MMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RU

SUMMIT7 Live Webinar

CMMC Published: A Comprehensive Overview of the Proposed CMMC Rule

Jacob Horne
Chief Cybersecurity Evangelist

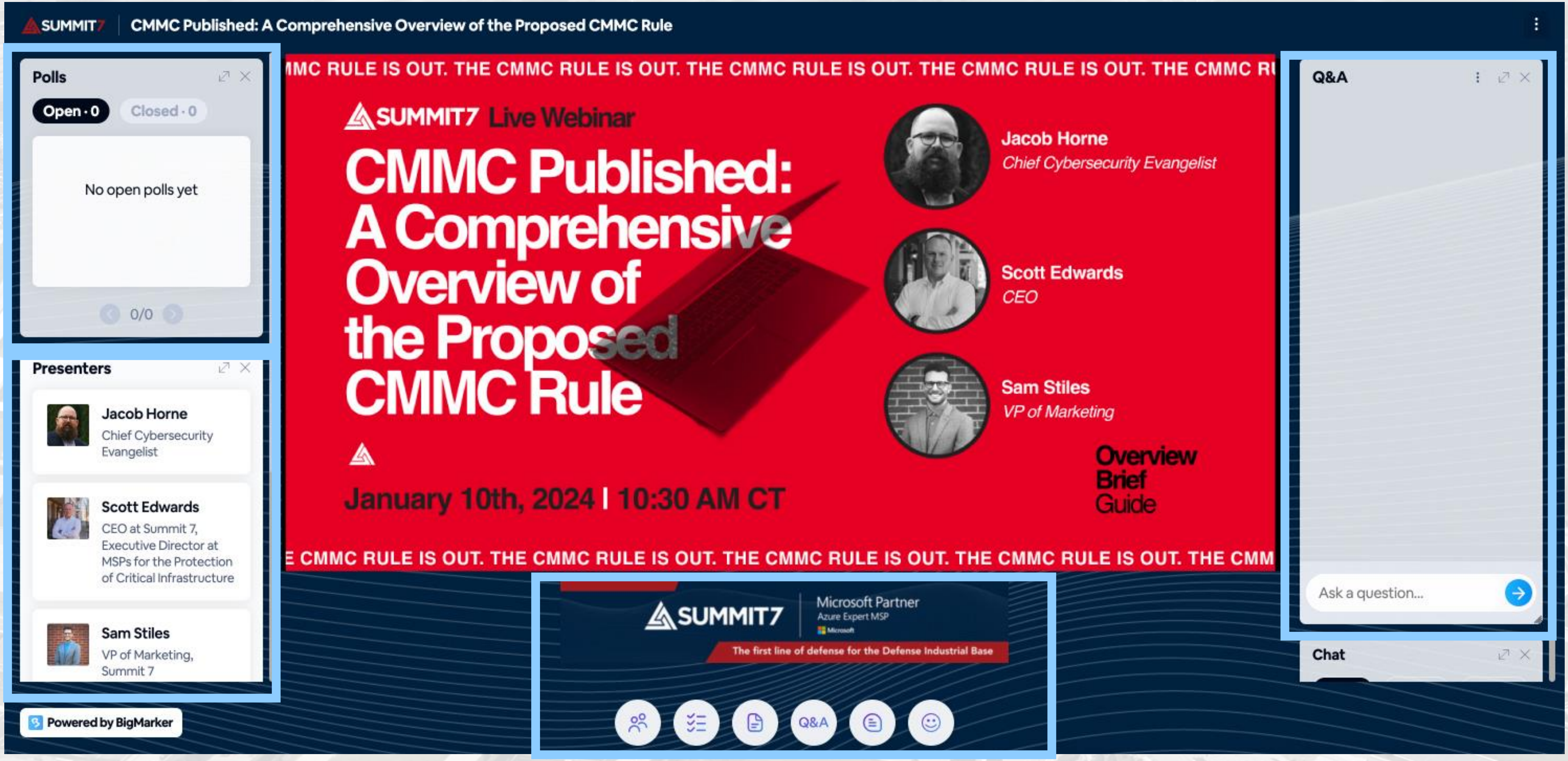
Scott Edwards
CEO

Sam Stiles
VP of Marketing

January 10th, 2024 | 10:30 AM CT

Overview
Brief
Guide

E CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMM



SUMMIT7 | CMMC Published: A Comprehensive Overview of the Proposed CMMC Rule

No open polls yet

Presenters

- **Jacob Horne** – Chief Cybersecurity Evangelist
- **Scott Edwards** – CEO at Summit 7, Executive Director at MSPs for the Protection of Critical Infrastructure
- **Sam Stiles** – VP of Marketing, Summit 7

MC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RU

SUMMIT7 Live Webinar

CMMC Published: A Comprehensive Overview of the Proposed CMMC Rule

January 10th, 2024 | 10:30 AM CT

Jacob Horne
Chief Cybersecurity Evangelist

Scott Edwards
CEO

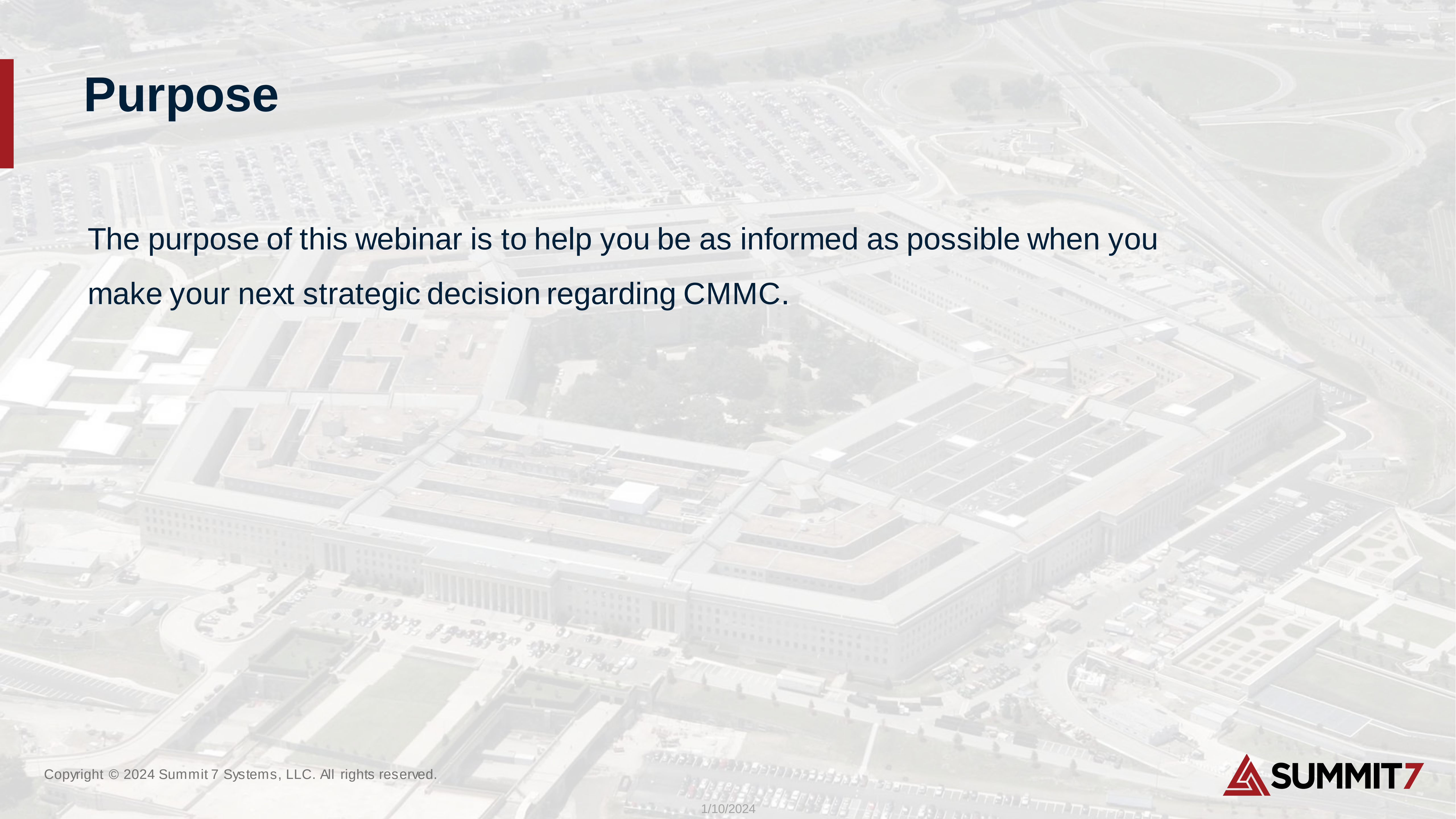
Sam Stiles
VP of Marketing

Overview Brief Guide

E CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMMC RULE IS OUT. THE CMM

SUMMIT7 | Microsoft Partner Azure Expert MSP Microsoft

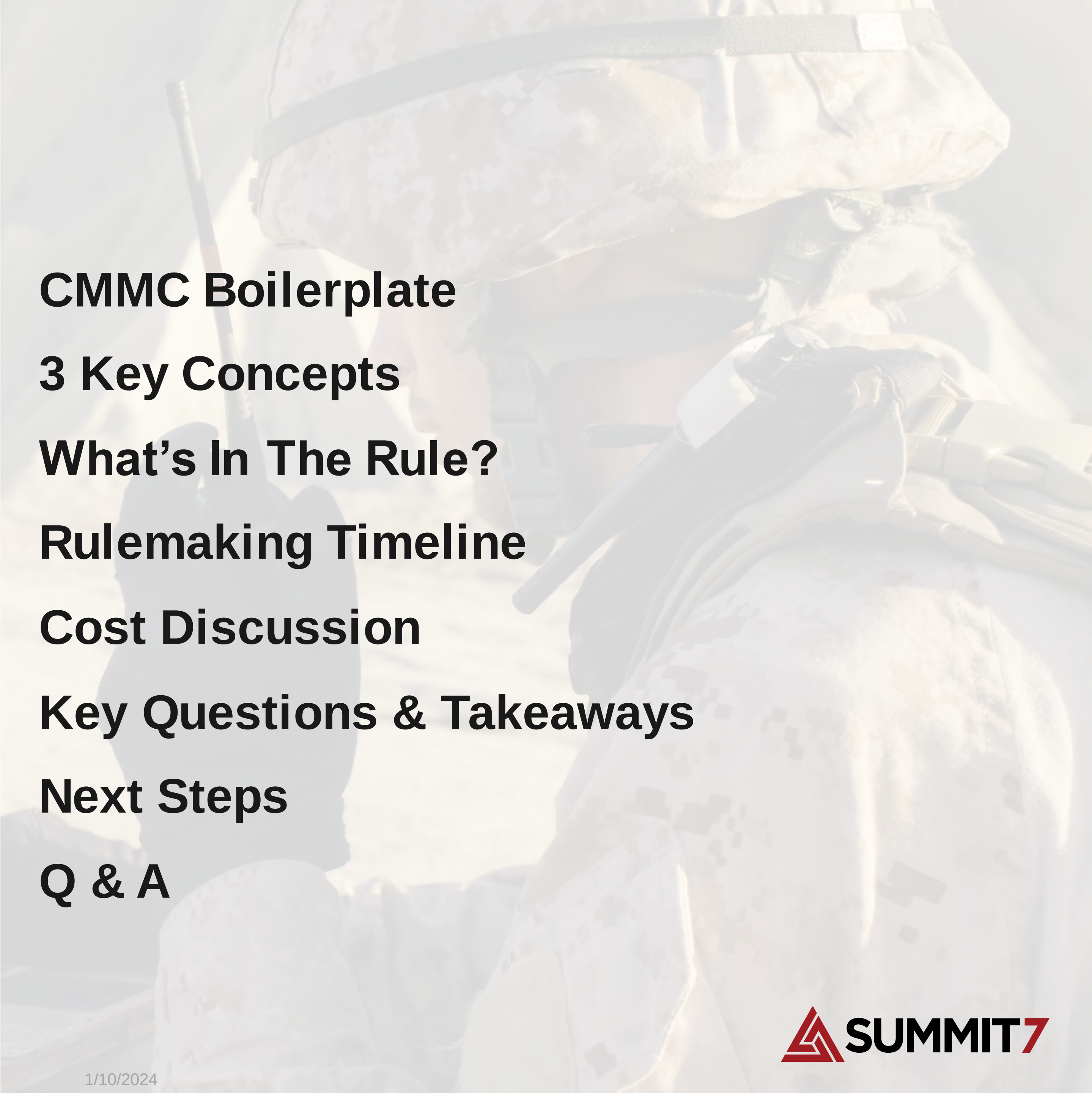
The first line of defense for the Defense Industrial Base



Purpose

The purpose of this webinar is to help you be as informed as possible when you make your next strategic decision regarding CMMC.

