An Open Response to the Suspension of CMMC Phase 2

A Statement from
MSPs for the Protection of Critical Infrastructure
July 2026

Where We Stand

On July 13, 2026, the Department of War suspended the November 2026 transition to Phase 2 of the Cybersecurity Maturity Model Certification (CMMC) program, directed requiring activities to designate only self-assessment levels during a 60-day review, and paused the higher-tier assessments that verify how well defense contractors actually protect Controlled Unclassified Information (CUI).

The MSP Collective exists to inform government and industry on exactly this question: how external service providers keep the Defense Industrial Base (DIB) secure, functional, and resilient.

Our members have built their businesses, and helped their clients build compliance, on the strength of the phased CMMC timeline. We offer this response in the constructive, advisory spirit that guides our work with Congress, the Department, and the CyberAB.

We want to be clear at the outset about what we are not saying. We do not defend unnecessary burden on small business. We have consistently advocated for the small and mid-sized firms across the DIB and supported appropriations to offset the one-time cost of reaching CMMC compliance. The compliance-cost and assessor-capacity concerns that motivated this suspension are real, and they deserve a serious answer.

But the answer to a capacity concern is to expand capacity, not to suspend verification. And on the specific question of capacity, the record does not support the premise on which this suspension rests.

The Capacity Shortage Claim Does Not Match the Data

The central justification for the suspension is that the assessor ecosystem cannot meet demand. The Department has characterized the problem as roughly 100,000 companies needing assessments against roughly 100 available assessors.

The observed data tells a different story. Drawing on the monthly CMMC ecosystem counts reported during CyberAB Town Halls from November 2025 through June 2026:

- **New monthly CMMC Level 2 certifications** climbed steadily, from 123 in November 2025 to 279 in June 2026.
- **At a conservative 50-percent-utilization assumption,** ecosystem throughput rose above 400 assessments per month, well ahead of demand.
- **Had that conservative capacity been fully used since November 2025,** the ecosystem could have produced 2,939 Level 2 certifications. It produced 1,717. The difference of 1,222 is not a shortage of assessors. It is unused capacity, assessors ready and waiting for work.

Stated plainly: The Department's shortage narrative does not match the observed demand.

Industry Is Already Delivering at Scale

The phased rollout was not failing. In its regulatory analysis, the Department estimated that roughly 500 companies would achieve CMMC certification in the first year of Phase 1. As of June 2026, more than 1,700 Level 2 assessments had been completed, roughly five times the Department's own projection.

A significant driver of that success is the more than 50 CMMC-certified managed service providers now delivering compliant solutions at scale to the small and mid-sized suppliers the program is meant to protect. This is precisely the public-private capacity that a capacity-based suspension assumes does not exist. It exists, it works, and it is being paused at the moment it is proving itself.

The Department of the Army has already recognized the model. On May 15, 2026, the Army awarded its Next Generation Commercial Operations in Defended Enclaves (NCODE) proof-of-concept to eight companies to provide no-cost CMMC services to small defense contractors, an effort written to scale across the services on a successful demonstration. **We urge that NCODE be allowed to proceed** rather than held in abeyance. Each month of delay falls hardest on the small businesses everyone agrees are the most vulnerable link in the supply chain.

Verification Is the Point

CMMC exists because self-attestation alone did not reflect the real security of contractor systems, and that gap contributed to the loss of sensitive defense information. Reverting to self-assessment does not reduce burden so much as remove the independent check, for precisely the contractors whose self-reports have proven least reliable. A pause that removes verification does not make the DIB more secure; it makes its gaps harder to see, at a moment when nation-state actors continue to target defense suppliers.

Consistency With the Path Forward

The suspension also sits uneasily with the government's own stated direction. The 2026 Unified Agenda of Regulatory and Deregulatory Actions, published July 3, 2026, identifies NIST SP 800-171 Revision 3 as the standard for non-federal systems handling CUI. A mid-course reversal risks confusing the very small businesses it aims to help and raising their costs. If the review produces substantive change, that change will require fresh rulemaking, extending the assurance timeline the FY2020 National Defense Authorization Act directed rather than shortening it.

Questions the Department's Review Should Answer

In the interest of a transparent, evidence-based review, the MSP Collective respectfully urges that the Department of War publicly address the following before the 60-day review concludes:

1. **The security basis.** What threat or risk assessment supported the decision to suspend Phase 2 and revert to self-assessment, and how does the interim posture preserve the security baseline Congress directed under Section 1648 of the FY2020 NDAA?
2. **The capacity premise.** What data underlies the conclusion that assessor capacity is insufficient, and how does it reconcile with the Cyber AB reporting showing substantial unused capacity?

3. **The verification gap.** What do the Defense Contract Management Agency's assessments show about the difference between contractors' self-reported scores and their independently verified scores, and what does that difference imply for relying on self-assessment as an interim baseline?
4. **Reliance and investment.** How did the review weigh the investments that assessors, managed service providers, and contractors made in reliance on the published November 2026 timeline?
5. **Resources for Small Businesses.** The Army awarded 8 companies the "Next-Gen Commercial Operations in Defended Enclaves" (NCODE) contract, which is designed to provide government supported CMMC ready enclaves to small defense contractors in a public/private partnership. Why was this awarded in May of 2026 without funding?
6. **Inconsistent Standard Impact on Rising Cost of Cybersecurity.** The Federal Acquisition Regulation (FAR) council proposed using DFARS 252.204-7012 in July 2026. The Department of Defense has spent considerable resources since 2016 to deploy DFARS 252.204-7012 in alignment with the FAR Council proposal. How would adopting a new and unique standard for the Department of Defense impact ballooning cybersecurity costs?
7. **Deployment Timeline.** In Oct 2016, the Defense Department issued DFARS 252.204-7012 using NIST 800-171 to protect CUI in a non-federal environment. CMMC is an assessment of those NIST requirements issued for the last decade. What is the scope of the review, and will any resulting changes be made through formal rulemaking rather than internal guidance? How long will a new standard take to implement and what is the impact on National Security?

An Offer to Help

The MSP Collective is an industry advisory group, and we mean it. We favor both a real verification floor and genuine relief for small business; these goals are compatible, and the assessment ecosystem is proving they can be met together. We welcome the opportunity to share our members' data and operational experience with the Department of War, the CyberAB, and the review team, and we stand ready to work toward a solution that keeps the DIB secure while lowering the barriers that keep good companies out of it.

Sincerely,
Membership of the MSP Collective