CMMC Phase II Pause

What Changed, What Didn't, and How to Use the Time Wisely

DTCGlobal.us

PRESENTED BY: Regan Edens
Chairman, CISC

CMMC INDUSTRY STANDARDS COUNCIL
e Pluribus Unum

info@dtcglobal.us
dtcglobal.us

DTC GLOBAL Copyright 2026 All Rights Reserved.

Purpose

Inform, Equip, & Enable Good Decisions

CMMC PNW attendees understand:

- What the US Depart of War CIO actually announced
- What remains required today
- Why the national security mission has not changed
- How to use the additional time to improve implementation and reduce risk
- Practical next steps to prepare for future certification

DTC GLOBAL Copyright 2026 All Rights Reserved.

About Regan Edens

National Security and Industry Cyber Thought Leader since 2006

- ✓ CMMC Evangelist, leading over 20,000 volunteer hours in CMMC standards and policy development
- ✓ Operationalized $ 3.5B in Globally Distributed DoD, IC, & SOF Missions & Technologies
- ✓ Received President's Lifetime Volunteer Service Award and led 19 Gold Medal Awardees
- ✓ DTC Global Advisory Services and Supply Chain Strategy for Security, Compliance, & Technology
- ✓ Led DoD Organizations Awarded 4 Defense Superior Civilian Service Awards and 14 Bronze Stars, 12 Army Commendation Medals, and 6 Army Achievement Medals
- ✓ Large Prime Contractors, Supply Chain Risk Management, and Tier Suppliers
- ✓ Clients: $46.8B Market Cap, 235k Employees, 300-325k Endpoints

Defense Cybersecurity & Compliance Leadership

Served/Serving:

- ✓ Chairman, CMMC Industry Standards Council, since Jan '22
- ✓ Cyber Advisory Board, Southern Methodist University, '22
- ✓ Policy Advisor, US Cyber Command on Controlled Unclassified Information
- ✓ Policy Advisor, Department of Defense on CMMC
- ✓ CYBER-AB Founding Director, Board of Directors, Aug 21 (Former)
- ✓ CYBER-AB Chairman of the Standards Management Committee, Aug 21 (Former)
- ✓ CYBER-AB Vice Chairman of the Training Committee, Aug 21 (Former)
- ✓ CYBER-AB Chairman/Co-Vice Chair of Standards Management Industry Working Group, Aug 21 (Former)
- ✓ CMMC-AB Co-Vice Chair of the Standards IWG, Aug 21 (Former)
- ✓ (ACTING) CYBER-AB Certified Master Instructor, Aug 21 (Former)
- ✓ CMMC Certified Instructor, Certified Professional, & Provisional Assessors
- ✓ CMMC Licensed Training Provider (Partner)

Copyright 2023 All Rights Reserved.

DTC GLOBAL Copyright 2026 All Rights Reserved.

DTCGlobal.us

Private Briefing

Use of content is authorized
for individual use only
and strictly limited.

Screenshots are authorized
for personnel use.

DTC GLOBAL Copyright 2026 All Rights Reserved.

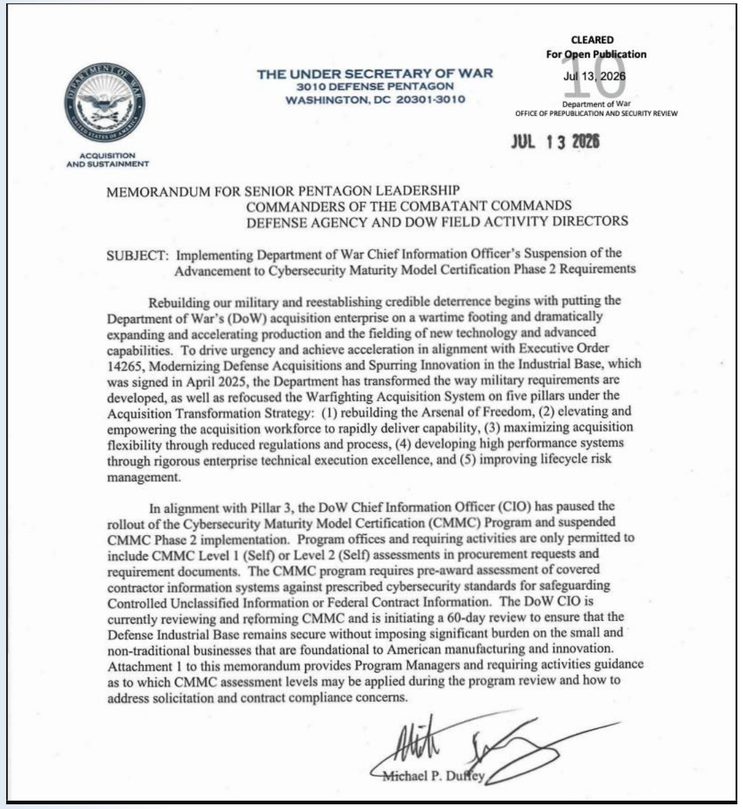
References

Inform, Equip, & Enable Good Decisions

YOUR Information Sources Matter

- DoW Press Release and Memorandum by DoW CIO, July 13, 2026
- CMMC FAQ, July 2026
- Memorandum on Class Deviation—Revolutionary Federal Acquisition Regulation (FAR) Overhaul Part 40, Defense FAR Supplement (DFARS) Part 240, Feb 1, 2026
- DFARS 252.204-7012 and DFARS 252.204-7021
- FAR CUI Rule Overhaul
- Other DoW Memorandums, Instructions, Supplemental Guidance 2017-2026