Agenda



- 01 CMMC Boilerplate
- 02 3 Key Concepts
- 03 What’s In The Rule?
- 04 Rulemaking Timeline
- 05 Cost Discussion
- 06 Key Questions & Takeaways
- 07 Next Steps
- 08 Q & A

On December 26th, 2023, the DoD published a proposed rule in the Federal Register outlining the CMMC 2.0 program

234 Pages

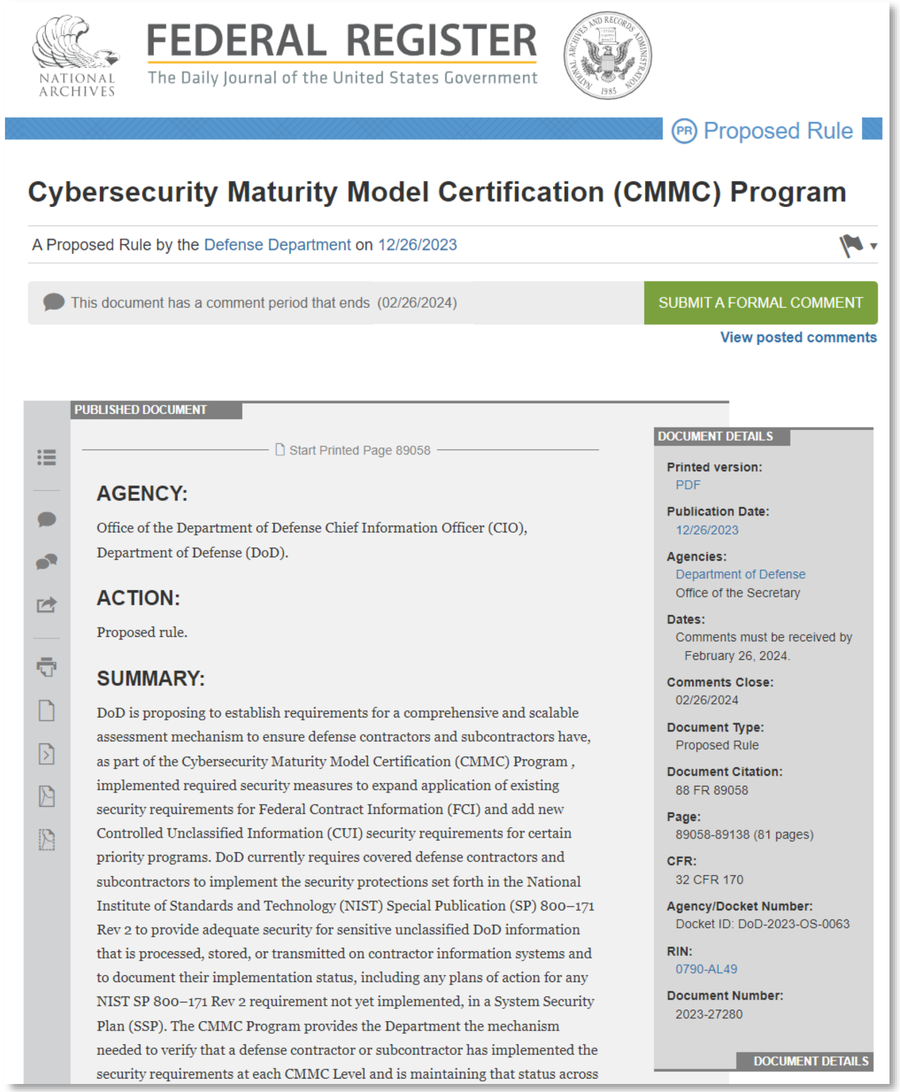
125 Acronyms & Definitions

67 footnotes

39 tables

16 standards incorporated by reference

9 guidance documents



Cybersecurity Maturity Model Certification (CMMC) Program

A Proposed Rule by the Defense Department on 12/26/2023

This document has a comment period that ends (02/26/2024)

Start Printed Page 89058

AGENCY:

Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD).

ACTION:

Proposed rule.

SUMMARY:

DoD is proposing to establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors have, as part of the Cybersecurity Maturity Model Certification (CMMC) Program , implemented required security measures to expand application of existing security requirements for Federal Contract Information (FCI) and add new Controlled Unclassified Information (CUI) security requirements for certain priority programs. DoD currently requires covered defense contractors and subcontractors to implement the security protections set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 Rev 2 to provide adequate security for sensitive unclassified DoD information that is processed, stored, or transmitted on contractor information systems and to document their implementation status, including any plans of action for any NIST SP 800–171 Rev 2 requirement not yet implemented, in a System Security Plan (SSP). The CMMC Program provides the Department the mechanism needed to verify that a defense contractor or subcontractor has implemented the security requirements at each CMMC Level and is maintaining that status across

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
12/26/2023

Agencies:
Department of Defense
Office of the Secretary

Dates:
Comments must be received by February 26, 2024.

Comments Close:
02/26/2024

Document Type:
Proposed Rule

Document Citation:
88 FR 89058

Page:
89058-89138 (81 pages)

CFR:
32 CFR 170

Agency/Docket Number:
Docket ID: DoD-2023-OS-0063

RIN:
0790-AL49

Document Number:
2023-27280

DoD needs assurance that contactor information systems are adequately secured to protect sensitive unclassified data; CMMC provides that mechanism

Policy issues addressed by CMMC:

Cyber Posture Verification

*"Current FAR and DFARS contract clauses **do not provide for DoD assessment and verification** of a defense contractor or subcontractor's implementation of the information protection requirements within those clauses **prior to contract award**."*

Close the POAM Loophole

*"At present, defense contractors and subcontractors can process, store, or transmit CUI **without having implemented all security requirements** set forth in NIST SP 800–171 Rev 2 and **without establishing concrete, prompt, and enforceable timelines** for addressing shortfalls and gaps documented in the Plan of Action."*

Advanced Persistent Threats (APT) Mitigation

*"**Existing requirements do not sufficiently address Advanced Persistent Threats** (APTs).*

CMMC Level 3 provides for government assessment of a contractor's implementation of a defined subset of NIST SP 800–172 Enhanced Security Requirements with DoD predefined parameters and specifications."

No Assessment Scalability

*"CMMC **addresses the Department's scaling challenges** by utilizing a private-sector accreditation structure.*

A DoD-authorized Accreditation Body will authorize, accredit, and provide oversight of C3PAOs which in turn will conduct CMMC Level 2 Certification Assessments of actual and prospective DoD contractors and subcontractors."

No Supply Chain Visibility

*"Today, DoD prime contractors must include DFARS clause 252.204–7012 in subcontracts for which performance will involve covered defense information, but **this does not provide the Department with sufficient insights** with respect to the cybersecurity posture of all members of a multi-tier supply chain for any given program or technology development effort."*

The goal of the CMMC program is to provide DoD with verification and assurance that cybersecurity requirements are being implemented by contractors and subcontractors

The CMMC Program has three key features:

3-Tiered Model

“There are three different levels of CMMC assessment, starting with basic safeguarding of FCI at Level 1, moving to the broad protection of CUI at Level 2, and culminating with higher level protection of CUI against risk from Advanced Persistent Threats (APTs) at Level 3.”

Assessment Requirement

“CMMC assessments allow the Department to implementation of cybersecurity requirements in DoD contracts and subcontracts, by assessing adequacy of contractor information system security compliance prior to award and during performance of the contract.”

Implementation through Contracts

With limited exceptions, the Department intends to require compliance with CMMC as a condition of contract award.”

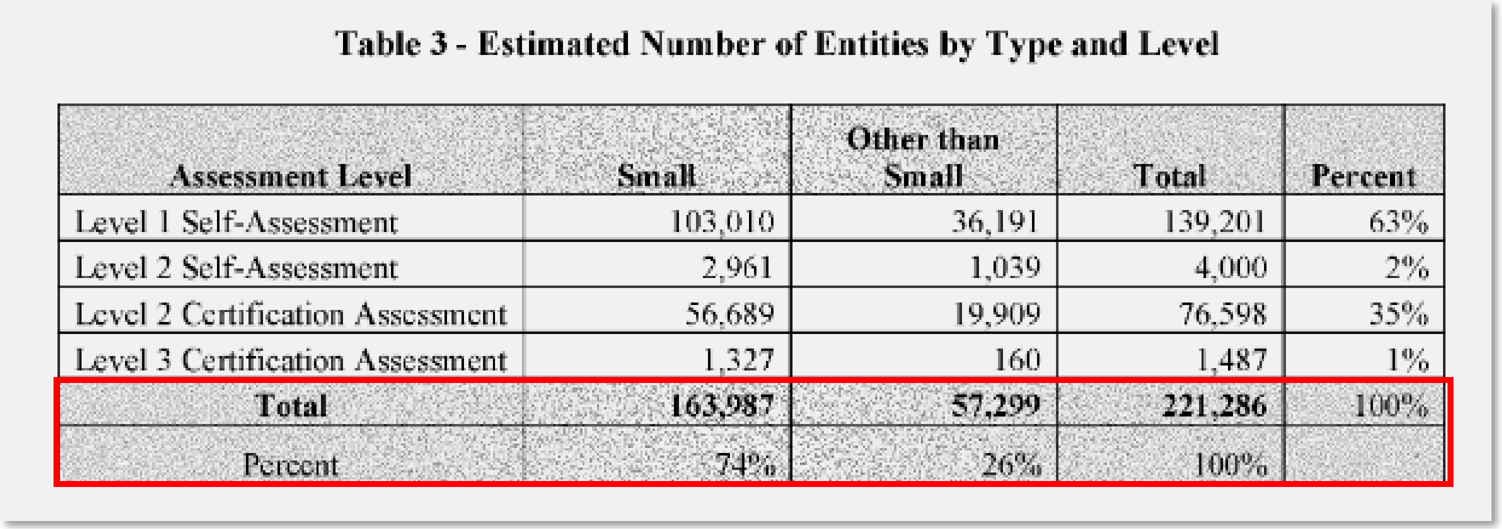


Table 3 - Estimated Number of Entities by Type and Level

Assessment Level	Small	Other than Small	Total	Percent
Level 1 Self-Assessment	103,010	36,191	139,201	63%
Level 2 Self-Assessment	2,961	1,039	4,000	2%
Level 2 Certification Assessment	56,689	19,909	76,598	35%
Level 3 Certification Assessment	1,327	160	1,487	1%
Total	**163,987**	**57,299**	**221,286**	100%
Percent	74%	26%	100%	

3 Key Concepts

3 Key Concepts allow us to unpack hundreds of pages in the proposed rule and understand almost any high-level CMMC conversation (rulemaking, preparation, etc.)

Why

The requirements assessed by CMMC are not imposed by CMMC

Important because it’s the reason why:

- CMMC estimates do not include the cost and time for implementation and maintenance, only assessment and affirmation.
- DoD says “you should have already implemented these requirements” 18 different times in the proposed rule.
- DoD has maintained the same rationale, justification, and policy basis for CMMC over time in the face of opposition, criticism, and trade-offs.

