Conquering CMMC: Staying Compliant and Competitive

Presented by:

Steve Gilmer, Director Cybersecurity, Technology Risk & Privacy, CohnReznick

Daryouche Behboudi, Director Cybersecurity, Technology Risk & Privacy, CohnReznick

Meet Your Presenters

CohnReznick

Steve Gilmer

Director, Cybersecurity, Technology Risk and Privacy

CohnReznick Advisory, LLC

Daryouche Behboudi

Director, Cybersecurity, Technology Risk and Privacy

CohnReznick Advisory, LLC

Contents

Topic 1	Controlled Unclassified Information (CUI)
Topic 2	CMMC Overview
Topic 3	CMMC/C3PAO Services
Topic 4	Assessments

Scoping CUI

Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
Assets that are in the CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	- Assets that process, store, or transmit CUI	- Document in the asset inventory - Document in the System Security Plan (SSP) - Document in the network diagram of the CMMC Assessment Scope - Prepare to be assessed against CMMC practices	- Assess against CMMC Practices, including SPAs
Security Protection Assets	- Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI		
Contractor Risk Managed Assets	- Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place - Assets are not required to be physically or logically separated from CUI assets	- Document in the asset inventory - Document in the SSP ○ Show these assets are managed using the contractor's risk-based security policies, procedures, and practices - Document in the network diagram of the CMMC Assessment Scope	- Review the SSP in accordance with practice CA.L2-3.12.4 ○ If appropriately documented, do not assess against other CMMC practices ○ If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks ○ The limited spot check(s) shall not materially increase the assessment duration nor the assessment cost ○ The limited spot check(s) will be within the defined assessment scope
Specialized Assets	- Assets that may or may not process, store, or transmit CUI - Assets include government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment		- Review the SSP in accordance with practice CA.L2-3.12.4 - Do not assess against other CMMC practices

What is CMMC?

- The Cybersecurity Maturity Model Certification (CMMC) is cybersecurity compliance framework currently applicable to organizations with contracts with the U.S. Department of Defense.
  - Defense Industrial Base (DIB) estimated at over 200,000 organizations
  - Contractors are in a wide variety of industries
- Scope of the framework is to protect Federal Contract Information (FCI) including Controlled Unclassified Information (CUI).
  - Extremely broad categories of information
  - Information sensitive to DoD, but doesn’t rise to the level of “classified”
- Assessments are performed by credentialed assessment companies called Certified 3rd Party Assessor Organizations (C3PAO)
  - Cyber Accreditation Body (Cyber AB) credentials assessors and consultants in concert with DoD

CMMC Rules: CFR32

The CMMC rule, 32 CFR Part 170, eCFR :: 32 CFR Part 170 -- Cybersecurity Maturity Model Certification (CMMC) Program which establishes the CMMC Program went into effect on December 16th, 2024:

- Establishes and defines the roles and responsibilities of the CMMC ecosystem:
  - CyberAB as the accreditation body
  - Certified Third-Party Assessor Organizations (C3PAOs) as independent third parties that are authorized by the CyberAB to conduct assessment
  - Other members of the ecosystem: training organizations and publishers
  - Defines the three levels of CMMC
- It does not impose any requirements on the Defense Industrial Base (DIB)

CMMC Rules: CFR48

- The rule, 48 CFR Parts 204, 212, 217, and 252, Federal Register : Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041) went into effect 11/16/2025, which:
  - Imposes the requirements to meet the appropriate level of CMMC controls on the DIB
  - Directs the DoD contracting officers to verify in SPRS, prior to awarding a contract, exercising an option or when new DoD UIDs (CAGE code) are provided, that the results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, are posted in SPRS.
  - Changes the references to NIST 800-171 to CMMC 2.0
  - Includes a new DFARS provision, 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, to provide notice to offerors of the CMMC level required by the solicitation and of the CMMC certificate or self-assessment results that are required to have been posted in SPRS by the apparently successful offeror prior to award, unless electronically posted. It also requires the offeror provide the CMMC UID[1] issued by SPRS for each contractor information system that will process, store, or transmit FCI or CUI during performance of a contract, task order, or delivery order resulting from this solicitation.