Private Briefing on CMMC Phase II Pause



CLEARED
For Open Publication
Jul 13, 2026
Department of War
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

THE UNDER SECRETARY OF WAR
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION AND SUSTAINMENT

JUL 13 2026

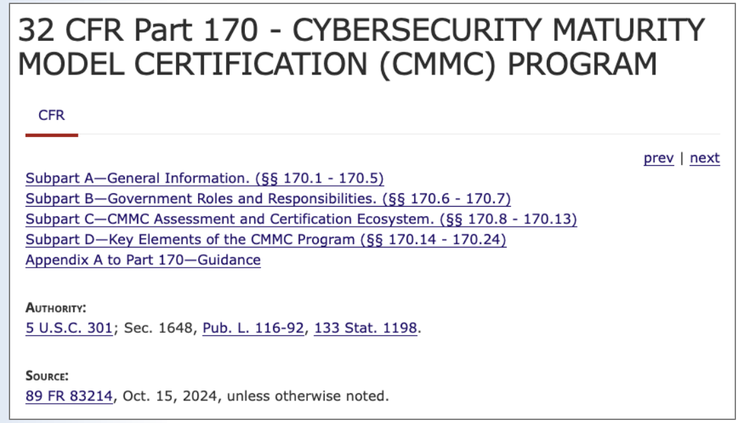
MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements

Rebuilding our military and reestablishing credible deterrence begins with putting the Department of War's (DoW) acquisition enterprise on a wartime footing and dramatically expanding and accelerating production and the fielding of new technology and advanced capabilities. To drive urgency and achieve acceleration in alignment with Executive Order 14265, Modernizing Defense Acquisitions and Spurring Innovation in the Industrial Base, which was signed in April 2025, the Department has transformed the way military requirements are developed, as well as refocused the Warfighting Acquisition System on five pillars under the Acquisition Transformation Strategy: (1) rebuilding the Arsenal of Freedom, (2) elevating and empowering the acquisition workforce to rapidly deliver capability, (3) maximizing acquisition flexibility through reduced regulations and process, (4) developing high performance systems through rigorous enterprise technical execution excellence, and (5) improving lifecycle risk management.

In alignment with Pillar 3, the DoW Chief Information Officer (CIO) has paused the rollout of the Cybersecurity Maturity Model Certification (CMMC) Program and suspended CMMC Phase 2 implementation. Program offices and requiring activities are only permitted to include CMMC Level 1 (Self) or Level 2 (Self) assessments in procurement requests and requirement documents. The CMMC program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding Controlled Unclassified Information or Federal Contract Information. The DoW CIO is currently reviewing and reforming CMMC and is initiating a 60-day review to ensure that the Defense Industrial Base remains secure without imposing significant burden on the small and non-traditional businesses that are foundational to American manufacturing and innovation. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance as to which CMMC assessment levels may be applied during the program review and how to address solicitation and contract compliance concerns.

Michael P. Duffey



32 CFR Part 170 - CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

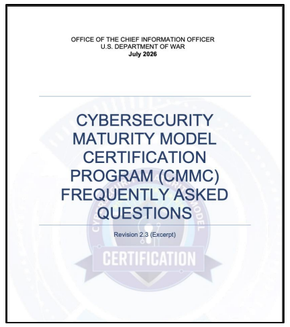
CFR

prev | next

Subpart A—General Information. (§§ 170.1 - 170.5)
Subpart B—Government Roles and Responsibilities. (§§ 170.6 - 170.7)
Subpart C—CMMC Assessment and Certification Ecosystem. (§§ 170.8 - 170.13)
Subpart D—Key Elements of the CMMC Program (§§ 170.14 - 170.24)
Appendix A to Part 170—Guidance

AUTHORITY:
5 U.S.C. 301; Sec. 1648, Pub. L. 116-92, 133 Stat. 1198.

SOURCE:
89 FR 83214, Oct. 15, 2024, unless otherwise noted.

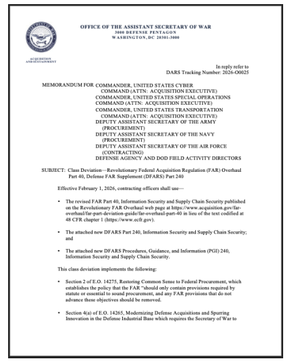


OFFICE OF THE CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF WAR
July 2026

CYBERSECURITY MATURITY MODEL CERTIFICATION PROGRAM (CMMC) FREQUENTLY ASKED QUESTIONS

Revision 2.3 (Excerpt)

CERTIFICATION



OFFICE OF THE ASSISTANT SECRETARY OF WAR
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

In reply refer to
DARS Tracking Number: 2024-O0025

MEMORANDUM FOR COMMANDER, UNITED STATES CYBER COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION COMMAND (ATTN: ACQUISITION EXECUTIVE)
DEPUTY ASSISTANT SECRETARY OF THE ARMY (PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY (PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (CONTRACTING)
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