What

Security requirements have multiple corresponding verification procedures

Important because organizations often:

- Assess themselves incorrectly leading to a false sense of readiness.
- Make incorrect statements and attestations to customers and the government regarding their implementation.
- Surprised when vendors and solutions don’t facilitate as much of their compliance as marketing led them to believe.

When

This one codifies the overall program

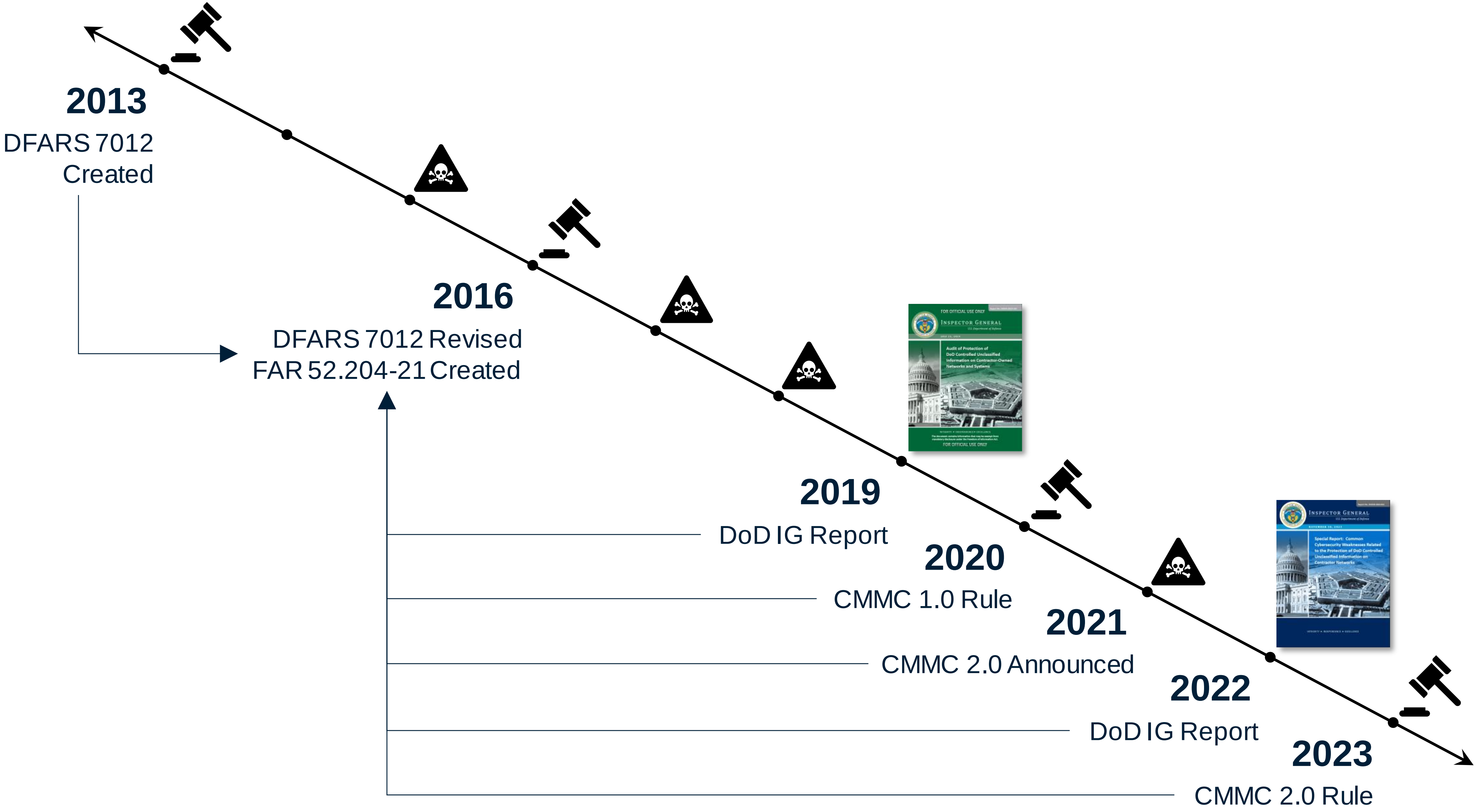
This one creates the contract clause

There are 2 different CMMC rules

Important because DoD roll-out estimates:

- Are unable to account for market forces outside of DoD’s control that will force contractors to achieve CMMC “early”.
- Focus on the roll-out of contract requirements rather than the demand shock of companies pursuing CMMC independently.
- Don’t attempt to estimate the time until both rules will be published as “final rules” and going into effect.

The requirements assessed by CMMC are not imposed by CMMC



2013
DFARS 7012
Created

2016
DFARS 7012 Revised
FAR 52.204-21 Created

2019
DoD IG Report

2020
CMMC 1.0 Rule

2021
CMMC 2.0 Announced

2022
DoD IG Report

2023
CMMC 2.0 Rule

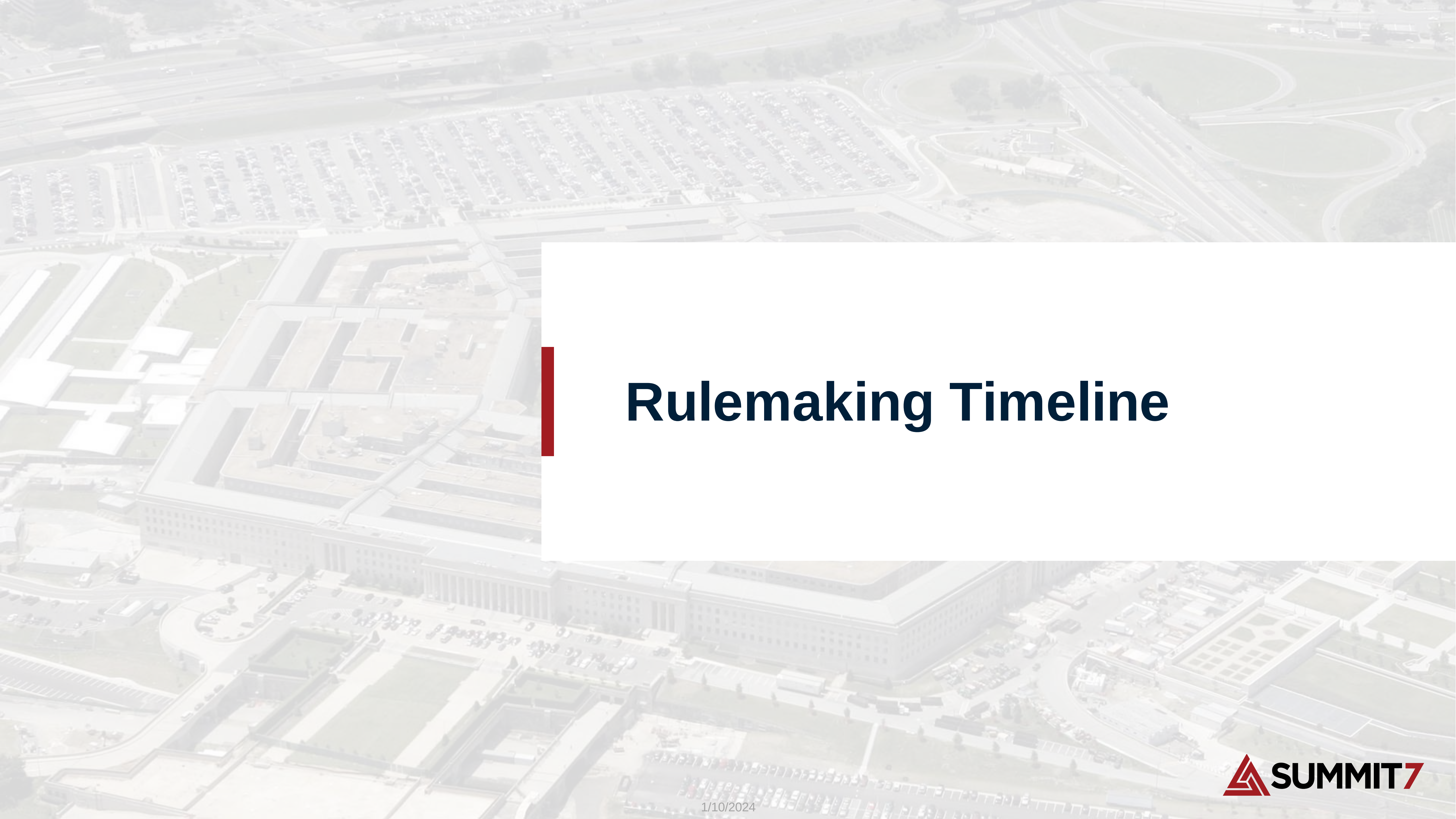
What’s in the rule

CMMC level requirements must be satisfied prior to contract award

	Self-Assessment		Certification Assessment	
	Level 1	**Level 2**	**Level 2**	**Level 3***
Requirement	15 requirements in FAR clause 52.204-21	110 requirements in NIST SP 800-171 **revision 2**	110 requirements in NIST SP 800-171 **revision 2**	24 requirements from NIST SP 800-172
Scoring[1]	**All requirements must be fully implemented**	"Fully implemented" requirements worth either 5, 3, or 1 point	"Fully implemented" requirements worth either 5, 3, or 1 point	"Fully implemented" requirements worth 1 point
Procedure	Verify 59 objectives via **SP 800-171A** Fully implemented: all objectives MET No open items: "Final Self-Assessment"	Verify 320 objectives via **SP 800-171A** Fully implemented: all objectives MET[2] No open items result in: "Final Self-Assessment"	Verify 320 objectives via **SP 800-171A** Fully implemented: all objectives MET[2] No open items result in: "Final Certification Assessment"	Verify 103 objectives via **SP 800-172A** Fully implemented: all objectives MET[2] No open items result in: "Final Certification Assessment"
POAMs	**No POAMs allowed**	Permissible open items[3]: "Conditional Self-Assessment" 180 days to close via self-assessment	Permissible open items[3]: "Conditional Certification Assessment" 180 days to close via C3PAO	Permissible open items[3]: "Conditional Certification Assessment" 180 days to close via DIBCAC
Assessment	Annual Results submitted to SPRS	Triennial (every 3 years) Results submitted to SPRS	Triennial (every 3 years) via C3PAO Results submitted to eMASS	Triennial (every 3 years) via DIBCAC Results submitted to eMASS
Affirmation	At each assessment and annually via senior company official	At each assessment and annually via senior company official	At each assessment and annually via senior company official	At each assessment and annually via senior company official
Scoping[4]	"Consider" External Service Providers (ESP) during assessment	ESPs must have L2 **final** cert	ESPs must have L2 **final** cert	ESPs must have L3 **final** cert

* Prerequisite: CMMC Level 2 Final Certification Assessment

1) See: §170.24 for scoring details
2) See: §170.16 – §170.18 for criteria
3) See: §170.21 for restrictions
4) See: §170.19



Rulemaking Timeline

CMMC is effective when the 32 CFR rule is published as a final rule; DoD’s phased roll-out begins when the 48 CFR rule is published as a final rule

CMMC “Program Rule”

“This rule establishes the CMMC Program and defines requirements both in general and based on the specific CMMC level and assessment type required by the contract and applicable subcontract.”

This rule codifies the program at Title 32 of the Code of Federal Regulations (CFR)

CMMC “Clause Rule”

“CMMC-related contractual processes will be addressed in DoD’s DFARS Case 2019-D041 which will be proposed by the Department in a separate rulemaking.”

