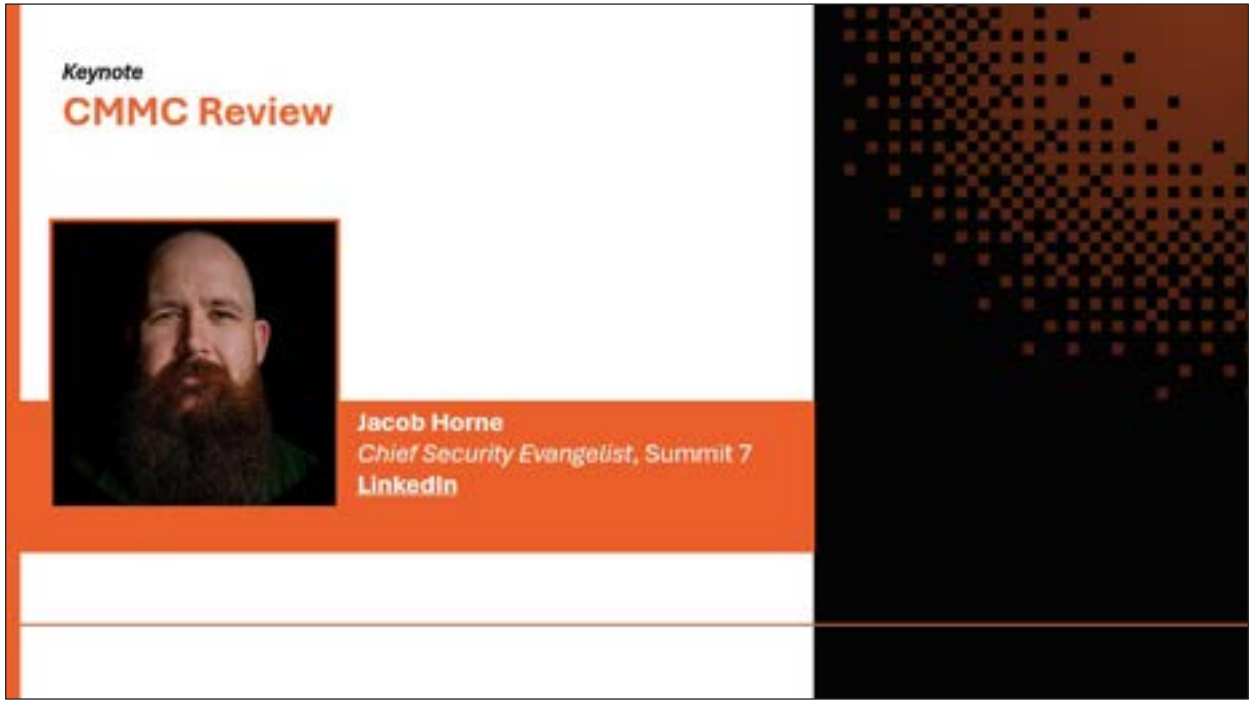
Hypori

The Biggest Mistakes You Can Make

Why defense contractors who are waiting to comply with CMMC will miss out on DoD contracts in 2025 and beyond



Hypori

Thank you for attending this Hypori's hybrid event! Carahsoft is the distributor for Hypori CMMC solutions available via NASA SEWP V, Department of General Services Pennsylvania, Educational Software Solutions and Services – OMNIA Partners, Public Sector, and other contract vehicles.

To learn how to take the next step toward acquiring Hypori's solutions, please check out the following resources and information:

For additional resources:
carah.io/HyporiResources

For additional Hypori solutions:
carah.io/HyporiSolutions

To purchase, check out the contract vehicles available for procurement:
carah.io/HyporiContracts

For upcoming events:
carah.io/HyporiEvents

For additional CMMC solutions:
carah.io/CMMCSolutions

To set up a meeting:
Hypori@carahsoft.com or 571-662-4800

carahsoft

For more information, contact Carahsoft or our reseller partners:
Hypori@carahsoft.com | 571-662-4800

The Biggest Mistake You Can Make

Why defense contractors who are waiting to comply with CMMC will miss out on DoD contracts in 2025 and beyond

