

CMMC: We Heard. We Acted. Your Input Shapes What's Next

From: OSD Pentagon OUSD A-S Mailbox OSBP Info

Sent: Friday, July 24, 2026 12:03 PM

Subject: CMMC: We Heard. We Acted. Your Input Shapes What's Next

Dear Subscribers,

The Department of War is inviting feedback from businesses and industry as part of a comprehensive review of the Cybersecurity Maturity Model Certification (CMMC) program.

On July 13, the Department of War (DoW) suspended implementation of CMMC Phase II and launched a 60-day review of the program to ensure the defense industrial base remains secure while reducing unnecessary burdens on the small, medium-sized, and non-traditional businesses that are foundational to American manufacturing and innovation. This effort supports the Department's commitment to strengthening cybersecurity while advancing acquisition transformation and industrial base growth.

We Heard. We Acted. Your Input Shapes What's Next.

The Department suspended CMMC Phase II and initiated this review after hearing consistent feedback from industry about the need to strengthen cybersecurity while reducing unnecessary cost, complexity, and administrative burden. Industry participation is essential to ensuring the next phase of CMMC reflects practical, scalable, and mission-focused solutions.

Share Your Feedback

The Department is actively seeking industry input through the official Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base Request for Information (RFI) on SAM.gov.

- Submit comments through the official SAM.gov RFI:
<https://sam.gov/workspace/contract/opp/89ef9bfb0834473791e991c712698d94/view>
- Deadline: Thursday, August 14, 2026, at 12:00 p.m. ET

Your feedback will help inform the CMMC Reform Task Force as it develops recommendations to strengthen cybersecurity while reducing unnecessary compliance burden across the defense industrial base.

The Department will also host a series of industry listening sessions in the coming weeks. Details will be shared through the DoW Office of Industrial Base Growth website, business.defense.gov, and on our social media channels. We encourage you to help amplify these opportunities throughout your network to maximize stakeholder participation.

What Businesses Should Know

Cybersecurity requirements remain in effect. The importance of strong cybersecurity has not changed.

While the Department reviews the CMMC program, companies should continue strengthening their cybersecurity posture and complying with existing contractual requirements. Specifically, organizations handling Controlled Unclassified Information (CUI) should continue to:

- Implement NIST SP 800-171 Rev. 2 security controls.
- Comply with applicable DFARS 252.204-7012 cybersecurity requirements.
- Complete required Phase I self-assessments.
- Maintain cybersecurity documentation and continue improving their cyber readiness.

Businesses should not pause their cybersecurity efforts. Investments made to strengthen cybersecurity remain valuable and will help organizations remain competitive, resilient, and prepared for future requirements.

Key Resources

For the latest official guidance, visit the DoW Chief Information Officer's CMMC resources:

- [DoW CIO CMMC Homepage](#)
- [CMMC Resources & Documentation](#)
- [CMMC Frequently Asked Questions \(FAQ\)](#)

Your Voice Matters

The Office of Industrial Base Growth encourages businesses of all sizes to share their perspectives. Industry feedback is essential to ensuring the Department develops a practical, effective, and scalable approach to cybersecurity that strengthens both national security and defense marketplace participation.

Thank you for helping shape the future of cybersecurity across the defense industrial base.

V/R,

OASW for Industrial Base Policy, OUSW for Acquisition & Sustainment
Office of Industrial Base Growth
<https://business.defense.gov>

To subscribe to the online LinkedIn edition, click here:
<https://www.linkedin.com/newsletters/7064673821869400064>