This rule creates the corresponding CMMC contract clause at Title 48 CFR

DoD’s phased roll-out and yearly assessment estimates are based on the 48 CFR final rule rather than the 32 CFR final rule

◔

Phase 1

Begins on the effective date of the 48 CFR CMMC Rule*

Level 1 and Level 2 self-assessment requirements included in all applicable solicitations and contracts as a condition of award**

*DoD discretion: prior to effective date of 48 CFR CMMC

**DoD discretion: Level 2 certification in place of self-assess

◑

Phase 2

Begins 6 months after the start of Phase 1*

CMMC Level 2 certification in all applicable solicitations and contracts as condition of award**

*DoD discretion: delay inclusion of L2 certification to an option period instead of condition of award

**DoD discretion: Level 3 certification instead

◕

Phase 3

Begins 1 year after the start of Phase 2*

CMMC Level 2 certification in all applicable solicitations and contracts as condition of award or exercise of option period.

CMMC Level 3 certification* in all applicable solicitations and contracts as condition of award.

*DoD discretion: delay inclusion of L3 certification to an option period instead of condition of award

●

Phase 4

Begins 1 year after the start of Phase 3

CMMC in all applicable solicitations and contracts including options periods on contracts awarded prior to Phase 4.

The CMMC program will be live when the 32 CFR rule is final, nullifying the phased roll-out based on customer demand and other market forces

“Complicating factors” stemming from the CMMC program’s “free market influences to propel implementation.”

Companies may serve as a prime contractor on one effort but a subcontractor on others.

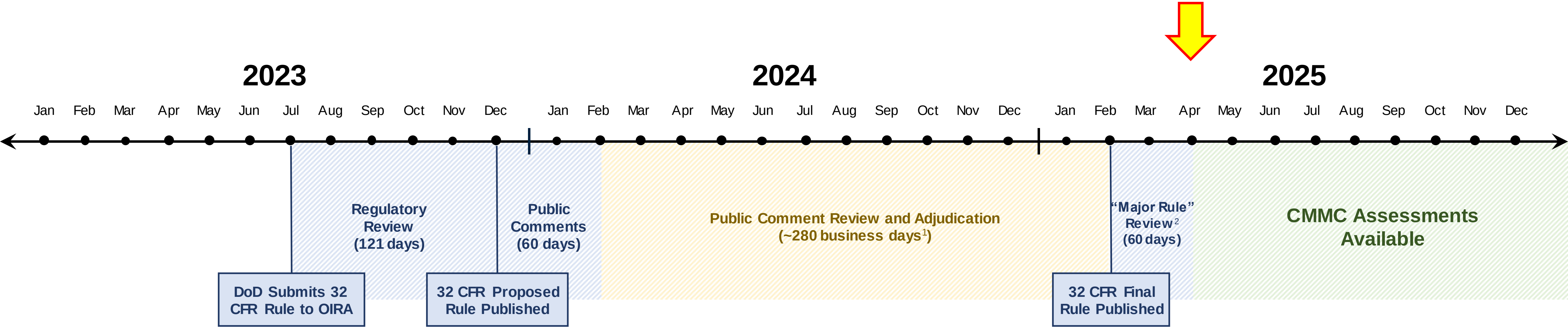
Companies may enter into subcontract agreements with more than one prime contractor for various opportunities.

The DoD does not control which defense contractors aspire to compete for which business opportunities.

The DoD does not control access to the assessment services offered by C3PAOs.

> ***“OSAs may elect to complete a self-assessment or pursue a certification assessment at any time after issuance of the rule in an effort to distinguish themselves as competitive for efforts that require an ability to adequately protect CUI.”***

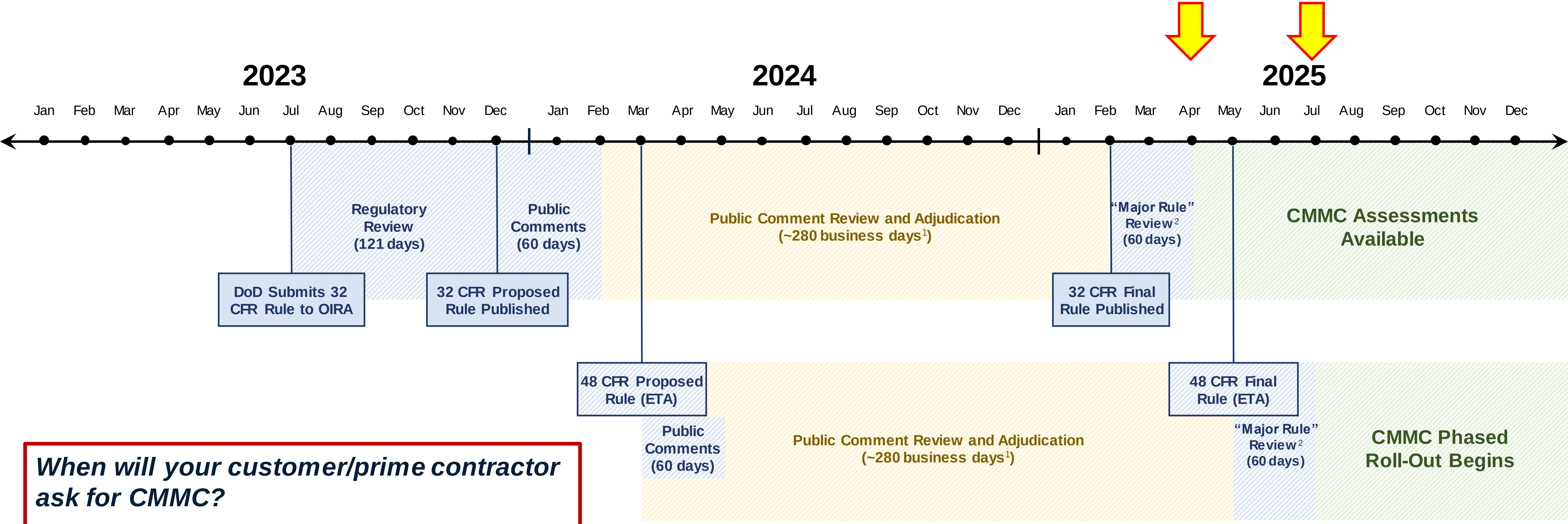
Actions of your customers and competitors regarding CMMC certifications after the final 32 CFR rule outweigh the start of DoD's "phased roll-out"


2023
2024
2025
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Regulatory Review (121 days)
Public Comments (60 days)
Public Comment Review and Adjudication (~280 business days[1])
"Major Rule" Review[2] (60 days)
CMMC Assessments Available
DoD Submits 32 CFR Rule to OIRA
32 CFR Proposed Rule Published
32 CFR Final Rule Published

[1] The 5% trimmed mean based on all DoD proposed rules 2009 - 2022.

[2] The Congressional Review Act (CRA) defines major rules as those that result in large effects on the economy, costs, competition, etc.

Actions of your customers and competitors regarding CMMC certifications outweigh the start of DoD's "phased roll-out"



2023

2024

2025

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

DoD Submits 32 CFR Rule to OIRA

Regulatory Review (121 days)

32 CFR Proposed Rule Published

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

32 CFR Final Rule Published

"Major Rule" Review[2] (60 days)

CMMC Assessments Available

48 CFR Proposed Rule (ETA)

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

48 CFR Final Rule (ETA)

"Major Rule" Review[2] (60 days)

CMMC Phased Roll-Out Begins

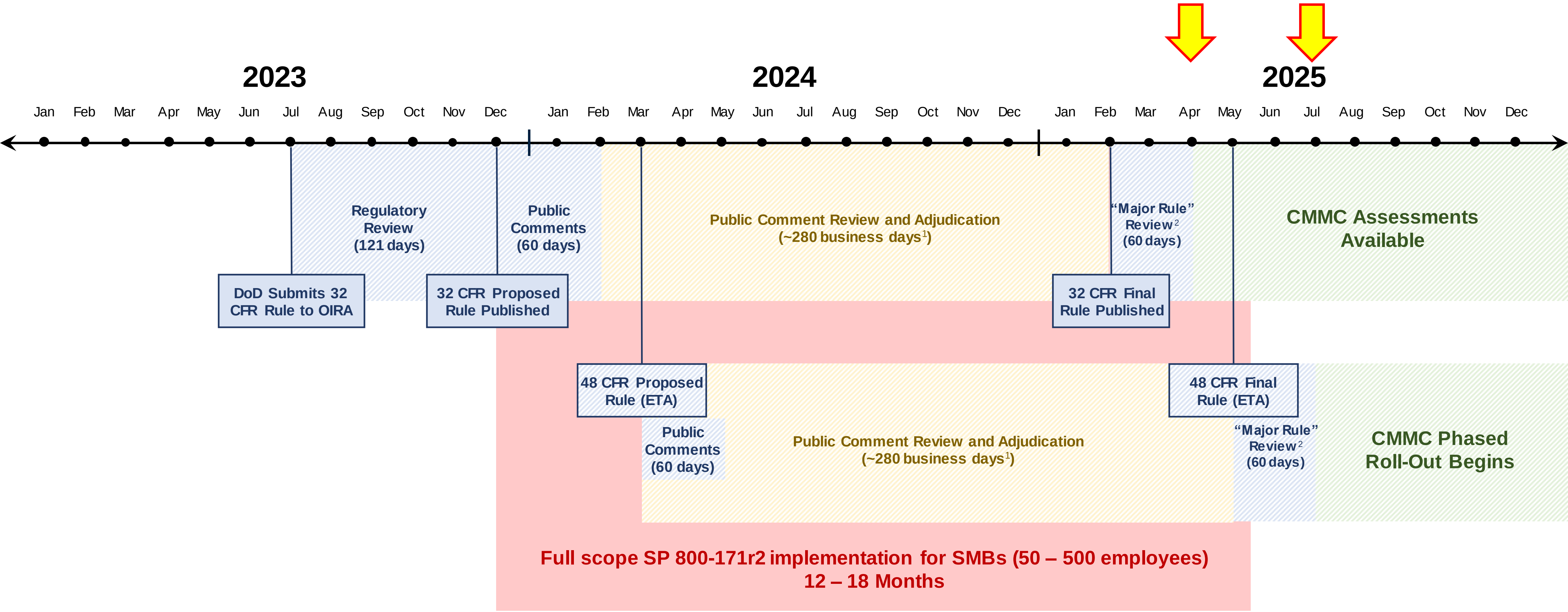
When will your customer/prime contractor ask for CMMC?

When will your competitors move to "distinguish themselves as competitive"?

1) The 5% trimmed mean based on all DoD proposed rules 2009 - 2022.

2) The Congressional Review Act (CRA) defines major rules as those that result in large effects on the economy, costs, competition, etc.

