

# CMMC CONNECT

---

Jan 2024

CMMC CONNECT

## WELCOME

- We are glad you're here!
- Ask your questions live or submit them in the Q&A
- Replay shared within 48 hours
- Feedback survey

**CMMC CONNECT**  
**YOUR TEAM**



**Dr. Thomas Graham**

CCP, CCA, CMMC Instructor  
VP, CISO



**Tara Lemieux**

CCP, CCA, CMMC Instructor  
CMMC Consultant



**Jeremy Mares**

VP, Sales  
Federal Accounts – CMMC

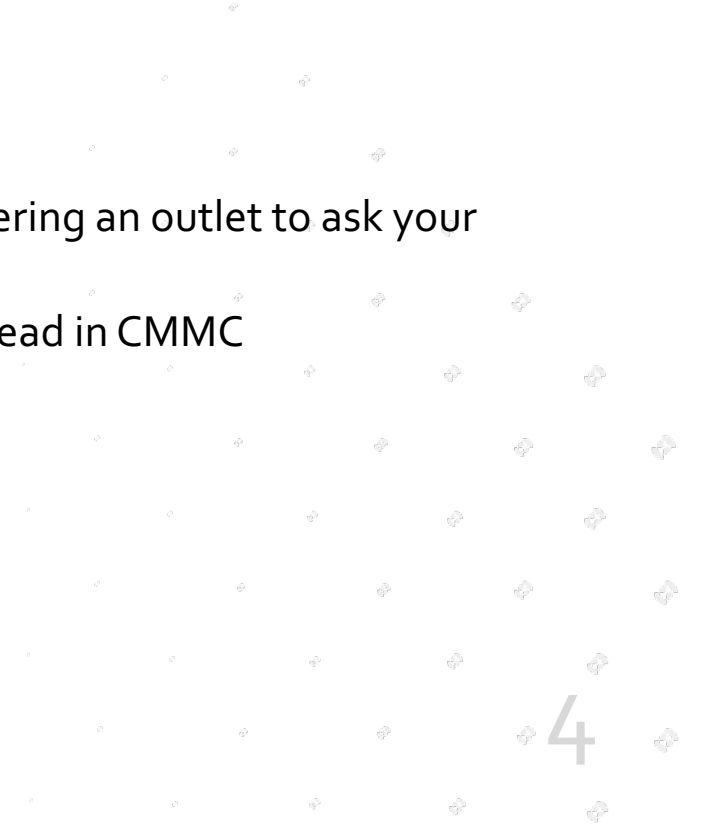


**Robert Teague**

CCA, CCP  
Director, CMMC Services



**CMMC CONNECT**  
**PURPOSE**

- For contractors to connect, interact, and learn from SMEs and each other
  - To cultivate an environment for casual + open CMMC discussions
  - To help you stay regularly informed about the latest CMMC developments, offering an outlet to ask your questions unique to your organization
  - To deepen your understanding, contribute to community building, and stay ahead in CMMC
- 

## CMMC Proposed Rule Overview

---

# THE CMMC PROPOSED RULE: IN A NUTSHELL



The new CMMC rule applies to **all** contractors within the Defense Industrial Base (DIB) – including, subcontractors, vendors, external service providers (ESPs), managed service providers (MSPs), managed security service providers (MSSPs) – who handle Federal Contract Information (FCI), Controlled Unclassified Information (CUI).



A proposed timeline has been established; this timeline addresses when the DoD expects to see the required **CMMC acquisition language** in ALL contracts. It does **not** extend or provide additional time for the organization to validate compliance.



Organizations **must demonstrate** continual compliance through a combination of self-assessments and certified third-party assessments (through authorized C3PAO).



Failure to comply **WILL** impact your contracting status.