[1] *"Cybersecurity Maturity Model Certification unique identifier (CMMC UID)means 10 alpha-numeric characters assigned to each CMMC assessment and reflected in the Supplier Performance Risk System (SPRS) for each contractor information system."*

A Forward Look at CMMC

CMMC requirements will be rolled out in 4 phases:

- **Phase 1 (Current):** Immediately upon publication, contractors must self-assess and affirm their compliance with CMMC Level 1 and 2 security controls when bidding for new contracts.
- **Phase 2 (11/10/2026):** This phase will start 1-year after Phase 1. Relevant contracts will require contractors to obtain a CMMC Level 2 certification obtained from a C3PAO to be able to be awarded contracts involving Controlled Unclassified Information (CUI).
- **Phase 3 (mid 2027-late 2027):** Contracts requiring advanced cybersecurity requirements will require CMMC L3 certification. The certification will only be granted as a result of an assessment conducted by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessors.
- **Phase 4 (2028):** Program fully implemented. CMMC Requirements are included in all DoD contracts, extensions and amendments.

The above phases are general guidelines. DoD Contract Officers can seek permission to include the CMMC requirements ahead of timeline as soon as the CFR 48 rule goes into effect. The same is true of the prime contractors. The flow-down requirements are already in effect.

The Four Levels of CMMC Assessments

CMMC Level	Scope	Method of Assessment	No. Controls/Objectives
1	FCI	Self-Assessment	15/59
2	CUI (Other OIGs)	Self-Assessment if the OSA[2] does not hold a clearance. Otherwise, C3PAO.	110/320
2	CUI from the following OIG[1]s: • Defense • Critical Infrastructure • Export Controlled Or DoD documentation with a distribution statement of C or D	C3PAO Assessment	110/320
3	CUIs in the second row requiring a higher level of safeguarding	Prerequisite is a C3PAO assessed Level 2 certification. DIBCAC[3] will assess the level 3 controls	24 additional controls

(1) OIG: Organizational Index Grouping
(2) OSA: Organization Seeking Assessment
(3) DIBCAC: Defense Industrial Base Cybersecurity Assessment Center

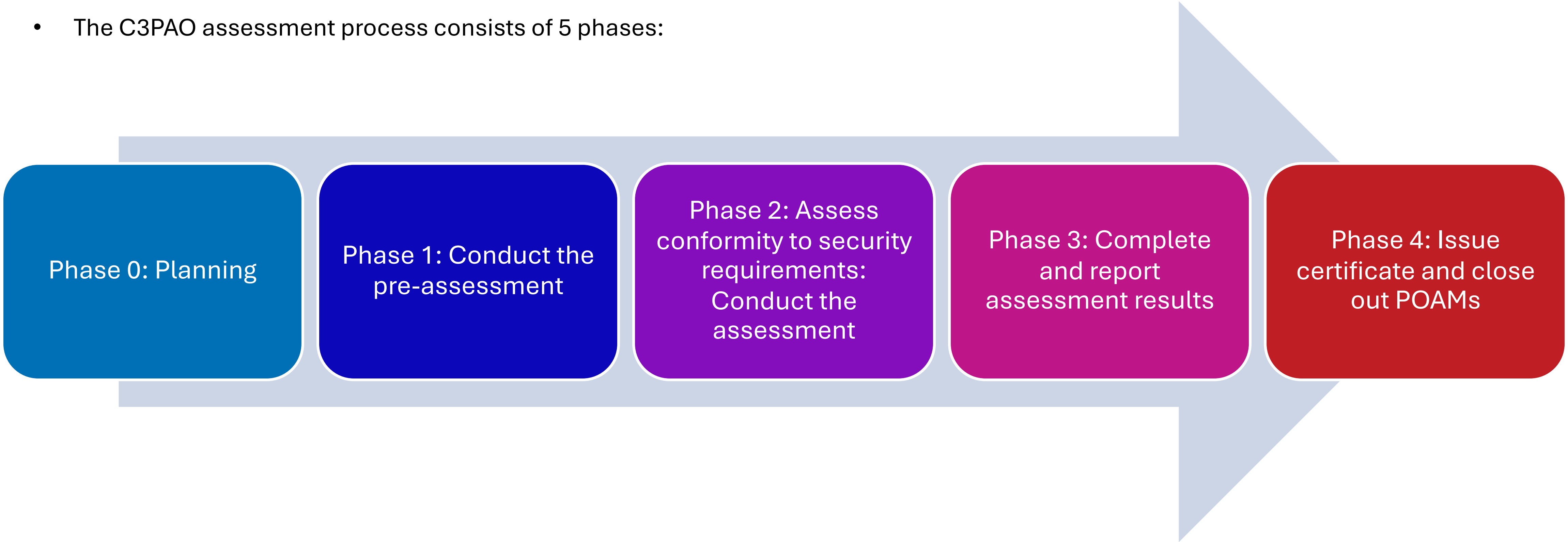
CMMC C3PAO and RPO Services

CohnReznick has been approved by the CMMC Accreditation Body (CyberAB) as both a C3PAO and an RPO. Both designations allow CohnReznick to help Department of Defense (DOD) contractors on their unique journey toward CMMC compliance. CohnReznick passed its second Certified 3rd Party Assessor Organization (C3PAO) assessment conducted by the DIBCAC on May 7, 2025.