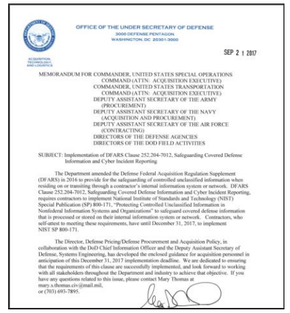
SUBJECT: Class Deviation—Revolutionary Federal Acquisition Regulation (FAR) Overhaul Part 40, Defense FAR Supplement (DFARS) Part 240

Effective February 1, 2026, contracting officers shall use—

- The revised FAR Part 40, Information Security and Supply Chain Security published on the Revolutionary FAR Overhaul web page at https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-40 in line of the text codified at 48 CFR chapter 1 (https://www.ecfr.gov);
- The attached new DFARS Part 240, Information Security and Supply Chain Security; and
- The attached new DFARS Procedures, Guidance, and Information (PGI) 240, Information Security and Supply Chain Security.

This class deviation implements the following:

- Section 2 of E.O. 14275, Restoring Common Sense to Federal Procurement, which establishes the policy that the FAR "should only contain provisions required by statute or essential to sound procurement, and any FAR provisions that do not advance these objectives should be removed.
- Section 4(a) of E.O. 14265, Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base which requires the Secretary of War to



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

SEP 2 1 2017

MEMORANDUM FOR COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION COMMAND (ATTN: ACQUISITION EXECUTIVE)
DEPUTY ASSISTANT SECRETARY OF THE ARMY (PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY (ACQUISITION AND PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (CONTRACTING)
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

The Department amended the Defense Federal Acquisition Regulation Supplement (DFARS) in 2016 to provide for the safeguarding of controlled unclassified information when residing on or transiting through a contractor's internal information system or network. DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires implementation of 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" to safeguard covered defense information that is processed or stored on their internal information system or network. Contractors, who self-attest to meeting these requirements, have until December 31, 2017, to implement NIST SP 800-171.

The Director, Defense Pricing/Defense Procurement and Acquisition Policy, in collaboration with the DoD Chief Information Officer and the Deputy Assistant Secretary of Defense for Systems Engineering, has established a process for contractors to request relief in anticipation of this December 31, 2017 implementation deadline. We are dedicated to ensuring that the requirements of this clause are successfully implemented, and look forward to working with all stakeholders throughout the Department and industry to achieve that objective. If you have any questions related to this issue, please contact Mary Thomas at mary.s.thomas.civ@mail.mil, or (703) 693-7895.

DTC GLOBAL Copyright 2026 All Rights Reserved.

A CMMC Baseline of Hard Truths

Greatest risk to Warfighter is TODAY, not in 2016

- Public Pressure on Congress → High Costs
- Pressure on Mid-Term Elections
- What is driving higher cost → Poor guidance, Inaccurate scoping, & higher than necessary labor costs
- 40-60% of OSC's "Not ready" for C3PAOs
- Extra time is needed across the board
- Program can be **easily** improved
- Lower costs without compromising security and assurance

False Claims Act (cybersecurity-related)

- **LOGZONE (June 2026)**: Alabama defense logistics contractor paid **$507,144** to resolve allegations of submitting false claims on Navy contracts by posting a perfect SPRS score of 110 while a DIBCAC assessment scored the company –170 on NIST SP 800-171 implementation.
- DOJ built the case from audit data without needing a whistleblower or successful breach.
- ITAR High Risk → Earlier relevant settlements (still shaping the enforcement climate into 2026) involved primes, subs, and suppliers for false cybersecurity certifications, missing system security plans, non-compliant cloud services, or inadequate protection of technical drawings under DFARS 252.204-7012. Swiss Automation (precision machining subcontractor) remains a clear example of the cyber + ITAR overlap for tier suppliers.

DTC GLOBAL Copyright 2026 All Rights Reserved.

A CMMC Baseline of Hard Truths

Far greater risk to Warfighter TODAY than in 2016

- Public Pressure on Congress → High Costs
- Higher Cost → Poor guidance, Inaccurate scoping, & higher than necessary labor costs
- 50% of OSC's "Not ready" for C3PAOs
- Pressure on Mid-Term Elections
- Extra time is needed across the board
- Program can be easily improved
- Ways to lower costs without compromising security and assurance

CUI Requirements are EXPANDING

- ✓ FAR CUI Rule is in effect → All Federal Agencies
- ✓ Requires safeguarding of CUI
- ✓ Requires flowdown to all Tiers
- ✓ Requires Agency enforcement
- ✓ Requires a Standard Form to identify CUI to Primes

DoW needs products to be delivered UNCOMPROMISED

- ✓ DIB is too big to protect
- ✓ Protect innovation while reducing attack surface
- ✓ DoW recognizes IoT/OT and resilience are persistent weaknesses even with CMMC
- ✓ DoW needs to better triage / prioritize Level 2 Certifications
- ✓ Better enforcement of affirmation
- ✓ Align interdepartmental guidance and resources into a coherent strategy

Private Briefing on CMMC Phase II Pause

DTC GLOBAL Copyright 2026 All Rights Reserved.