Average implementation extends beyond the estimated 32 CFR final rule


2023
2024
2025
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

DoD Submits 32 CFR Rule to OIRA

Regulatory Review (121 days)

32 CFR Proposed Rule Published

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

32 CFR Final Rule Published

"Major Rule" Review[2] (60 days)

CMMC Assessments Available

48 CFR Proposed Rule (ETA)

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

48 CFR Final Rule (ETA)

"Major Rule" Review[2] (60 days)

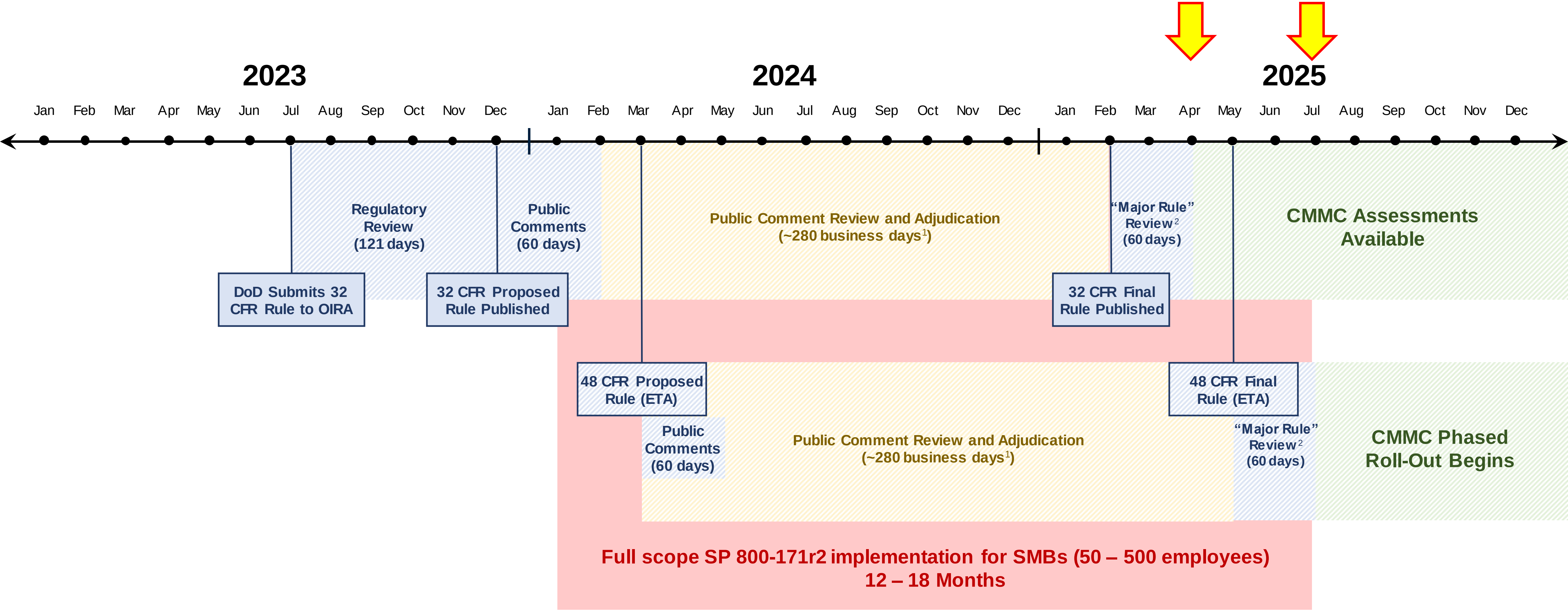
CMMC Phased Roll-Out Begins

Full scope SP 800-171r2 implementation for SMBs (50 – 500 employees)
12 – 18 Months

[1] The 5% trimmed mean based on all DoD proposed rules 2009 - 2022.

[2] The Congressional Review Act (CRA) defines major rules as those that result in large effects on the economy, costs, competition, etc.

Average implementation extends beyond the estimated 32 CFR final rule



2023
2024
2025
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

DoD Submits 32 CFR Rule to OIRA

Regulatory Review (121 days)

32 CFR Proposed Rule Published

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

32 CFR Final Rule Published

“Major Rule” Review[2] (60 days)

CMMC Assessments Available

48 CFR Proposed Rule (ETA)

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

48 CFR Final Rule (ETA)

“Major Rule” Review[2] (60 days)

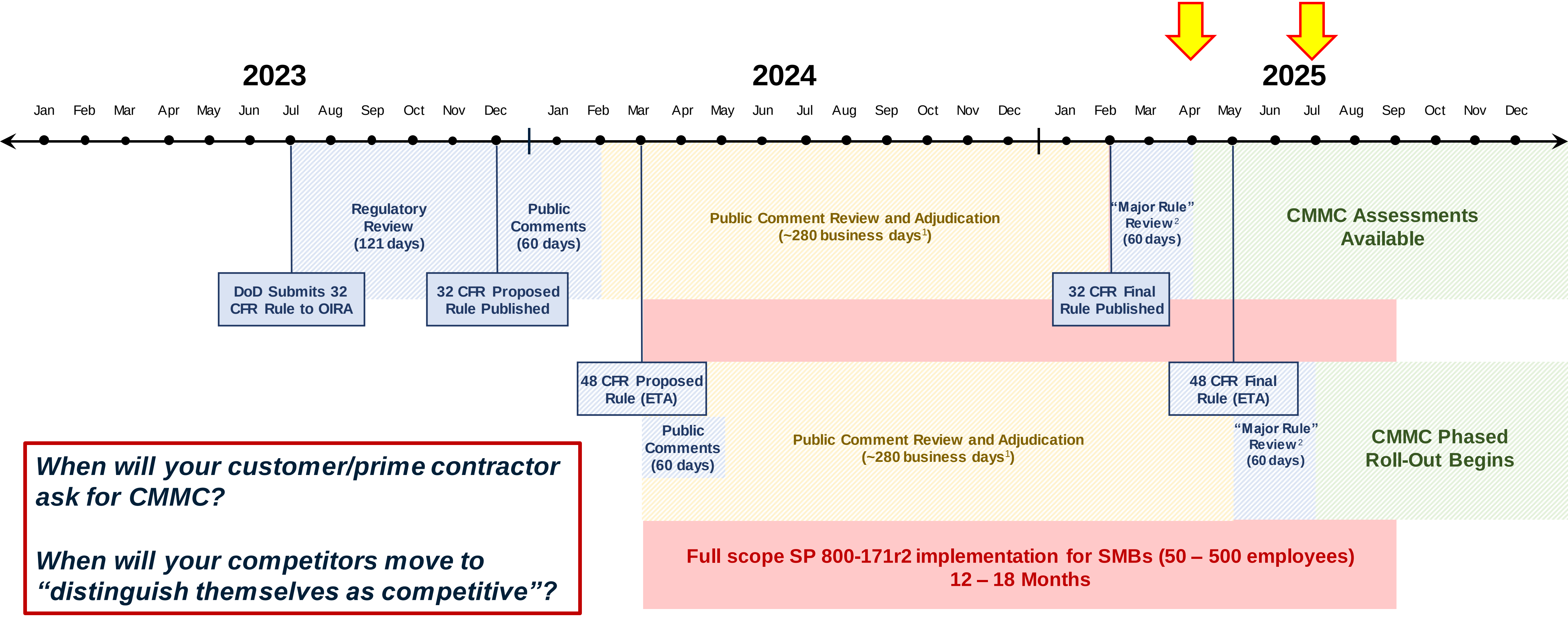
CMMC Phased Roll-Out Begins

Full scope SP 800-171r2 implementation for SMBs (50 – 500 employees)
12 – 18 Months

[1] The 5% trimmed mean based on all DoD proposed rules 2009 - 2022.

[2] The Congressional Review Act (CRA) defines major rules as those that result in large effects on the economy, costs, competition, etc.

Average implementation extends beyond the estimated 32 CFR final rule



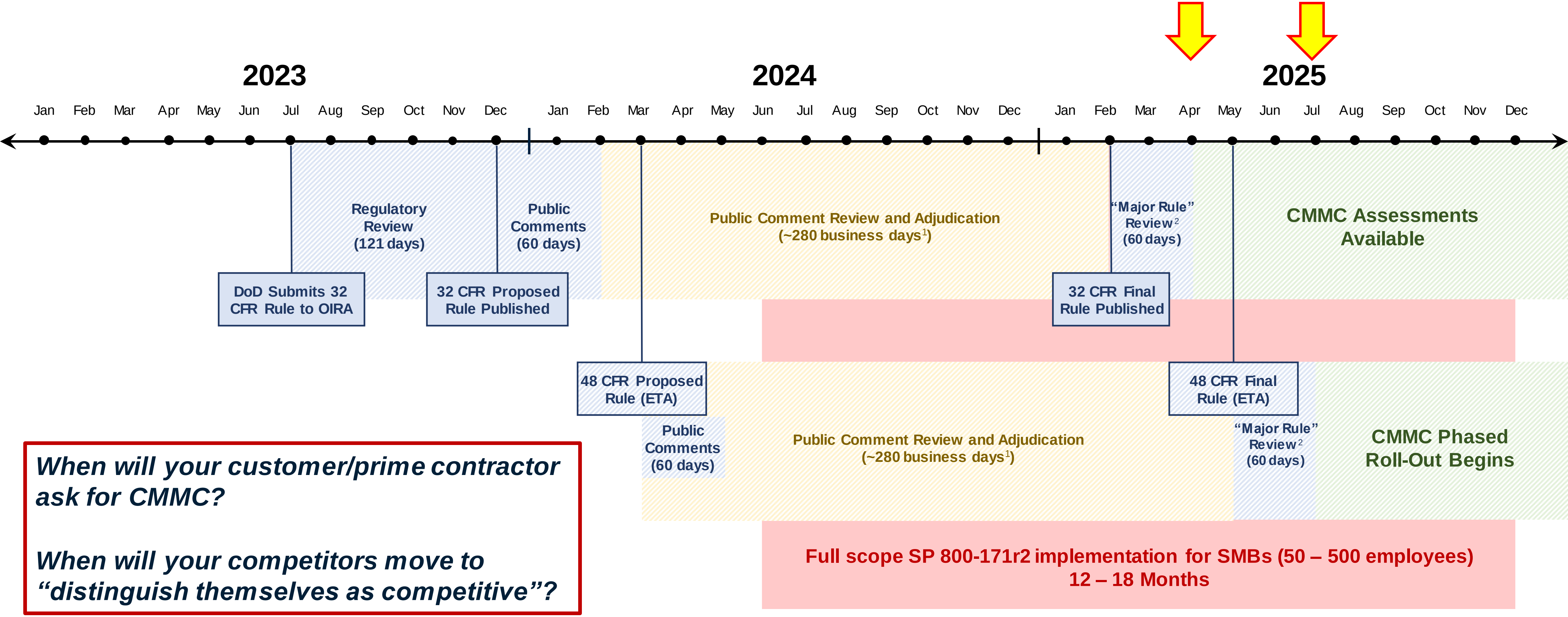
2023
2024
2025
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Regulatory Review (121 days)
Public Comments (60 days)
Public Comment Review and Adjudication (~280 business days1)
"Major Rule" Review2 (60 days)
CMMC Assessments Available
DoD Submits 32 CFR Rule to OIRA
32 CFR Proposed Rule Published
32 CFR Final Rule Published
48 CFR Proposed Rule (ETA)
48 CFR Final Rule (ETA)
Public Comments (60 days)
Public Comment Review and Adjudication (~280 business days1)
"Major Rule" Review2 (60 days)
CMMC Phased Roll-Out Begins
Full scope SP 800-171r2 implementation for SMBs (50 – 500 employees) 12 – 18 Months

When will your customer/prime contractor ask for CMMC?

When will your competitors move to "distinguish themselves as competitive"?

[1] The 5% trimmed mean based on all DoD proposed rules 2009 - 2022.
[2] The Congressional Review Act (CRA) defines major rules as those that result in large effects on the economy, costs, competition, etc.

Average implementation extends beyond the estimated 32 CFR final rule



2023
2024
2025
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

DoD Submits 32 CFR Rule to OIRA

Regulatory Review (121 days)

32 CFR Proposed Rule Published

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

32 CFR Final Rule Published

"Major Rule" Review[2] (60 days)

CMMC Assessments Available

48 CFR Proposed Rule (ETA)

Public Comments (60 days)

Public Comment Review and Adjudication (~280 business days[1])

48 CFR Final Rule (ETA)

"Major Rule" Review[2] (60 days)

CMMC Phased Roll-Out Begins

Full scope SP 800-171r2 implementation for SMBs (50 – 500 employees)
12 – 18 Months

When will your customer/prime contractor ask for CMMC?

When will your competitors move to "distinguish themselves as competitive"?

[1] The 5% trimmed mean based on all DoD proposed rules 2009 - 2022.
[2] The Congressional Review Act (CRA) defines major rules as those that result in large effects on the economy, costs, competition, etc.

Cost Discussion

The proposed rule divides costs into four categories; implementation and maintenance is only estimated for CMMC Level 3

Nonrecurring Engineering Costs (Implementation)

Hardware, software, and the labor to implement.

Assumes the requirements assessed at CMMC levels 1 and 2 have already been implemented.

Only appear in CMMC Level 3.

Recurring Engineering Costs (Maintenance)

Annual fees and labor for technology refresh.

Assumes the requirements assessed at CMMC levels 1 and 2 have already been implemented.

Only appear in CMMC Level 3.