CMMC Third-Party Assessment Organization (C3PAO) Services		Registered Provider Organization (RPO) Services	
CMMC assessment will be conducted not by the U.S. government but by Certified Assessors sponsored by C3PAOs, independent organizations approved and accredited by the CyberAB. C3PAOs must complete an accreditation process and an approved training and must show independence in their work.		The RPO certification acknowledges that CohnReznick is familiar with the basic constructs of the CMMC Standard and can deliver non-certified CMMC consulting services. As an RPO, we can guide and prepare organizations toward their desired level of CMMC maturity.	
CohnReznick C3PAO services THE CYBER AB CMMC CERTIFICATION AUTHORIZED C3PAO	• Sponsoring CMMC assessments: Engage Certified Assessors ("Provisional Assessors" during the program rollout period), perform assessment, review the quality of assessments, and submit assessment results to the CyberAB for approval • Project-managing the assessment process	**CohnReznick RPO services** THE CYBER AB CMMC CERTIFICATION REGISTERED PRACTITIONER ORGANIZATION RPO	• Consulting services to help companies prepare for CMMC assessments • Training and coaching on CMMC assessments • Tools and templates to help prepare for the assessment

C3PAO Assessment

- The C3PAO assessment process consists of 5 phases:



Phase 0: Planning

Phase 1: Conduct the pre-assessment

Phase 2: Assess conformity to security requirements: Conduct the assessment

Phase 3: Complete and report assessment results

Phase 4: Issue certificate and close out POAMs

Frequently Asked Questions

- I do not know how to scope the assessment.

Follow the data. That is why the CUI flow diagram is important. It helps you define your system boundary.

- CMMC Level 2 is too onerous for my organizations risk profile.

It is not your risk profile that is important. The risk profile is DoD's.

- It is too difficult to implement.

CMMC L2 is based on standards first published in 12/31/2016 with a major revision on 2/21/2020. DIB members had over 8 years to implement the controls.

- I don't know if I have CUI

If your contract includes DFARS Clause 252.204-7012, you have obligated your organization to safeguard CUI.

- CUI Markings: Is non-CUI ever marked CUI? Can our IP be marked CUI to prevent FOIA discovery?

It is possible that items are mismarked as CUI, talk to your Contract Office or Prime if you suspect this; Something Proprietary should be Marked CUI//PROPIN (see NARA.gov for details on markings)

Major Reasons Why Assessments Fail?

- **Not being ready for the assessment:** Develop an assessment playbook which should include the name of individuals responsible for each control family and links to the relevant piece of evidence.
- **Poor credential management:** lack of MFA, accounts for employees that left still active, …
- **Improper cryptography:** Use of non FIPS compliant cryptographic modules/algorithms
- **Lack of continuous monitoring:** continuous monitoring plan not in place
- **Incomplete, inconsistent or outdated documentation:** SSP does not match policy, policy is a few years old, …
- **Incomplete inventories:** ESPs and CSPs missing, SPA is missing, no CRMA, no Specialized assets
- **Non-Compliant External Service Providers (ESPs: MSPs or MSSPs):** ESPs are not CMMC L2 certified, or they do not meet the requirements of the relevant control
- **Lack of Shared Responsibility Matrices with your CSPs or ESPs**.
- **Inadequate vulnerability management:** Lack of vulnerability management plan with well defined and risk informed SLAs.

Questions?

Steve Gilmer

Director, Cybersecurity, Technology Risk and Privacy

CohnReznick Advisory, LLC

Phone: 703-744-8539
Email: Steve.gilmer@cohnreznick.com

in linkedin.com/In/stevegilmer

Daryouche Behboudi

Director, Cybersecurity, Technology Risk and Privacy

CohnReznick Advisory, LLC

Phone: 703-744-8507
Email: Daryouche.Behboudi@cohnreznick.com

in linkedin.com/In/daryouchebehboudi

WWW.COHNREZNICK.COM