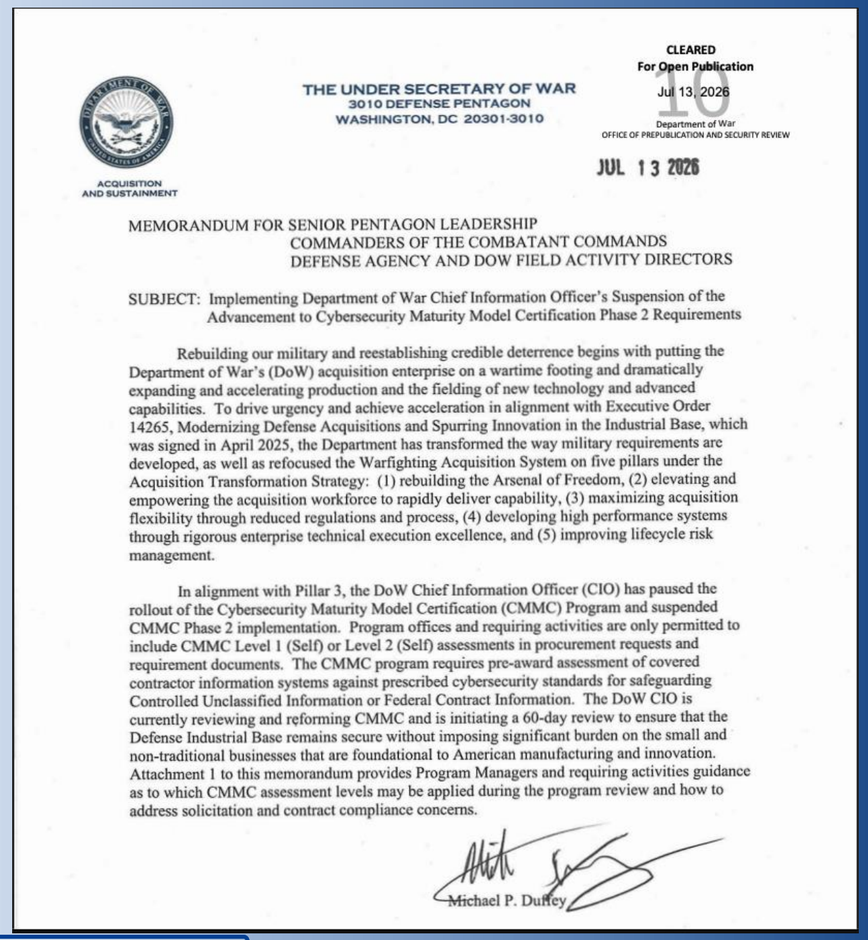
Announcement

What Changed?

Words Matter…

Suspension of Phased Implementation Schedule, Including November 2026 Phase 2 Transition:

- The upcoming November 2026 transition to Phase 2 of CMMC implementation is suspended.
- During the 60 day review period of suspension, Program Managers and requiring activities must only include the need for CMMC Level 1 (Self) or Level 2 (Self) assessments in procurement request and requirement documents.
- Program Managers and requiring activities may **not** designate CMMC Level 2 (C3PAO) or Level 3 (DIBCAC) assessments during this period.



CLEARED
For Open Publication
Jul 13, 2026
Department of War
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

THE UNDER SECRETARY OF WAR
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION AND SUSTAINMENT

JUL 13 2026

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements

Rebuilding our military and reestablishing credible deterrence begins with putting the Department of War's (DoW) acquisition enterprise on a wartime footing and dramatically expanding and accelerating production and the fielding of new technology and advanced capabilities. To drive urgency and achieve acceleration in alignment with Executive Order 14265, Modernizing Defense Acquisitions and Spurring Innovation in the Industrial Base, which was signed in April 2025, the Department has transformed the way military requirements are developed, as well as refocused the Warfighting Acquisition System on five pillars under the Acquisition Transformation Strategy: (1) rebuilding the Arsenal of Freedom, (2) elevating and empowering the acquisition workforce to rapidly deliver capability, (3) maximizing acquisition flexibility through reduced regulations and process, (4) developing high performance systems through rigorous enterprise technical execution excellence, and (5) improving lifecycle risk management.

In alignment with Pillar 3, the DoW Chief Information Officer (CIO) has paused the rollout of the Cybersecurity Maturity Model Certification (CMMC) Program and suspended CMMC Phase 2 implementation. Program offices and requiring activities are only permitted to include CMMC Level 1 (Self) or Level 2 (Self) assessments in procurement requests and requirement documents. The CMMC program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding Controlled Unclassified Information or Federal Contract Information. The DoW CIO is currently reviewing and reforming CMMC and is initiating a 60-day review to ensure that the Defense Industrial Base remains secure without imposing significant burden on the small and non-traditional businesses that are foundational to American manufacturing and innovation. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance as to which CMMC assessment levels may be applied during the program review and how to address solicitation and contract compliance concerns.

