassified Information (CUI) and critical national security information, and we believe the issue described below is resolvable through targeted oversight and discrete regulatory and contractual updates.

A regulatory gap for MSPs with privileged access to CUI environments

DoW contractors and subcontractors subject to CMMC Level 2 requirements must implement the NIST SP 800-171 security framework to protect CUI. In practice, however, many of these contractors rely on managed service providers (MSPs) to deliver ongoing and regular support and active administration of networks, endpoints, identity systems, security tooling, monitoring, and incident response. MSPs are essential to lowering costs and accelerating time to compliance, particularly for small to medium sized businesses (SMBs). However, not all MSPs meet the security standards necessary to protect CUI. By the nature of these services, MSP personnel often possess privileged or administrative access to the very systems and networks that process, store, or transmit CUI, and can therefore materially affect (and potentially undermine) the security posture required for CMMC compliance.

Yet MSPs are not defined in 32 CFR Part 170, and current scoping constructs for External Service Providers (ESPs) do not clearly and consistently impose an obligation on MSPs commensurate with the CMMC level of the contractor they service. The regulatory text and associated definitions create ambiguity in how an Organization Seeking Assessment (OSA) can satisfy scoping and assessment requirements when the ESP is an MSP that is not itself certified at the applicable CMMC level.

For example, 32 CFR § 170.19(c)(2) provides that when an ESP that is not a Cloud Service Provider processes, stores, or transmits CUI, "the services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment," and further requires documentation in the OSA's System Security Plan (SSP), as well as an ESP service description and Customer Responsibility Matrix (CRM). The regulation also notes that an ESP "may voluntarily undergo a CMMC certification assessment" to reduce the effort required during the OSA's assessment. In the MSP context, this approach is often unworkable or insufficient because the MSP's tooling, processes, staffing, and infrastructure are frequently

multi-tenant and implemented across numerous customers, or located overseas, making it practically difficult for a contractor's assessment to meaningfully evaluate the MSP-delivered services without an MSP-level obligation to undergo its own assessment at the appropriate level.

Stated simply: the contractor is clearly required to meet CMMC Level 2 and implement NIST SP 800-171 controls, but the MSP with operational control and privileged access to the contractor's environment can fall outside any explicit "must be certified" requirement, despite representing a path into the environment for adversaries.

MSPs are already defined in federal law, but that definition is not incorporated into Part 170

Congress has already defined "managed service provider" at 6 U.S.C. § 650(18): an entity delivering services such as network, application, infrastructure, or security services via ongoing and regular support and active administration, on customer premises, in the provider's data center (including hosting), or in a third-party data center. We believe this statutory definition is a natural and appropriate basis for closing the Part 170 definitional gap and aligning regulatory expectations with operational realities in the DIB.

A visibility gap: DoW does not know how many contractors are using MSPs, which MSPs, or their CMMC status

The second issue is oversight and visibility. DoW currently does not have a reliable inventory of how many contractors and subcontractors are using MSPs to manage any part of their IT infrastructure, which MSPs are in use, or whether those MSPs hold CMMC certification appropriate to the role they play in CUI environments. Industry sources estimate there are tens of thousands of MSPs operating in the United States, and MSP reliance among small and medium-sized businesses is widespread—particularly among manufacturers, which make up a substantial portion of the DIB supplier ecosystem. The combined effect is (1) a blind spot for DoW and (2) an expanded supply-chain attack surface for nation-state and criminal actors seeking to compromise sensitive defense information by targeting service providers with broad downstream access.

Request for HASC Action

To address these vulnerabilities in a practical and measurable way, the MSP Collective respectfully requests the Committee's assistance in two areas:

1. **Request a DoW survey of MSP use across the DIB.**

   We ask that the House Armed Services Committee formally request DoW to conduct a survey of DoW contractors and subcontractors (at minimum those with CMMC Level 2 requirements) to determine:

   - Whether the contractor uses an MSP to manage any portion of its IT environment that supports systems processing, storing, or transmitting CUI (or Security Protection Data);
   - The identity of each MSP used for such services; and
   - Whether each MSP holds CMMC certification (and at what level), or whether the MSP's services were fully assessed within the scope of the contractor's CMMC assessment.

This survey would provide DoW and Congress a clearer understanding of the scope of exposure and the practical extent to which MSPs are handling or enabling access to CUI without an explicit certification requirement.

2. **Close the definitional and contractual gap through targeted updates.**

   We request support for the following targeted changes:

   (a) Amend 32 CFR Part 170 to (i) define "managed service provider" consistent with 6 U.S.C. § 650(18), and (ii) require MSPs that provide services to DoW contractors, specifically where those services involve administrative access to, or support for, systems that process, store, or transmit CUI, to meet CMMC certification requirements commensurate with the contractor (or subcontractor) to whom they provide those services.

   (b) Modify DFARS 252.204-7012(b)(2)(i) to clarify that MSP-supported covered contractor information systems are subject to NIST SP 800-171 requirements. We propose the following revision (new language in brackets):

   "Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system **[and any managed service provider providing services thereto]** shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations' …"

Conclusion and Call to Action

CMMC is designed to reduce systemic cyber risk in the DIB, but a definitional and scoping ambiguity for MSPs, paired with a lack of DoW visibility into MSP usage, creates an unnecessary vulnerability that adversaries can exploit. Our requested actions are narrow, achievable, and aligned with DoW's stated intent: ensuring that those with functional control over systems handling CUI meet appropriate, verifiable security standards.

Thank you for your leadership and for considering these recommendations. We would welcome the opportunity to brief you and Committee staff, provide technical examples of how MSP access is commonly structured in contractor environments, and support draft language that closes the gap without imposing unnecessary burden on small businesses.

Very Respectfully,

Amy Edwards
Director, Legislative Affairs