JACOB HORNE | 03.13.2025

SUMMIT7

Agenda

01 CMMC 101

02 Timeline & “Phased Roll-Out”

03 CMMC Levels & Waivers

04 CMMC Assessment Readiness Lead Time

05 Procurement Administrative Lead Time

06 Key Takeaways

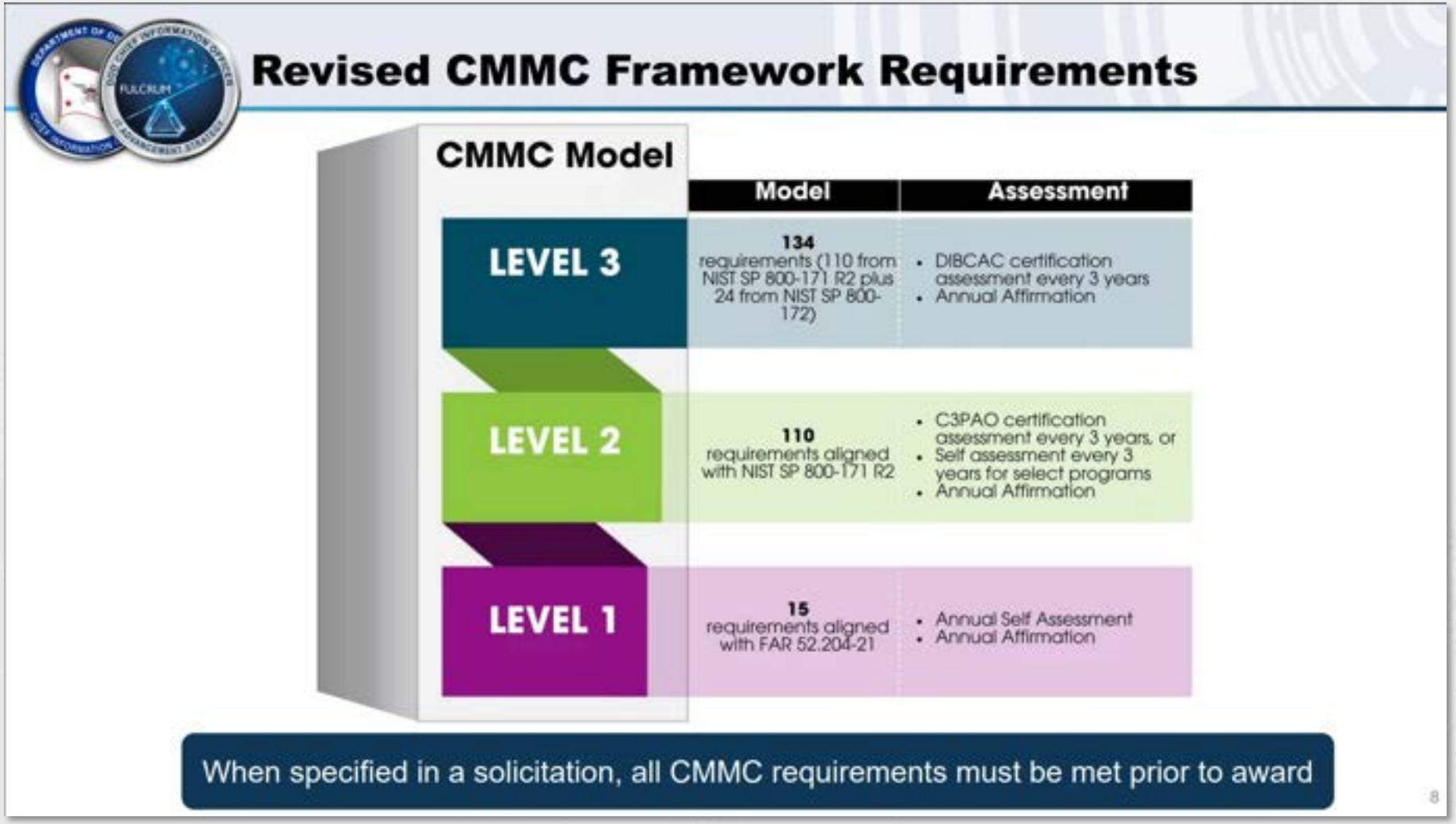
07 Q&A

CMMC 101

How hard could it be?