Michael P. Duffey

Private Briefing on CMMC Phase II Pause

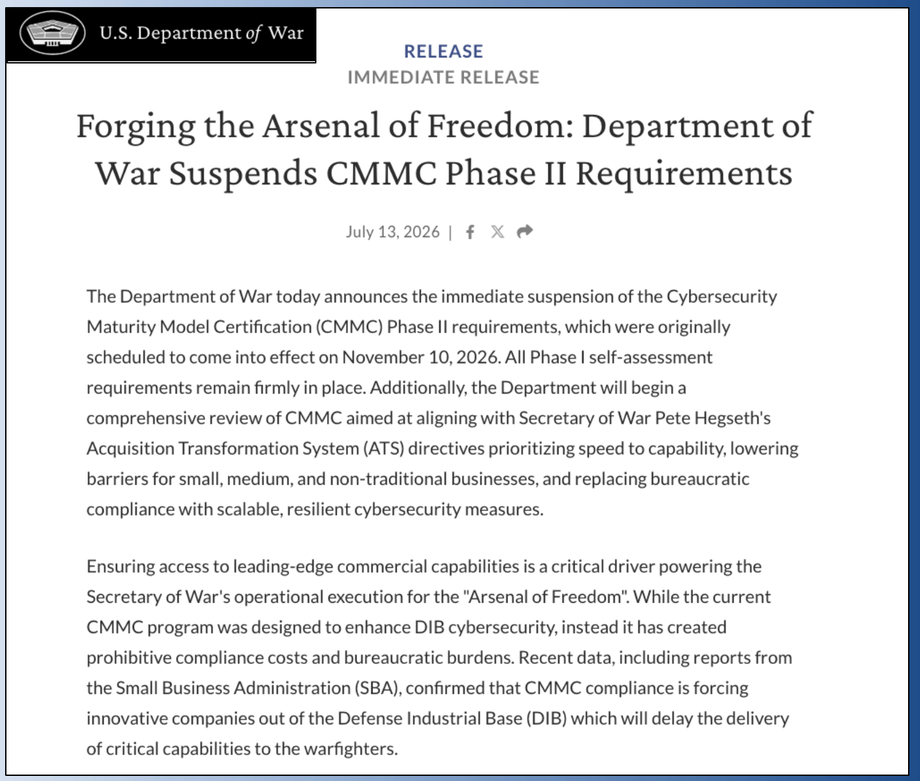
DTC GLOBAL Copyright 2026 All Rights Reserved.

Private Briefing on CMMC Phase II Pause

60 Day Review Period?

Words Matter…

- **RFI Request:** Request for Information (RFI) completed.
- **CMMC Reform Task Force:** To realign our cybersecurity posture with the principles of the ATS, the Department CIO is establishing a CMMC Reform Task Force to conduct a comprehensive top-to-bottom review of the certification program.
- This task force will serve as the central hub for synthesizing industry feedback from our public Request for Information (RFI) regarding compliance challenges.
- Using these insights, the team will recommend realistic, scalable security measures that prioritize speed to capability and lower barriers for small and non-traditional businesses, delivering their final report to the DoW CIO within 60 days.



U.S. Department of War

RELEASE

IMMEDIATE RELEASE

Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements

July 13, 2026 |

The Department of War today announces the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which were originally scheduled to come into effect on November 10, 2026. All Phase I self-assessment requirements remain firmly in place. Additionally, the Department will begin a comprehensive review of CMMC aimed at aligning with Secretary of War Pete Hegseth's Acquisition Transformation System (ATS) directives prioritizing speed to capability, lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures.

Ensuring access to leading-edge commercial capabilities is a critical driver powering the Secretary of War's operational execution for the "Arsenal of Freedom". While the current CMMC program was designed to enhance DIB cybersecurity, instead it has created prohibitive compliance costs and bureaucratic burdens. Recent data, including reports from the Small Business Administration (SBA), confirmed that CMMC compliance is forcing innovative companies out of the Defense Industrial Base (DIB) which will delay the delivery of critical capabilities to the warfighters.

DTC GLOBAL Copyright 2026 All Rights Reserved.

Private Briefing on CMMC Phase II Pause

CMMC Timeline

- ✓ **2024 –** The CMMC Final Rule (32 CFR Part 170), published October and effective on December 16, 2024.
- ✓ **2025 –** CMMC Phase I Affirmation Requirements Begin (Nov to Nov 26)

- ✓ DFARS 252.204-7012 continues
- ✓ CMMC contract clause (DFARS 252.204-7021) issuances

- ➢ **CMMC Phase II start date on Nov 26 is paused**
- ➢ **60 Days Pending Review**
- ➢ **CMMC Phase I continues…**

✓ **Contract Eligibility REQUIRES CMMS Phase I Compliance**

DTC GLOBAL Copyright 2026 All Rights Reserved.

Private Briefing on CMMC Phase II Pause

CMMC Phase I – What Did NOT Change?

Words Matter…

- During this interim period, the Department will enforce cybersecurity compliance with the NIST SP 800-171 Rev 2 standard through self-assessments and **select government-led assessments**, focusing on tangible cyber hygiene rather than administrative overhead.
- It is critical to note that this action does not eliminate the requirement for companies to protect federal data.
- All defense contractors and subcontractors remain contractually obligated to safeguard covered defense information in accordance with DFARS clause 252.204-7012.

U.S. Department of War

RELEASE

IMMEDIATE RELEASE

Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements

July 13, 2026 |

The Department of War today announces the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which were originally scheduled to come into effect on November 10, 2026. All Phase I self-assessment requirements remain firmly in place. Additionally, the Department will begin a comprehensive review of CMMC aimed at aligning with Secretary of War Pete Hegseth's Acquisition Transformation System (ATS) directives prioritizing speed to capability, lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures.