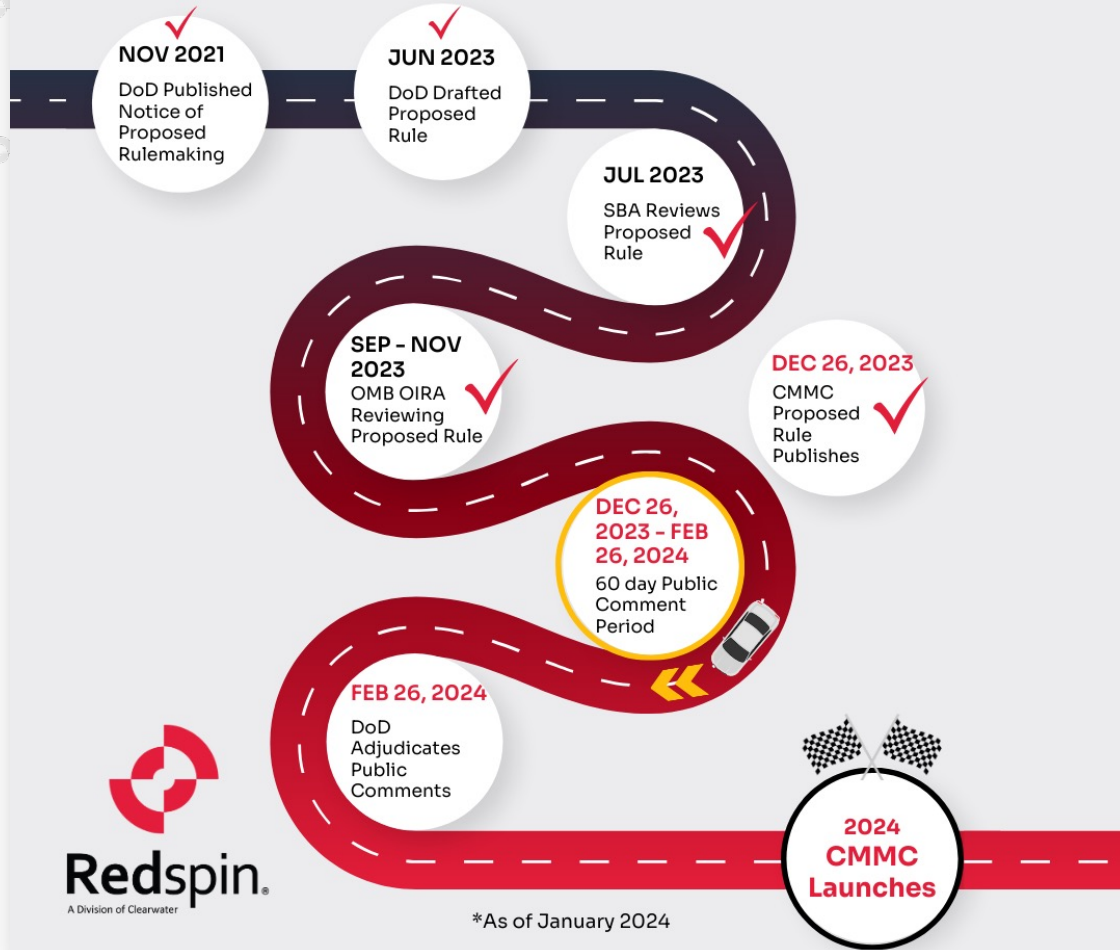
CMMC CONNECT

## LEGISLATIVE CHANGES

**The CMMC Rule Released:** The Cybersecurity Maturity Model Certification (CMMC) proposed rule was released on December 26, 2023, introducing significant changes and refinements to the CMMC Program.

- The primary focus of this legislation is to ensure defense contractors and subcontractors **comply** with information protection requirements for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
- Establishes Prime **accountability** for validation of cybersecurity flow down requirements to subcontractors, vendors, and service providers
- Proposes a **phased implementation** of CMMC requirements adding verbiage to all related acquisitions by 2026.

## CMMC Estimated Rulemaking Timeline & Projections



### CMMC CONNECT

## ESTIMATED TIMELINE

- The rule will be implemented in **four phases**, gradually increasing the requirement and number of contracts that include CMMC assessment stipulations.
- **Immediate compliance is required**, and will be evidenced through self-assessments, external 3rd party assessments, and government led assessments.
- The rule will apply to ALL contracts and subcontracts that require the contractor to process, store, or transmit CUI/FCI on contractor information systems, including commercial item contracts (exception COTS).
- Phased implementation will span 3 years with the expectation that the CMMC acquisition requirements for Levels 1, 2, and 3 will be included in ALL solicitations by October 2026.



CMMC CONNECT

# THE CMMC CYCLE

YEAR 1

## INITIAL SELF-ASSESSMENT AND SPRS ENTRY/UPDATE

- Determine Target CMMC Level
- Conduct a comprehensive self-assessment against NIST SP 800-171 r2
- Record and/or update assessment scores within the Supplier Performance Risk System (SPRS).

YEAR 2

## CONTINUOUS SELF-ASSESSMENT AND SPRS MONITORING

- Regularly review and update CMMC compliance status
- Ensure ongoing accuracy of data entered into SPRS; record any relevant security changes.

YEAR 3

## C3PAO/GOVERNMENT LED FORMAL CERTIFICATION

- Participate in a formal assessment conducted by a Certified Third-Party Assessment Organization (C3PAO) or Government Entity.
- Comply with all evaluation criterion and assessment procedures.

