LIVE WEBINAR

CMMC Unlocked What 48 CFR Means for Your Business

Thursday, September 18th 1-2 PM Eastern









Topics

- Introduction
- The History of CMMC
- Overview of 48 CFR
 - Flow-Down Requirements
- CMMC Assessments
 - CMMC Level 2 What Contractors Must Do
 - Preparing for Assessments
- Next Steps for Contractors
- Q&A







Meet the Speakers



Tobias Musser
Co-CEO MNS Group





Michael Dempsey
CEO CISEVE





Brian HubbardPresident, Evolved Cyber









Tobias Musser
Co-CEO MNS Group

A CMMC Level 2 Certified MSP/MSSP

STAFFED BY:

- CMMC Certified Professionals (73 CCP)
- CMMC Certified Assessors (40+ CCA's)
- Registered Practitioners (100% Staff RP's)

OVERVIEW

- Headquarters in Maryland Supporting 300+ locations worldwide
- Security and compliance-focused
- Modeled on a risk framework, we assist our partners to identify and minimize risk areas: operational, financial, technological, human, vendor, client, and reputational.
- Committed to protecting the USA, business by business.







Michael Dempsey
CEO CISEVE

CISEVE is one of the first Authorized C3PAOs

CISEVE is an organization committed to servicing our clients with the highest integrity and quality. Our reliable, professional, certified and cleared staff provide services to a variety of industries through a commitment to confidentiality and integrity.

CISEVE is led by cybersecurity experts from various fields, backgrounds with over 50 years of total experience that pulls together to provide the most current and secure approaches to protecting and assessing your organization.









Brian Hubbard
President, Evolved Cyber

- 40+ years in cybersecurity, supporting DoD, NSA, and commercial enterprises
- Lead author of the original NIST Cybersecurity Framework (CSF) while supporting NIST
- Former Director of Commercial & Cybersecurity at Edwards
 Performance Solutions built and led CMMC practice
- Extensive experience delivering Joint Surveillance Voluntary Assessments (JSVA) and CMMC assessments
- Founder & President, Evolved Cyber Solutions specializing in CMMC consulting, training, and assessments
- Certified CMMC Assessor (CCA), CMMC Certified Professional (CCP), and Certified Instructor
- Proven track record guiding OSCs to successful assessment outcomes
- Industry thought leader and frequent speaker on cybersecurity compliance readiness

Disclaimer:

We would love to perform your assessment, so we cannot offer any advice during this webinar pertaining to your specific environment.



The History Of CMMC

(Cybersecurity Maturity Model Certification)







CMMC Objectives

- Safeguard and protect CUI (Controlled Unclassified Information) and FCI (Federal Contract Information)
- Create a consistent standard for cybersecurity across the DIB (Defense Industrial Base)
- Increase accountability and compliance through C3PAOs (Certified Third-party Assessment Organizations) assessments
- Strengthen our National Security to protect our warfighters











CMMC Levels

Level	Requirements	# of Controls	Information	Assessment Type
1 Foundational	FAR 52.204-21	15	FCI	Self-assessment
2 Advanced	DFARS 252.204-7012	110	CUI	 Self-assessment C3PAO *Both require the same effort and stringency
3 Expert	-	24	CUI	A Final Level 2 C3PAO certification for the same scope (on a three-year cycle), a DIBCAC Level 3 certification assessment (three-year cycle)







The History of CMMC

September 2019

CMMC was announced as the DoW's effort to move beyond self-attestation for NIST SP 800-171 and protect the defense supply chain.

January 31, 2020

CMMC 1.0 was released.



November 4, 2021

After an internal review, DoW unveiled 'CMMC 2.0' streamlining the model to three levels.

October 15, 2024

The program was formally codified as 32 CFR Part 170 (effective December 16, 2024).

September10, 2025

DFARS/48 CFR rule was finalized, allowing CMMC clauses appear in DoW contracts beginning November 10, 2025.