Ensuring access to leading-edge commercial capabilities is a critical driver powering the Secretary of War's operational execution for the "Arsenal of Freedom". While the current CMMC program was designed to enhance DIB cybersecurity, instead it has created prohibitive compliance costs and bureaucratic burdens. Recent data, including reports from the Small Business Administration (SBA), confirmed that CMMC compliance is forcing innovative companies out of the Defense Industrial Base (DIB) which will delay the delivery of critical capabilities to the warfighters.

DTC GLOBAL Copyright 2026 All Rights Reserved.

What Did NOT Change?

Do not be confused --> CMMC Phase I continues

- ✓ All organizations must still implement and meet CMMC Level 2 requirements to **AFFIRM** their contract eligibility in CMMC Phase 1

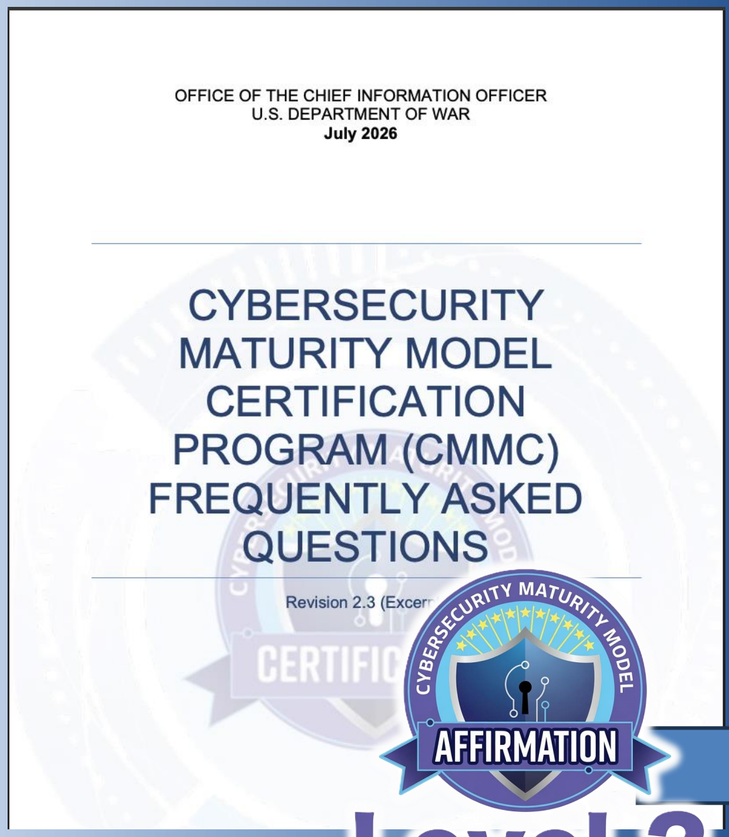
What Does That Mean?

Words Matter…

- **B-Q2.** What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and CMMC?

- **B-A2.** NIST SP 800-171 is the federal safeguarding standard for controlled unclassified information (CUI) required by 32 Code of Federal Regulations (CFR) Part 2002, which the Department implemented contractually through inclusion of Defense Federal Acquisition Regulation Supplement clause 252.204-7012 in applicable contracts.

- As of November 10, 2025, applicable contractors are required to **undergo a Level 2 self-assessment** to **verify compliance** with those NIST SP 800-171 Revision 2 requirements.



What Does That Mean?

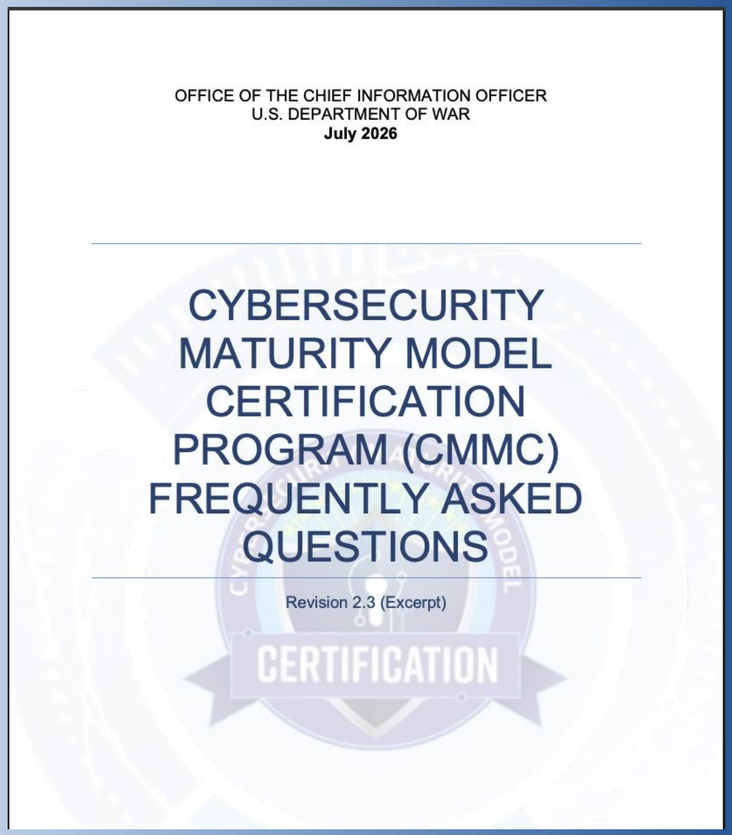
Words Matter…

CMMC Phase I → Contract Eligibility

- ✓ **DFARS 252.204-7012 Contract Clause**
- ✓ **32 CFR Part 2002,**
- ✓ **NIST 800-171 Rev 2.**
- ✓ **32 CFR Part 170 Scope and External Services**
- ✓ **SPRS Score & Reporting**