You could be asked to provide proof of certification by a Prime or a DoD contract. *-This would require a C3PAO.*

**CMMC PROPOSED APPROACH REVIEWS**

## **CMMC LEVEL 1 ASSESSMENT FOCUS**

- Level 1 compliance in the CMMC framework is often referred to as 'Basic Cyber Hygiene' and involves implementing the 15 basic cybersecurity controls outlined in FAR 52.204-21. These controls are designed to protect FCI and focus on safeguarding information systems against the most common cyber threats.
- Serves as an entry point for contractors in the Defense Industrial Base (DIB) and requires that the contractor provide for basic protections, including but not limited to: regular data backups, regular change of password, training, installation and updates to AV software and more.
- At level 1, organizations are required to conduct a SELF ASSESSMENT against the 17 CMMC Practices outlined in the CMMC L1 Assessment Guide.

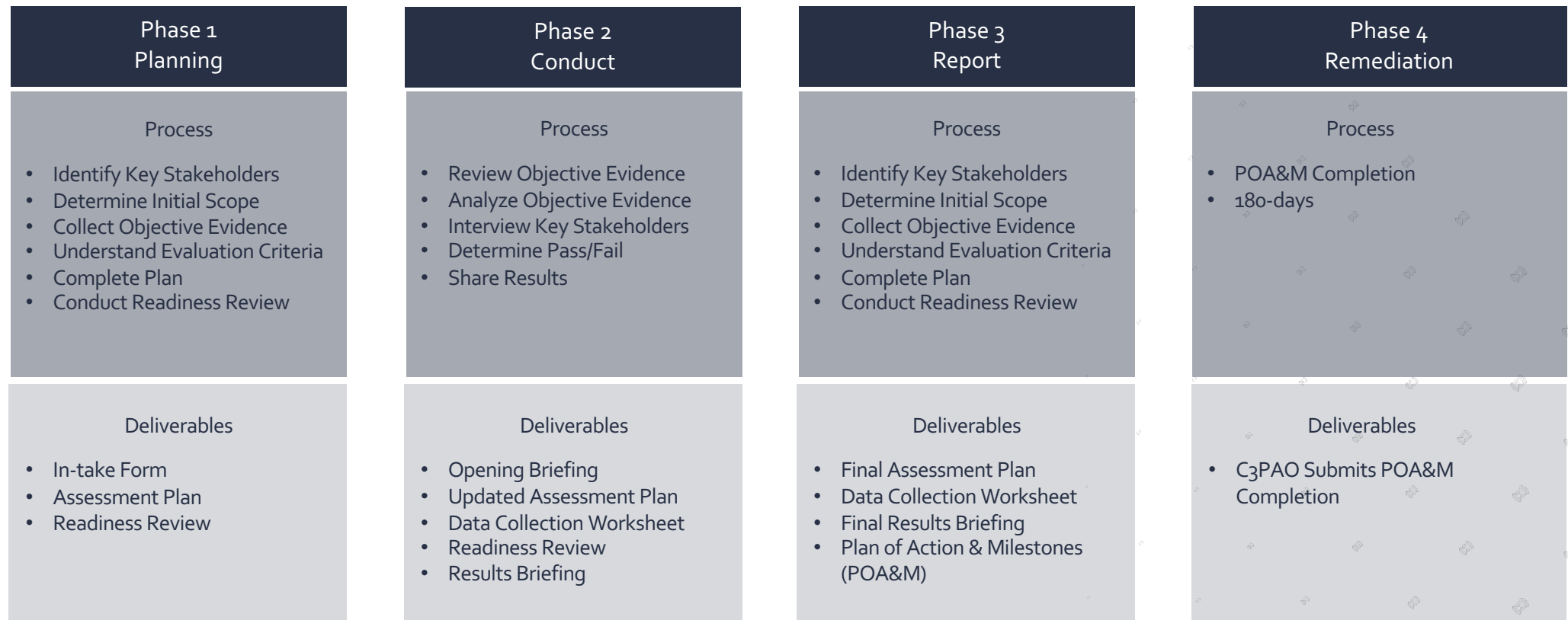
**CMMC PROPOSED APPROACH REVIEW**

## **CMMC LEVEL 2 ASSESSMENT FOCUS**

- Aligned with the 14 control families and 110 practices within NIST SP 800-171 using the CMMC Assessment Methodology outlined for CMMC L2 certifications
- Acts as a training tool for staff to prepare for certification assessment interview sessions
- Plan of Action & Milestones (POA&M) is allowed
  - Remediation guidance will be provided for each item in the POA&M
  - Provides accurate assessment of compliant practices and procedures
  - Also details a clear roadmap to full compliance and a 110 score
- Would require a **triennial C<sub>3</sub>PAO Certification Assessment**, with **annual Self Assessments**.