2017 **NIST 800-171 CUI**

NST

Defense contractors are required to meet NIST 800-171when handling controlled unclassified information (CUI)



2020 **CMMC 1.0 Released**



Cybersecurity Maturity Model Certification (CMMC) framework: Standardized cybersecurity approach over entire Defense Industrial Base, including suppliers. Interim Rule effective 11/30/20





Streamlined model announced after public comments. November 2021

2023 NIST SP 800-171 r.3



Revised draft guidelines announced for CUI. Final to be published early 2024

2024 32 CFR CMMC **Rule Published**



Published Oct 15, 2024; effective Dec 16, 2024. Defines the CMMC program inside the DoW.

2025 48 CFR Rule **Published**



Published Sept 10, 2025; effective Nov 10, 2025, Implements CMMC in solicitations and contracts through DFARS clauses.

Requirements start appearing in new DoD contracts on the effective date.





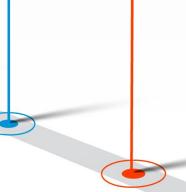


2023 **CMMC Review** Complete CMMC regulatory process is completed: DoD submitted CMMC rule to the OIRA in

July. November 2023 OIRA completed their review.

OIRA





Defense CUI

Defense CUI is unclassified information related to DoD missions or systems that the government says must be safeguarded and shared only on a need-to-know basis (per the CUI Registry's "Defense" category).











What Counts as "Defense CUI"?

Examples of Defense CUI categories

- Controlled Technical Information (CTI)
- DoD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Privileged Safety Information
- Unclassified Controlled Nuclear Information Defense



Gut Check: If your team creates, receives, or stores any of the above for a DoD program, or if you handle documents marked as CUI, you likely handle CTI.











Overview of 48 CFR

What You Need to Know









48 CFR (DFARS) is the enforcement lever that turns the CMMC program from policy into contract reality.







32 CFR

- Became effective December 16, 2024
- Established the CMMC program
- Provides the framework for implementing CMMC across the DIB.
- Defines the roles, responsibilities, and structure of the CMMC ecosystem.
- Guides the certification process

48 CFR

- Effective: November 10, 2025
- Establishes uniform policy and procedures across the federal government
- Includes clauses that require compliance with NIST SP 800-171 and CMMC Certification for handling CUI/FCI
- Covers technical data rights, counterfeit part avoidance, cost accounting, and supply chain integrity.
- Mandatory flow-down: Primes must ensure subcontractors comply with requirements for cybersecurity and sourcing









What Changed?

Topic	Pre-publication	Post-publication
Core clauses in play	DFARS 7012 , 7019 , 7020 (safeguarding, SPRS score + assessment methodology). No 7025. 7021 existed but wasn't the active CMMC engine.	New provision 252.204-7025 (notice of level) + updated clause 252.204-7021 (CMMC compliance).
Award Gate	Award eligibility tied to current NIST 800-171 assessment score in SPRS .	Award/option requires current CMMC status at the specified level and annual affirmation in SPRS .
Status "currency" windows	N/A for CMMC (no enforced CMMC status windows).	Final L1: 1 yr; Final L2/L3: 3 yrs; Conditional L2/L3: ≤180 days; affirmation ≤1 yr.
Conditional Status	N/A	Conditional (L2/L3) certification allowed up to 180 days. Must close POA&M to reach Final certification
CMMC UID	No concept	Contractors must list 10-char CMMC UID(s) per in-scope info system
SPRS Postings	Post NIST 800-171 assessment summary score; no CMMC affirmation	
Phase-in	No phase-in	3 year phase-in
Flowdown, Supplier Checks	Flowdown of 7012/7019/7020, no way for primes to view subs CMMC status or SPRS	Flow down 7021; prime must ensure subs have current required CMMC status ; subs may share

CMMC Unlocked





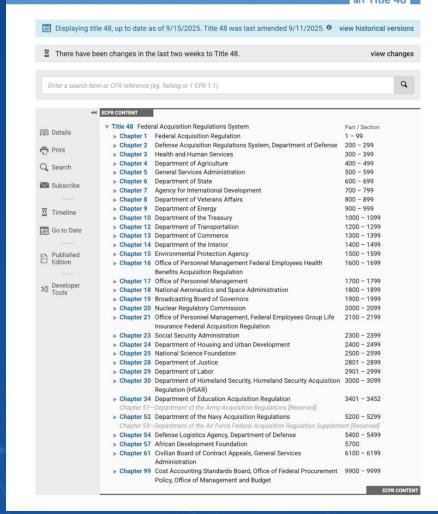


What is New?