Organizations must still:

- Follow DFARS 7012 requirements, safeguards, & cyber incident reporting
- Follow DoW policy guidance
- Protect and handle Controlled Unclassified Information (CUI) IAW requirements
- Implement NIST SP 800-171 on systems necessary to perform contracts
- Maintain required evidence /access and supporting documentation
- Update registration and SPRS Score


OFFICE OF THE CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF WAR
July 2026

CYBERSECURITY MATURITY MODEL CERTIFICATION PROGRAM (CMMC) FREQUENTLY ASKED QUESTIONS

Revision 2.3 (Excerpt)

DTC GLOBAL Copyright 2026 All Rights Reserved.

CMMC Phase I Affirmation Requirements

Critical Requirements

Minimum SPRS score 80% or 88 points required for Conditional Affirmation

⚠ **No Prohibited POA&M Items**

Adequate and sufficient evidence to support all documentation

⚠ Annual Affirmation is related to annual risk and security assessment(s) → SSP updates

Prohibited POA&M Items

⚠ **AC.L2-3.1.20 External Connections → External/Managed Services**

- AC.L2-3.1.22 Control Public Information
- PE.L2-3.10.3 Escort Visitors
- PE.L2-3.10.4 Physical Access Logs
- PE.L2-3.10.5 Manage Physical Access

180-Day Deadline

All other POA&M items must be closed **within 180 days**.

Full affirmation requires 110 SPRS score with sufficient evidence.

If not, supervised remediation by DoD COR and Prime Contractor

DTC GLOBAL Copyright 2026 All Rights Reserved.

Why the Pause Matters for YOU

Hard Truth – To Safeguard the DIB, the attach surface has to shrink

Organizations that understand the pause will gain a competitive advantage.

- Complete readiness ASAP → Update documentation
- Demonstrate **readiness early** to customers and "Customers of customers"
- Differentiate to win more business
- Fill the gap as the preferred low risk supplier
- Look for buying opportunities → YOUR competitors & Supply Chain
- Work with suppliers **to lower delivery risks and costs**

DTC GLOBAL Copyright 2026 All Rights Reserved.

Why the Pause Matters for YOU

Don't

The organizations that misunderstand the pause are likely to:

- Stop implementation
- Delay decisions
- Lose momentum
- Increase contractual risk of stop work
- Increase False Claims risk
- Spend more later (demand +)

Those organizations under compliance stress will:

- Sell at a discount
- Merge
- Seek investors or Fold
- Exit defense work

*"Periods of regulatory transition often **accelerate market consolidation**. Organizations with mature cybersecurity capabilities, strong balance sheets, and a long-term strategy may **find opportunities to acquire at a discount** complementary technologies, talent, competitors, or even suppliers that strengthen their position within the Defense Industrial Base." **AS9100 Hard Lessons Learned & Relived***

Private Briefing on CMMC Phase II Pause

DTC GLOBAL Copyright 2026 All Rights Reserved.

How to use the time wisely..

7 Expensive Lessons Learned

Lesson 1 40-60% of OSC's are turned away by C3PAOs
→ Implementation guidance LOWERS costs and accelerates readiness

Lesson 2 CUI Identification/ flow is still the foundation
→ CUI received, developed, and shared → DoD Instruction 5230.24

Lesson 3 CMMC impacts the entire scope of contract performance, not just IT
→ Follow the flow of CUI

DTC GLOBAL Copyright 2026 All Rights Reserved.

How to use the time wisely..

7 Expensive Lessons Learned

Lesson 4 Business stakeholders and IT stakeholders work TOGETHER to determine scope