CMMC CONNECT

# CMMC LEVEL 2 CERTIFICATION ASSESSMENT PROCESS



CMMC PROPOSED APPROACH REVIEW

## CMMC LEVEL 3 ASSESSMENT FOCUS

- For CMMC Level 3, when CMMC becomes a final rule, contractors and applicable subcontractors will be required to implement the 24 selected security requirements from NIST SP 800–172, as detailed in table 1 to § 170.14(c)(4). CMMC Level 2 is a prerequisite for CMMC Level 3.
- Adds a requirement for contractors and applicable subcontractors to **verify through DoD assessment** and receive certification that all applicable CMMC Level 3 security requirements from NIST SP 800–172 have been implemented.
- **Selected requirements** are allowed to have a POA&M that must be closed out within 180 days of the assessment
- **Requires a CMMC L2 certification prior to engaging the CMMC L3 assessment process.**

## ARE YOUR VENDORS AND SUBCONTRACTORS COMPLIANT?

- **Mandatory Compliance for Subcontractors:**
  - Every subcontractor must meet CMMC requirements relevant to their level of data access.
  - Non-compliance in the supply chain can lead to vulnerabilities in our national defense
- **Assessing Subcontractors' Cybersecurity Posture**
  - Conduct thorough evaluations of your subcontractors' cybersecurity practices; note that many Prime contractors are already taking definitive action
  - Implement continuous monitoring of subcontractor compliance
  - Identify and address weak links in the supply chain to prevent data breaches; regularly update cybersecurity measures.
- **Impacts on Contracting Opportunities**
  - Non-compliant subcontractors can disqualify your firm from Defense contracts.

## CONTINUOUS COMPLIANCE

- CMMC isn't a 'one and done' certification; it requires ongoing adherence to cybersecurity practices and periodic reassessments
  - Regularly update and maintain cybersecurity measures; employ continuous monitoring and management of cyber risks.
- Periodic Reassessments
  - Mandatory reassessment every three years for certification maintenance and renewal.
  - Contractor must remain compliant with evolving legislation, standards, and practices accordingly.
- Documentation and Reporting:
  - Maintain comprehensive records of cybersecurity practices and incidents (add Incident Reporting link)
  - Regularly review and update cybersecurity policies and procedures.

**Remember: Your vigilance protects our nation and our warfighters.**

## Open Q&A

---

“CMMC, LIFE, THE UNIVERSE, AND EVERYTHING...”



# ASK US ANYTHING!

REDSPIN'S CMMC CONNECT, JANUARY 2024



**Dr. Thomas Graham**

CCP, CCA, CMMC Instructor  
VP, CISO

[linkedin.com/in/tgrahamphd/](https://www.linkedin.com/in/tgrahamphd/)



**Tara Lemieux**

CCP, CCA, CMMC Instructor  
CMMC Consultant

[linkedin.com/in/tara-lemieux-4385781/](https://www.linkedin.com/in/tara-lemieux-4385781/)



**Jeremy Mares**

VP, Sales  
Federal Accounts - CMMC

<https://www.linkedin.com/in/jeremy-mares-redspin/>



**Robert Teague**

CCA, CCP  
Director, CMMC Services

<https://www.linkedin.com/in/robert-j-teague-mba-cmmc-ca-cmmc-cp-113151a8/>



**We are here to help.**

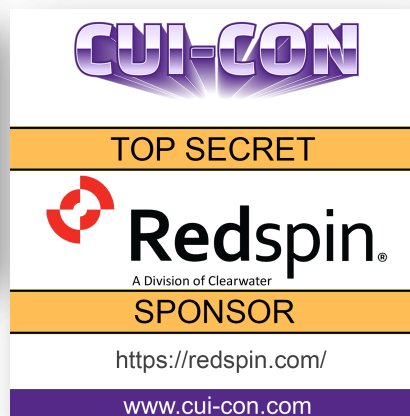
*Moving federal contractors to a more secure, compliant, and resilient state in order to better validate the security of the federal supply chain.*

## UPCOMING EVENTS



### AFECA's WEST 2024 | Feb 13-15 | San Diego, CA

Visit us at booth #1720, near the main entrance!



### CUI – CON | Feb 22-23 | Orlando, FL

Stop by our exhibiting table, and make sure to catch our speaking session "What Happens After We Are Certified?"



### CMMC Connect | Feb 29

We will be back next month. Same format, new/pressing questions, 30-minute session! Registration required.



### CIC 2024 | Mar 13-15

Our experts are lined up for a few speaking sessions and we are looking forward to staying ahead of CMMC with this in-person 2-day conference!



A Division of Clearwater

[www.Redspin.com](http://www.Redspin.com)

[CMMC Resources >](#)

888.907.3335

info@Redspin.com

[LinkedIn.com/company/redspin-inc](https://www.linkedin.com/company/redspin-inc)