When defense contractors handle covered data, they have cybersecurity requirements to protect that data

CMMC is a program that verifies if those requirements have been implemented



https://dodcio.defense.gov/cmmc/Resources-Documentation/

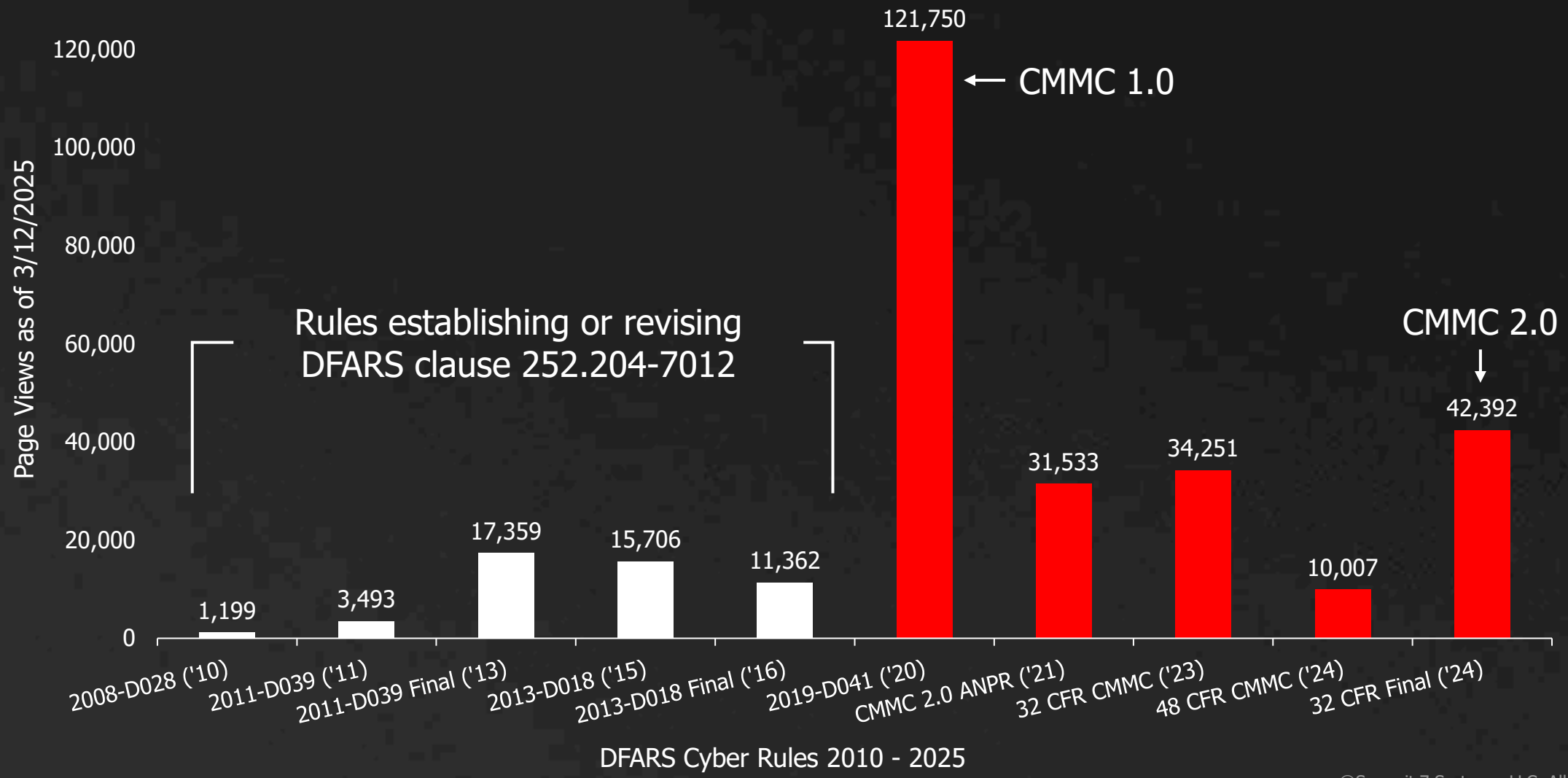
CMMC isn’t making you *do* the requirements.

CMMC is making sure *you did* the requirements.

-Jacob Horne, Chief Cybersecurity Evangelist

CMMC rules are read 5x more than DFARS 252.204-7012 rules

Failure to comply with existing requirements is why CMMC exists in the first place