Assessment Costs

Cost of the four notional phases of assessment.

Assumes the organization passes the assessment on the first attempt (conditional or final).

Affirmation Costs

Costs to submit affirmations to SPRS.

Includes initial and any subsequent affirmations (such as POAM closeout).

> *"Costs associated with implementing the requirements … are **assumed to have been already implemented** and, therefore, are not accounted for in this cost estimate."*

> *"The FAR and DFARS requirements for safeguarding FCI and CUI **predate the CMMC Program by many years**, and baseline costs for their implementation are assumed to vary widely based on factors including, but not limited to, company size and complexity of the information systems to be secured."*

CMMC is a six-figure problem

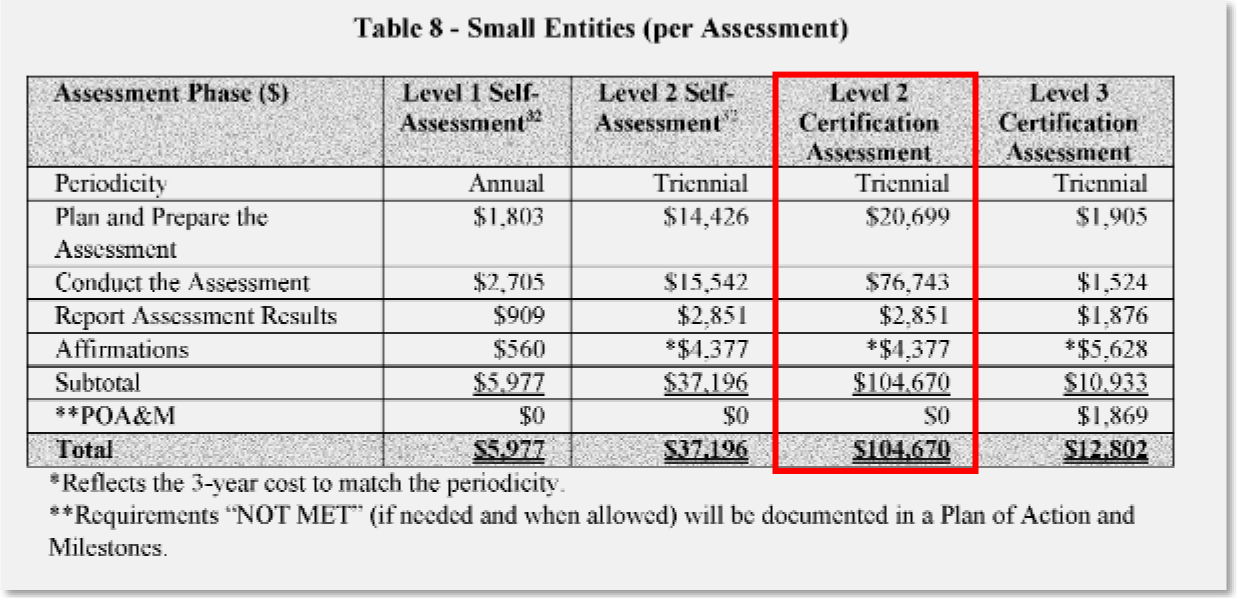


Table 8 - Small Entities (per Assessment)

Assessment Phase ($)	Level 1 Self-Assessment[32]	Level 2 Self-Assessment[33]	Level 2 Certification Assessment	Level 3 Certification Assessment
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,803	$14,426	$20,699	$1,905
Conduct the Assessment	$2,705	$15,542	$76,743	$1,524
Report Assessment Results	$909	$2,851	$2,851	$1,876
Affirmations	$560	*$4,377	*$4,377	*$5,628
Subtotal	$5,977	$37,196	$104,670	$10,933
**POA&M	$0	$0	$0	$1,869
Total	**$5,977**	**$37,196**	**$104,670**	**$12,802**

*Reflects the 3-year cost to match the periodicity.

**Requirements "NOT MET" (if needed and when allowed) will be documented in a Plan of Action and Milestones.

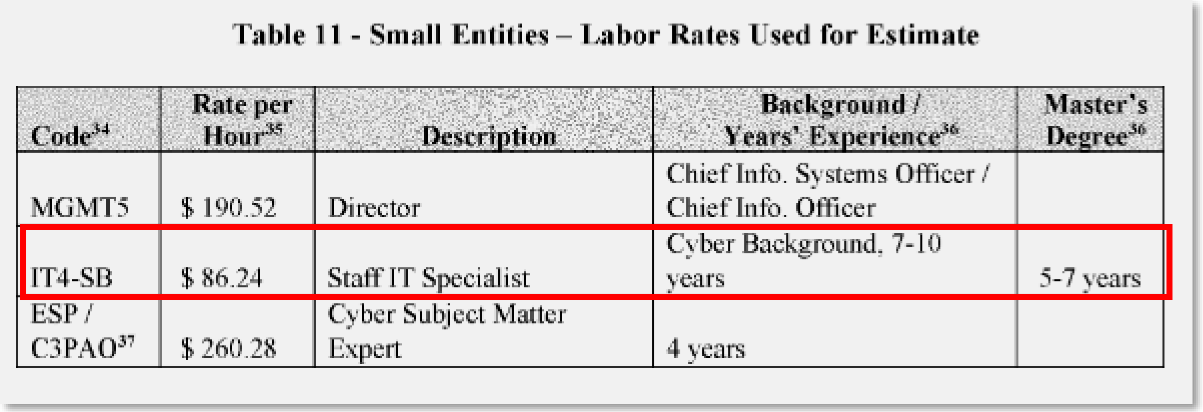
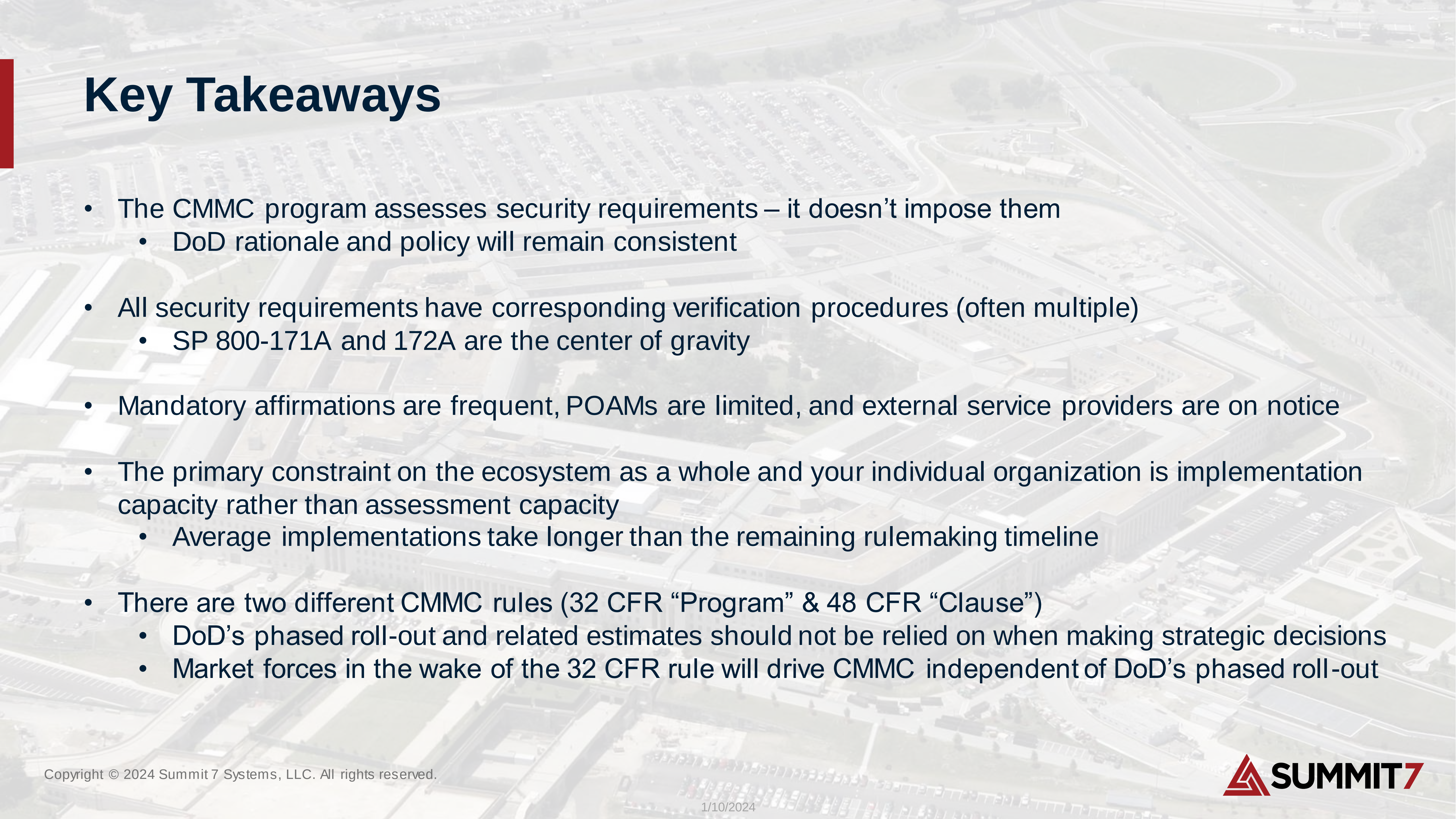


Table 11 - Small Entities – Labor Rates Used for Estimate

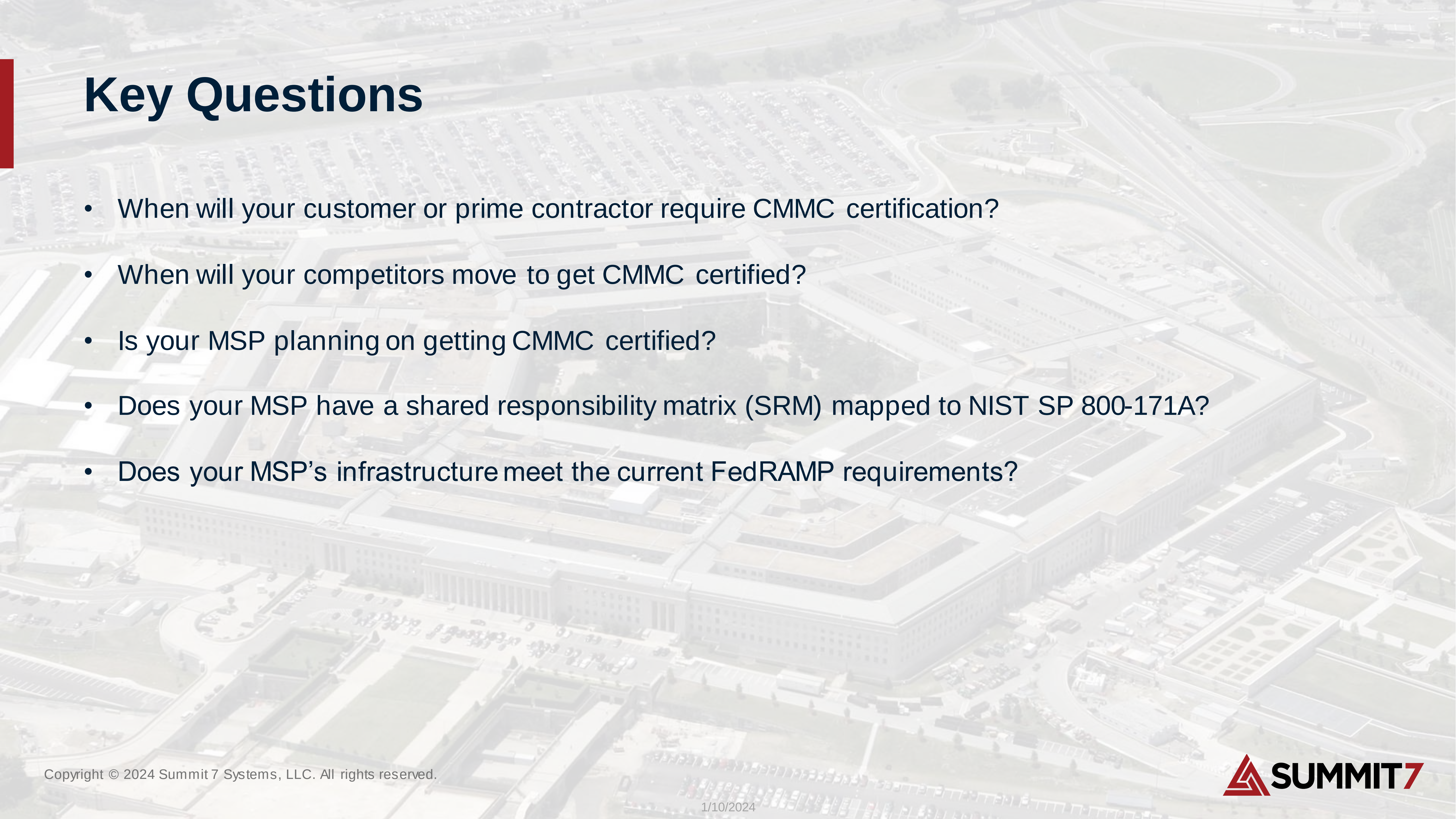
Code[34]	Rate per Hour[35]	Description	Background / Years' Experience[36]	Master's Degree[36]
MGMT5	$ 190.52	Director	Chief Info. Systems Officer / Chief Info. Officer	
IT4-SB	$ 86.24	Staff IT Specialist	Cyber Background, 7-10 years	5-7 years
ESP / C3PAO[37]	$ 260.28	Cyber Subject Matter Expert	4 years	