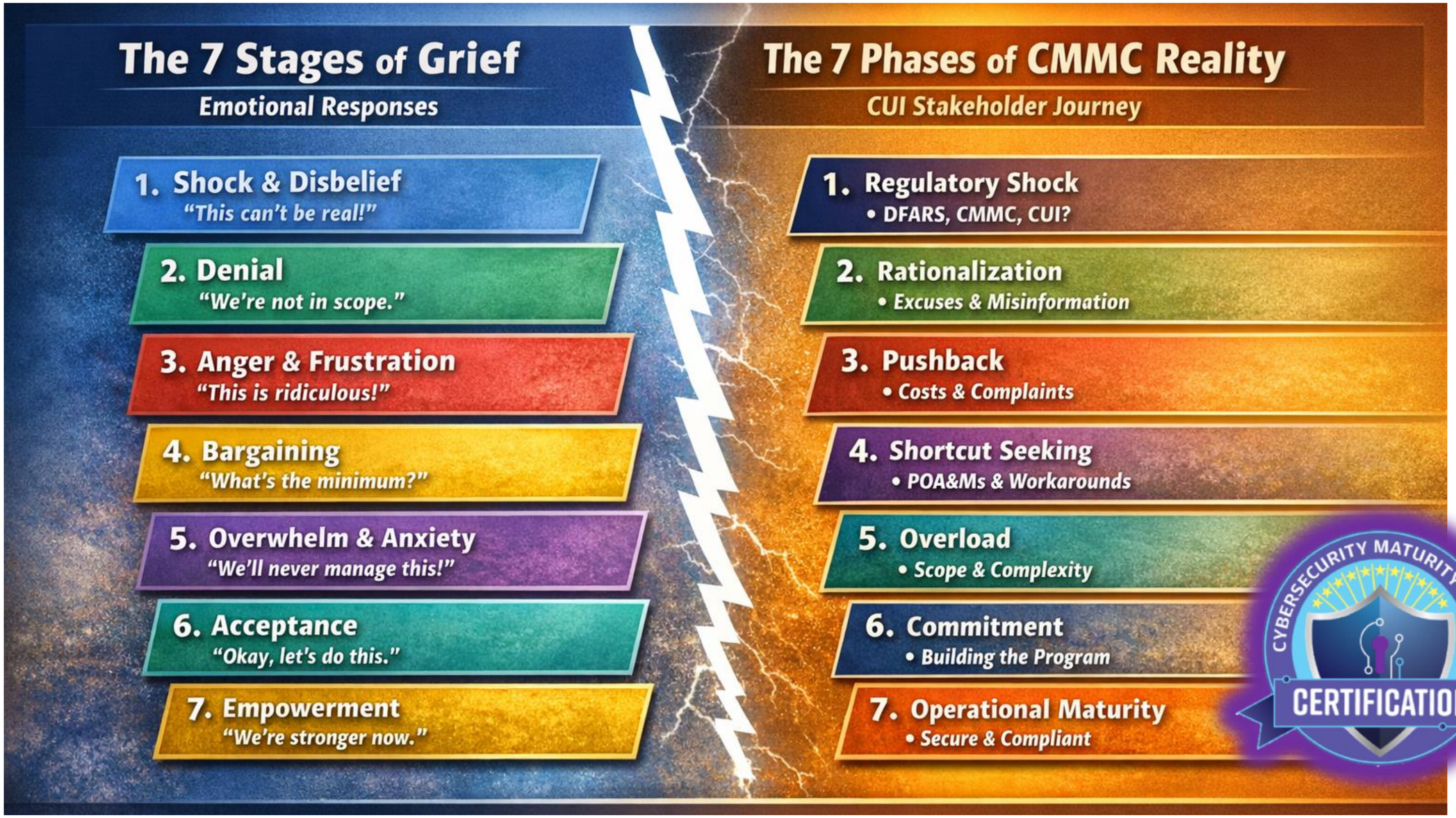
Lesson 5 Scope determines cost → Over/Under Scoping drives up costs / rework

Lesson 6 Manage services readiness is a serious risk

Lesson 7 Supply Chain, Supply Chain, Supply Chain

DTC GLOBAL Copyright 2026 All Rights Reserved.

GRIT and Empathy are required



How to use the time wisely..

7 Expensive Lessons Learned

Lesson 4 Business stakeholders and IT stakeholders work TOGETHER to determine scope

Lesson 5 Scope determines cost → Over/Under Scoping drives up costs / rework

Lesson 6 Manage services readiness is a serious risk

Lesson 7 Supply Chain, Supply Chain, Supply Chain

DTC GLOBAL Copyright 2026 All Rights Reserved.

So what's the good news...

The people who will stand before have walked through fire...

- ✓ Mike Snyder, Ryan Bonner, Eric Crusious
- ✓ Stuart Itkin, Brandon Sessions, Koren Wise
- ✓ Jerry Leishman, Tiffany Groce, Rick Rosenbury

DTC GLOBAL Copyright 2026 All Rights Reserved.

How to use the time wisely..

Recommendations

- Get your implementation done.
- Update your documentation, ANNUAL requirements.
- Verify your External Services ACTUALLY MEET REQUIREMENTS.
- Update your SPRS Score to 88 then 110 when ready.
- Engage customers and customers of customers.
- Work on Supply Chain risk.
- CONTRACT ELIGABILITY IS THE CRITICAL GOAL
- Be ready for Certification to resume….

DTC GLOBAL Copyright 2026 All Rights Reserved.

DTCGlobal.us

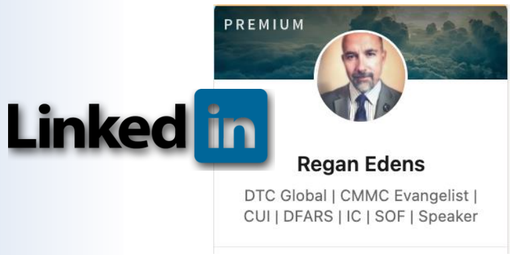
Private Briefing

Your Questions?

DTC GLOBAL Copyright 2026 All Rights Reserved.

CUI Supply .com

DTCGlobal.us



Regan Edens
Chief Transformation & Compliance
Email: ReganEdens@dtcglobal.us
www.dtcglobal.us

DTC GLOBAL Copyright 2026 All Rights Reserved.