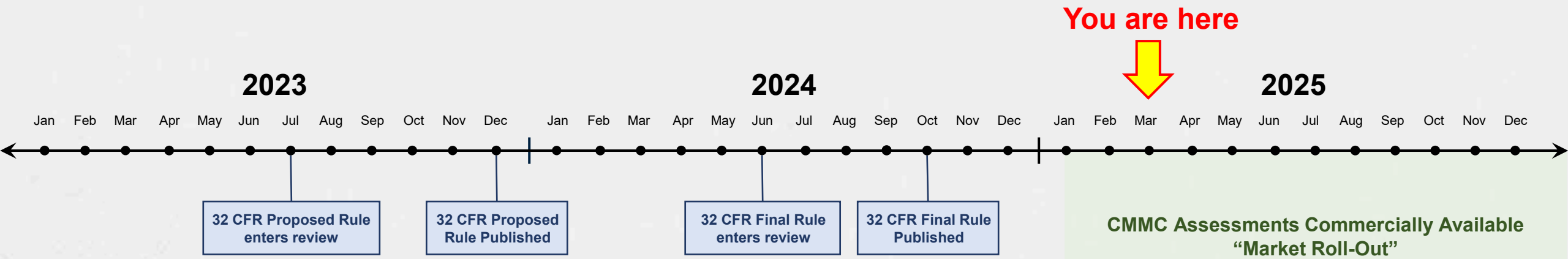


CMMC Timeline & “Phased Roll-Out”

Contracting on borrowed time

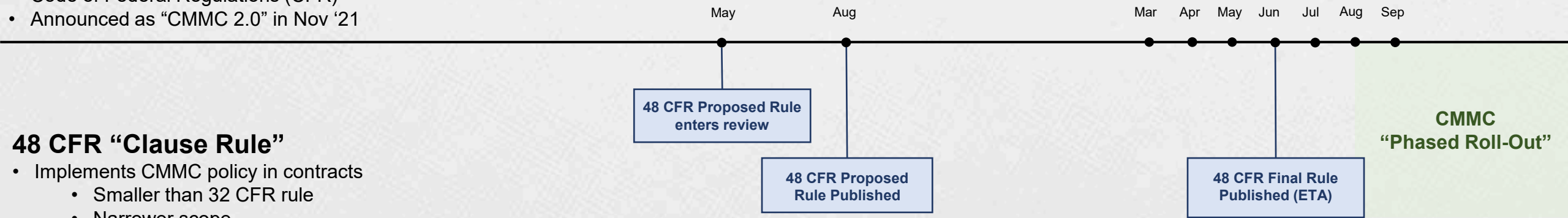
The CMMC regulation went into effect 12/16/2024

Certification assessments are commercially available; will be required in defense contracts ~Summer 2025



32 CFR "Program Rule"

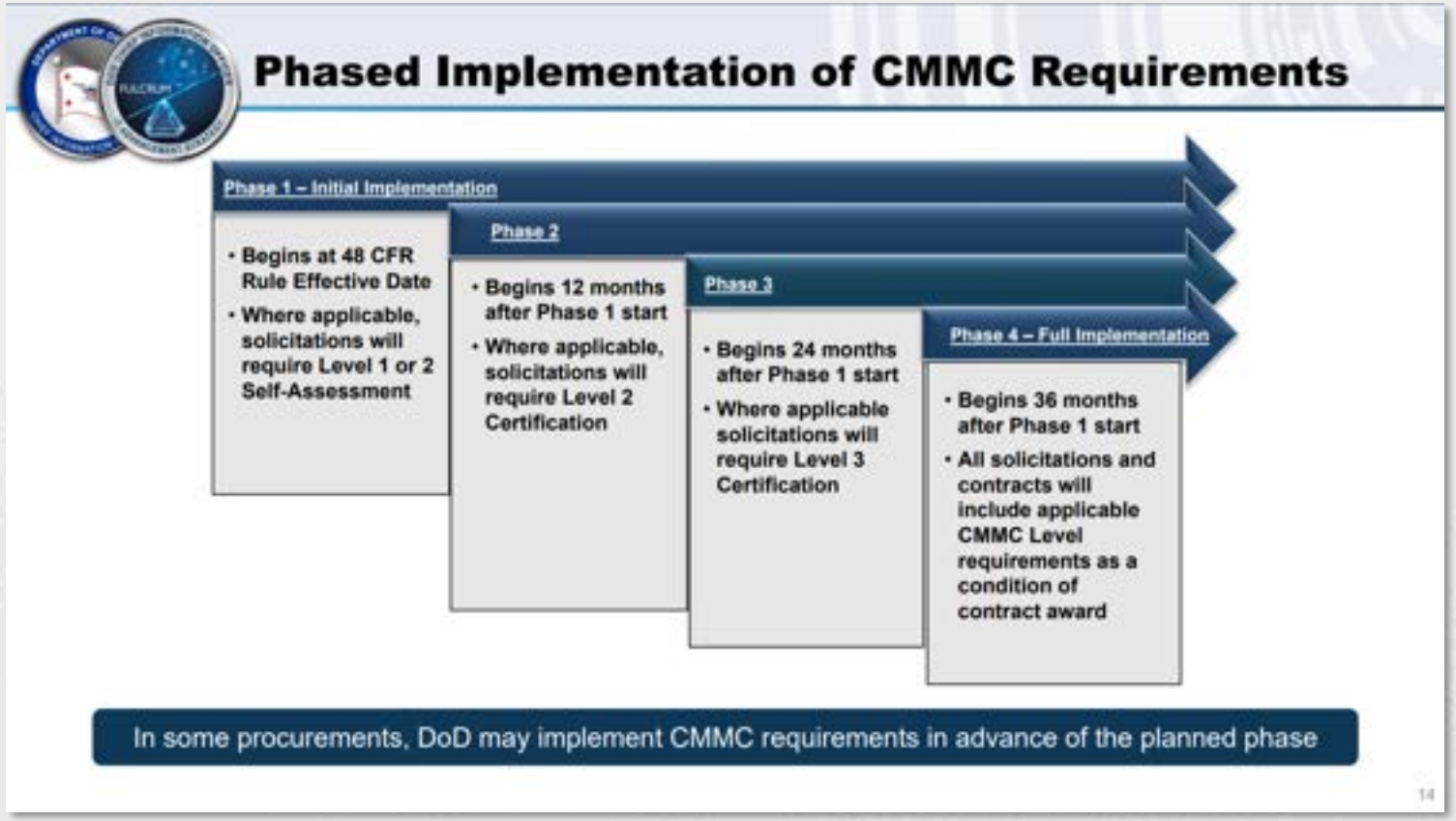
- Codifies CMMC policy at Title 32 of the Code of Federal Regulations (CFR)
- Announced as "CMMC 2.0" in Nov '21