Key Takeaways & Questions



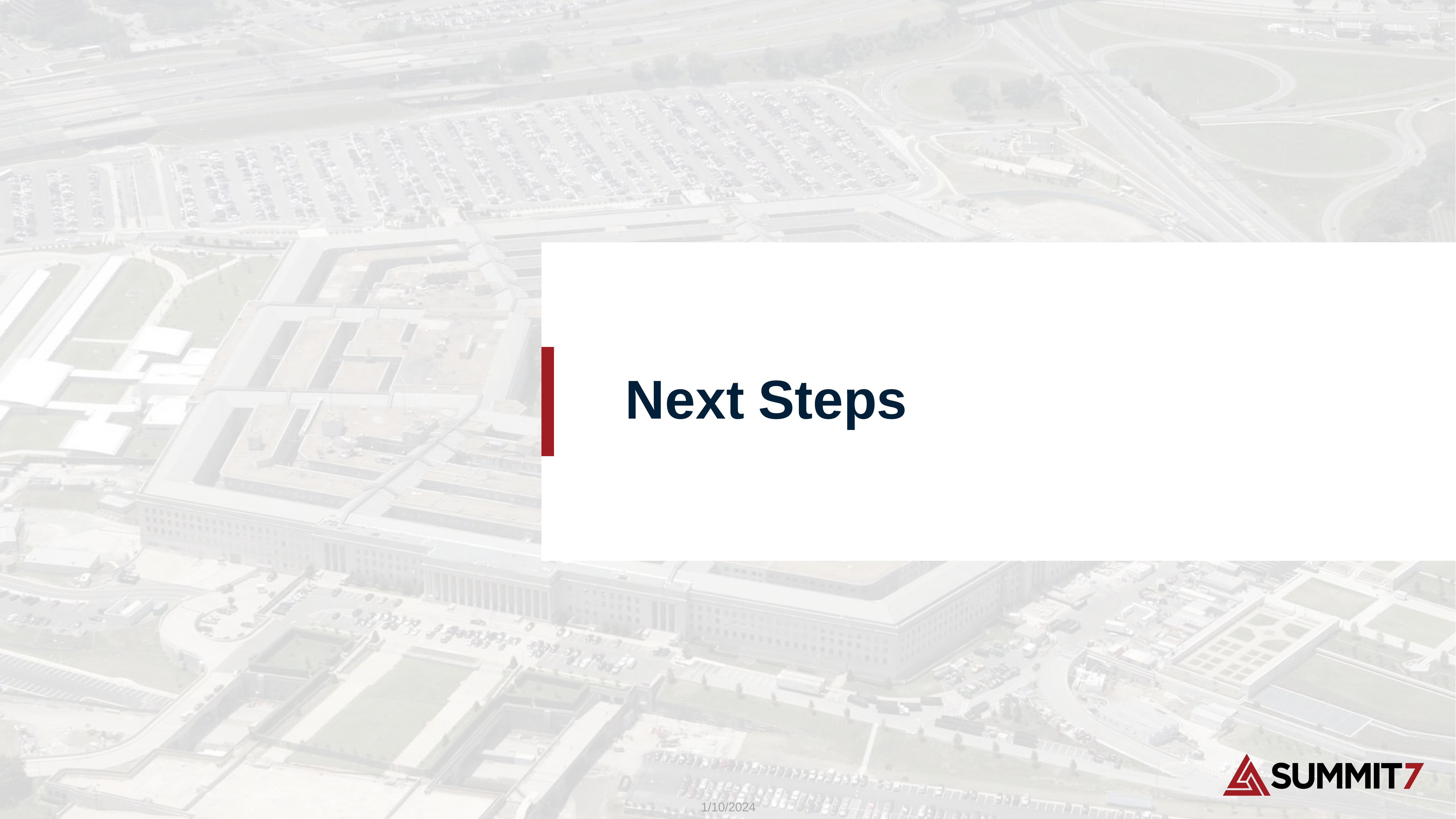
Key Takeaways

- The CMMC program assesses security requirements – it doesn't impose them
  - DoD rationale and policy will remain consistent
- All security requirements have corresponding verification procedures (often multiple)
  - SP 800-171A and 172A are the center of gravity
- Mandatory affirmations are frequent, POAMs are limited, and external service providers are on notice
- The primary constraint on the ecosystem as a whole and your individual organization is implementation capacity rather than assessment capacity
  - Average implementations take longer than the remaining rulemaking timeline
- There are two different CMMC rules (32 CFR "Program" & 48 CFR "Clause")
  - DoD's phased roll-out and related estimates should not be relied on when making strategic decisions
  - Market forces in the wake of the 32 CFR rule will drive CMMC independent of DoD's phased roll-out



Key Questions

- When will your customer or prime contractor require CMMC certification?
- When will your competitors move to get CMMC certified?
- Is your MSP planning on getting CMMC certified?
- Does your MSP have a shared responsibility matrix (SRM) mapped to NIST SP 800-171A?
- Does your MSP’s infrastructure meet the current FedRAMP requirements?



Next Steps

What should you do next?

1. (If you haven’t already) Implement NIST SP 800-171 (CMMC Level 2) now.
2. Reach out to your existing service providers to verify they are set up to be CMMC compliant to the same level as you.
3. Start preassessment readiness activities now.
4. Reach out to a CMMC Certified 3rd Party Assessor (C3PAO).

Remember: **“**CMMC isn't *making* you do the requirements; it's *making sure* you did the requirements” -

Summit 7 Overview

CMMC DFARS 7012 NIST 800-171 ITAR

Microsoft Licensing

Selecting the right cloud environment and licensing for security and compliance

CMMC Solutions

Solution sets for protecting data such as FCI, CUI, and ITAR to maintain CMMC compliance and win more DoD contracts.

Managed Services

Managed IT, Security, & Compliance

Summit 7 is solely focused on the Defense Industrial Base.

8 Passed DoD Client Assessments

450+ CMMC / NIST Implementations

200 S7 Staffed US Persons

850+ Clients – we only support Defense Contractors

3 CMMC Certified Assessors (CCA)

12 CMMC Certified Professionals (CCP)

We are trusted by the industry, big and small.

BOEING · eutelsat AMERICA CORP eutelsat GROUP · Rockwell Automation · CLINKENBEARD · 7th SEVENTH SENSE CONSULTING · AU

L3HARRIS · NVIDIA · BAE SYSTEMS · BLUEHALO · HDR · USC University of Southern California

SUMMIT7

Microsoft’s #1 Partner for Gov

Microsoft Partner
Azure Expert MSP
Microsoft

Microsoft
Solutions Partner
Modern Work

Specialist
- Adoption and Change Management
- Calling for Microsoft Teams
- Meetings and Meeting Rooms for Microsoft Teams
- Teamwork Deployment
- Modernize Endpoints

Microsoft
Solutions Partner
Infrastructure
Azure

Specialist
- Microsoft Windows Virtual Desktop
- Infra and Database Migration

Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Security

Specialist
- Threat Protection
- Information Protection and Governance
- Identity and Access Management
- Cloud Security

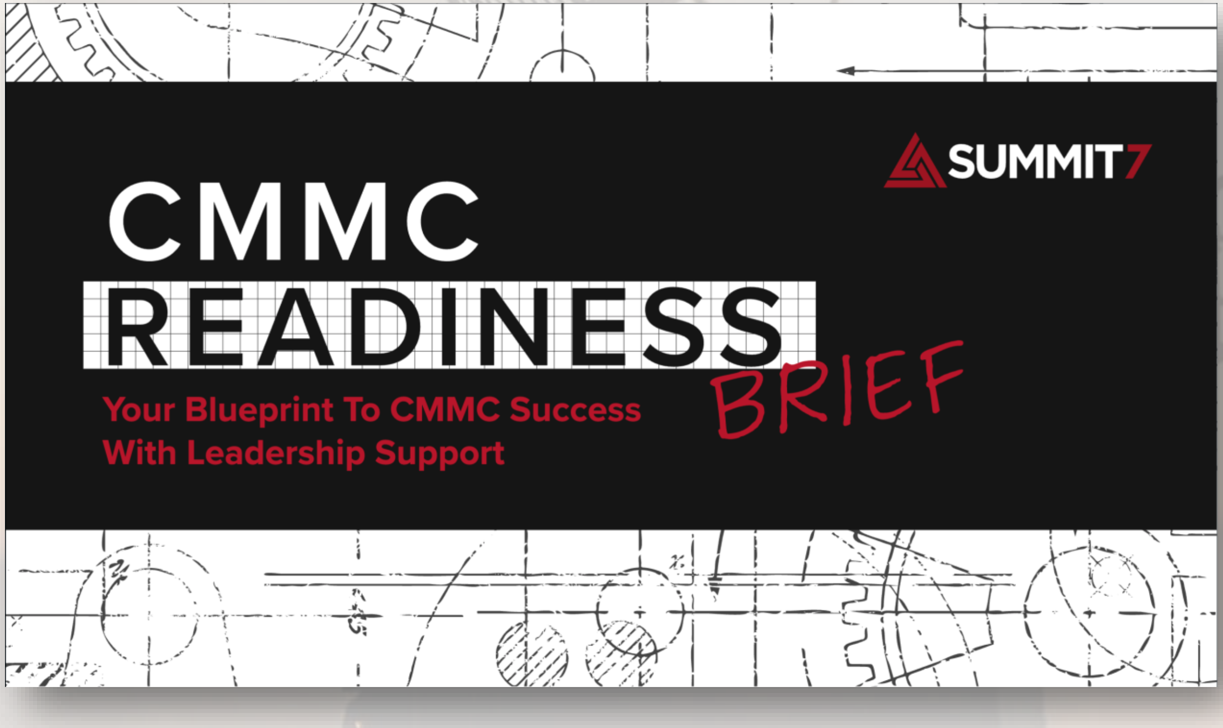
Microsoft
Solutions Partner
Data & AI
Azure