- Effective Date: November 10th, 2025
- Clarifications: Newly clarified definitions, FCI, CMMC Status, CMMC UID, current
- Conditional statuses allowed: Up to 180 days with a valid POA&M; award can proceed. (Level 2-3)
- Flowdown Reaffirmed: Supplier checks
- Award gate: No award, option, or PoP extension unless the current required CMMC status and current annual affirmation are in SPRS for each in-scope system.



iii\ Title 49











SPRS Score

Supplier Performance Risk System

- An SPRS score is a numeric summary of your organization's implementation of NIST SP 800-171 using the DoW Assessment Methodology
- CMMC assessment results flow into SPRS and are used pre-award to verify you meet the required level
- Primes must confirm that subs have current SPRS scores on file before award
 - Level 1 within 1 year
 - Level 2/3 within 3 years
 - 180 days if Conditional











What Contractors Should know

- **CMMC UIDs:** You must provide 10 character UIDs for each in-scope information system, COs will check SPRS by UID, and you must report UID changes during performance.
- SPRS postings & affirmations: Post self-assessment results for each UID not covered by a C3PAO/DIBCAC assessment and complete an annual "affirming official" affirmation per UID.
- Flowdown & supplier checks: Flow down the clause when subs process/store/transmit FCI/CUI and ensure subs have a current CMMC status prior to subaward; subs must post their self-assessments and annual affirmations in SPRS.
- **Prime visibility limits:** Primes cannot view a subcontractor's SPRS CMMC record; subs may share screenshots/printouts to prove status.
- Scope & exclusions: Applies to unclassified contractor information systems that process/store/transmit FCI or CUI; DoD only; COTS excluded (but applies to commercial items/services).
- Phased roll-in: DFARS clause prescription reflects a phased implementation—watch solicitations for the required level and plan accordingly.









CMMC Assessments

Get Assessed, Get Compliant, Win Contracts







Types of CMMC Assessments

- Self-Assessment (Level 1 and 2)
- Mock Assessment
- Level 2 C3PAO Assessment
- Level 3 (DIBCAC) Assessment













The Assessment

It's an interview/review 320 objectives (questions)!

Includes:

- Compliance with 110 controls
- 72-hour incident reporting to the DoW
- Cooperation with DoW investigations
- Requires strong systems, processes, and training
- It's a full-company effort. (You cannot simply throw the program to your IT guy to figure out.)
- Assessors are also looking for *muscle-memory* that these practices are truly implemented.











The Urgency of CMMC Certification





It's active and required for defense contracts.



CMMC Gatekeeping

Certification determines contract eligibility for award and competitiveness.



C3PAOs are booking out months in advance.

Delays could mean lost opportunities for contractors.









Getting Ahead of the Rule

What Contractors Can Do Now







What C3PAOs Are Seeing









Waitlisting

A growing backlog of companies seeking assessments

Underestimated Workload

Many OSCs underestimate the time and steps to prepare for their assessment

Larger Scope Than Expected

The assessment is more rigorous and detailed than many expect (Not a "IT" thing)

Requirement Expectations

Many primes are beginning to require certification from their subs









What To Do Now



Post Your SPRS Score

Update your applicable "self" level 1 & 2 assessment results in SPRS



Plan POA&Ms

Closeouts to finish with 180 days, and schedule your assessment



Scrutinize Your Supply Chain

Require subs handling FCI/CUI to have a posted status in SPRS pre-award



Be Prepared! This could roll out faster than expected









Q&A









THANKYOU