48 CFR "Clause Rule"

- Implements CMMC policy in contracts
  - Smaller than 32 CFR rule
  - Narrower scope
  - Far fewer public comments

The CMMC "Phased Roll-Out" is not a reliable basis for making strategic decisions; DoD has full discretion over each phase



https://dodcio.defense.gov/cmmc/Resources-Documentation/

DoD Discretion by Level 2 Roll-Out Phase

Phase 1:

- Can include requirements prior to effective date of the 48 CFR CMMC rule
- Level 2 certification instead of self-assessment

Phase 2:

- Can delay inclusion of L2 certification to an option period instead of condition of award
- Level 3 certification instead of L2

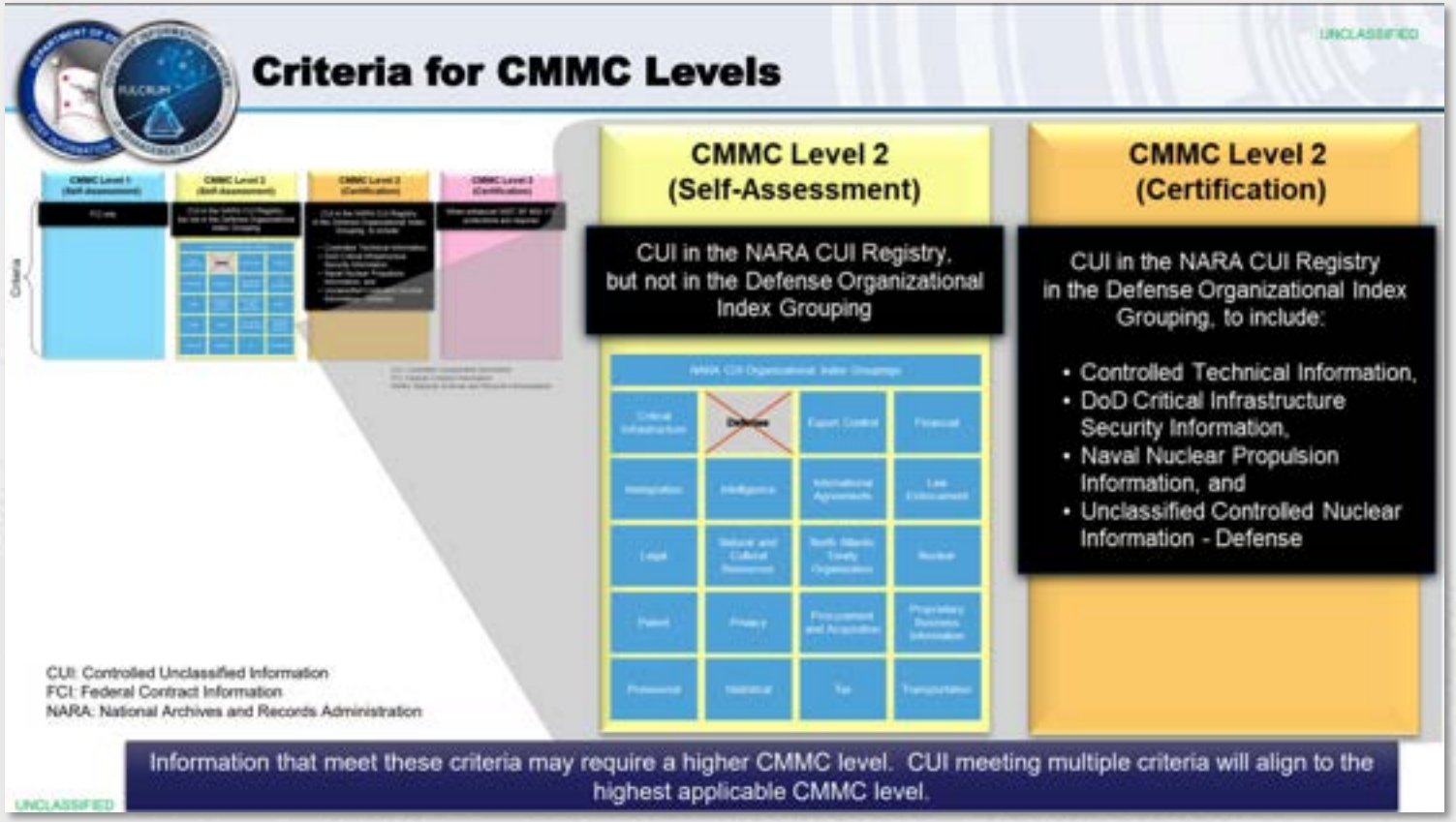
CMMC Level Determination & Waivers

"Ain't nobody self-assessing CMMC Level 2" - DoD

CMMC Level 2 Self-Assessments will be extremely rare

Plan to achieve level 2 via 3rd-party assessment

December 2024



https://dodcio.defense.gov/cmmc/Resources-Documentation/

January 2025

CLEARED
For Open Publication
Jan 17, 2025
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW
January 15, 2025

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing the Cybersecurity Maturity Model Certification (CMMC) Program; Guidance for Determining Appropriate CMMC Compliance Assessment Levels and Process for Waiving CMMC Assessment Requirements

The defense industrial base (DIB) is the target of recurrent and progressively sophisticated cyber attacks targeting Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) processed in, stored on, or transmitted over nonfederal unclassified information systems. These attacks threaten Department of Defense (DoD or Department) mission execution, reduce warfighting capabilities, weaken American technological superiority, and exfiltrate intellectual property and national security information. The Department is undertaking multiple efforts to reduce the risk of cyber attacks to DIB businesses.