Specialist
- Infra and Database Migration

SUMMIT7

Your Blueprint to CMMC Success

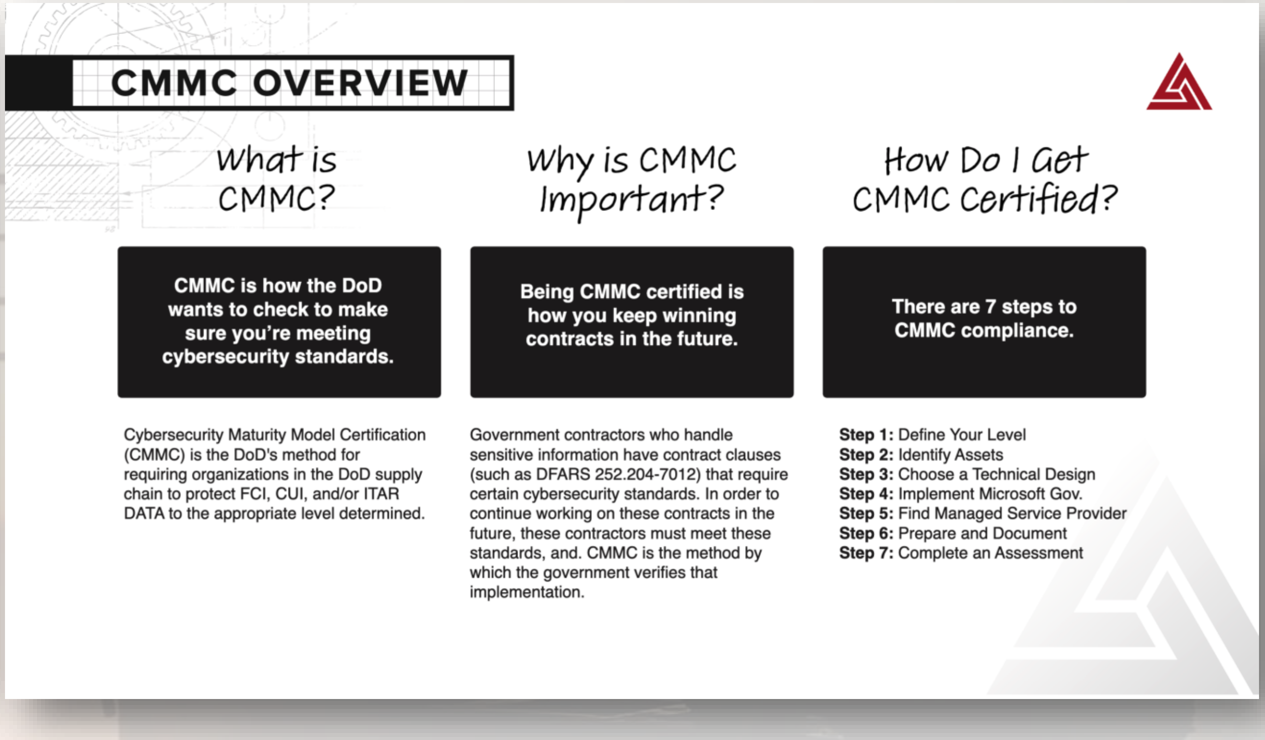
The CMMC Readiness Brief



SUMMIT7

CMMC READINESS BRIEF

Your Blueprint To CMMC Success With Leadership Support



CMMC OVERVIEW

What is CMMC?

CMMC is how the DoD wants to check to make sure you're meeting cybersecurity standards.

Cybersecurity Maturity Model Certification (CMMC) is the DoD's method for requiring organizations in the DoD supply chain to protect FCI, CUI, and/or ITAR DATA to the appropriate level determined.

Why is CMMC Important?

Being CMMC certified is how you keep winning contracts in the future.

Government contractors who handle sensitive information have contract clauses (such as DFARS 252.204-7012) that require certain cybersecurity standards. In order to continue working on these contracts in the future, these contractors must meet these standards, and. CMMC is the method by which the government verifies that implementation.

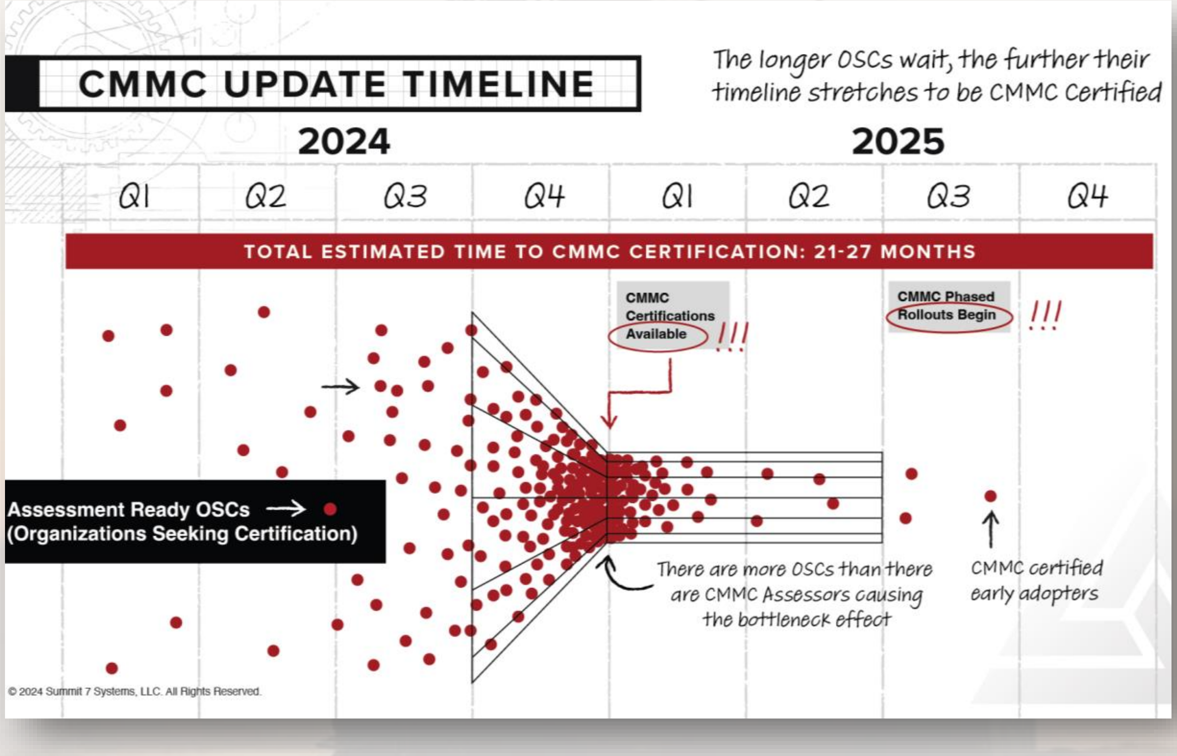
How Do I Get CMMC Certified?

There are 7 steps to CMMC compliance.

Step 1: Define Your Level
Step 2: Identify Assets
Step 3: Choose a Technical Design
Step 4: Implement Microsoft Gov.
Step 5: Find Managed Service Provider
Step 6: Prepare and Document
Step 7: Complete an Assessment

Your Blueprint to CMMC Success

The CMMC Readiness Brief



CMMC UPDATE TIMELINE

The longer OSCs wait, the further their timeline stretches to be CMMC Certified

TOTAL ESTIMATED TIME TO CMMC CERTIFICATION: 21-27 MONTHS

CMMC Certifications Available !!!

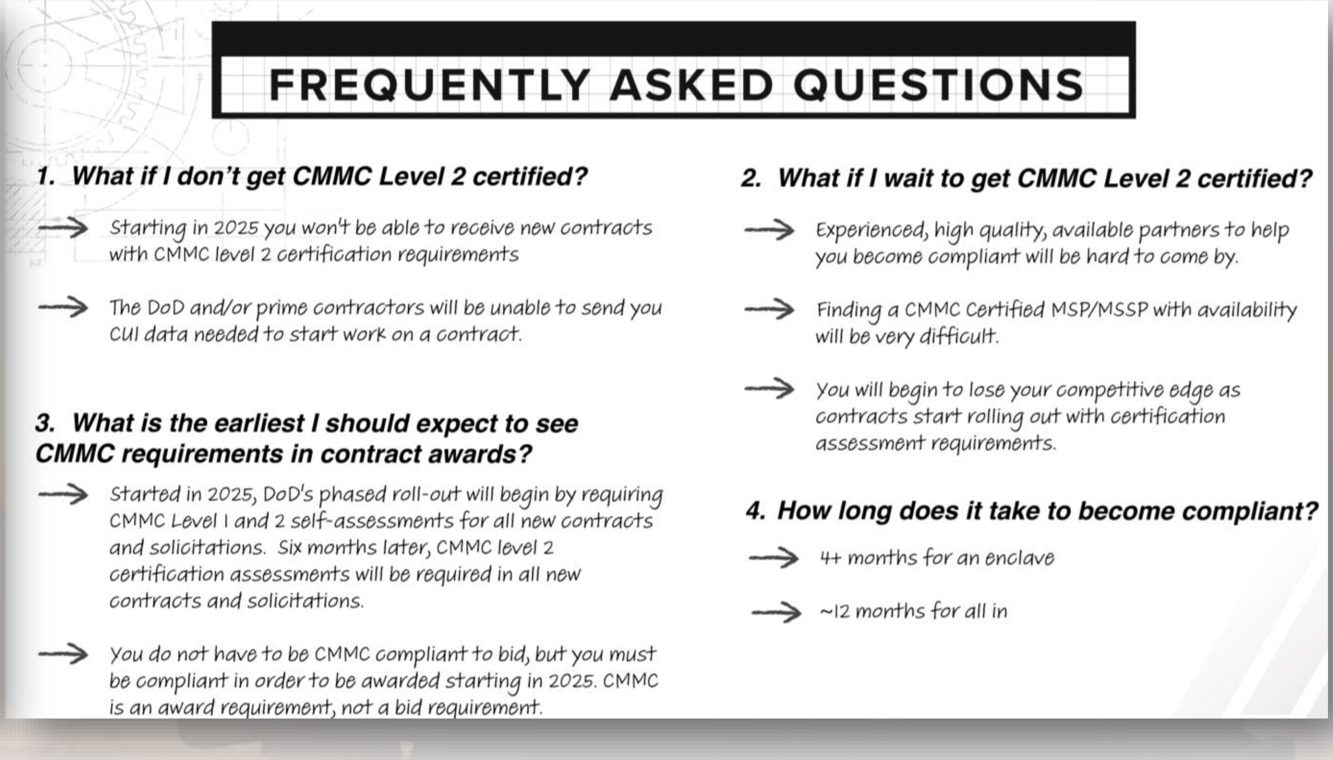
CMMC Phased Rollouts Begin !!!

Assessment Ready OSCs →
(Organizations Seeking Certification)

There are more OSCs than there are CMMC Assessors causing the bottleneck effect

CMMC certified early adopters

© 2024 Summit 7 Systems, LLC. All Rights Reserved.



FREQUENTLY ASKED QUESTIONS

1. What if I don't get CMMC Level 2 certified?

→ Starting in 2025 you won't be able to receive new contracts with CMMC level 2 certification requirements

→ The DoD and/or prime contractors will be unable to send you CUI data needed to start work on a contract.

3. What is the earliest I should expect to see CMMC requirements in contract awards?

→ Started in 2025, DoD's phased roll-out will begin by requiring CMMC Level 1 and 2 self-assessments for all new contracts and solicitations. Six months later, CMMC level 2 certification assessments will be required in all new contracts and solicitations.

→ You do not have to be CMMC compliant to bid, but you must be compliant in order to be awarded starting in 2025. CMMC is an award requirement, not a bid requirement.

2. What if I wait to get CMMC Level 2 certified?

→ Experienced, high quality, available partners to help you become compliant will be hard to come by.

→ Finding a CMMC Certified MSP/MSSP with availability will be very difficult.

→ You will begin to lose your competitive edge as contracts start rolling out with certification assessment requirements.

4. How long does it take to become compliant?

→ 4+ months for an enclave

→ ~12 months for all in

Q & A

Questions & Answers

✉ **Contact Us:** cmmc@summit7.us