Defense contractors and subcontractors are required to safeguard unclassified nonpublic information by applying specified network security requirements, as defined in DoD Instruction 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, which includes identified CUI and FCI that resides in or transits contractor unclassified information systems. Title 32 of the Code of Federal Regulations (CFR) § 2002 describes requirements for adequate safeguarding that, in the context of Defense contracts, are implemented through Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. This clause applies to contracts that require the processing, storing, or transmitting of CUI on contractor-owned information systems.

To enhance the security of DoD information and reduce the risk of cyber attacks to DIB businesses, the Department established the Cybersecurity Maturity Model Certification (CMMC) Program. The final CMMC Program rule was published to the *Federal Register* on October 15, 2024 and is codified in Title 32 CFR Part 170. The CMMC Program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding CUI or FCI. The CMMC Program will implement pre-award assessments of contractor compliance with the appropriate information safeguarding requirements. Title 32 CFR § 170 defines applicability of CMMC requirements and Title 48 CFR DFARS provisions and clauses will implement those requirements.

Upon publication of the final Title 48 CFR DFARS rule, 2019-D041, Program Managers and requiring activities shall include the need for CMMC assessments in procurement request and requirement documents in accordance with phase-in timelines described in Title 32 CFR § 170.3. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance to apply when determining the appropriate CMMC assessment level to include in each DoD solicitation and contract. Service and Component Acquisition Executives are authorized to waive inclusion of CMMC assessment requirements in DoD solicitations. Waivers are discussed in Attachment 2.

https://dodprocurementtoolbox.com/uploads/DOPSR_Cleared_OSD_Memo_CMMC_Implementation_Policy_d26075de0f.pdf

CMMC Level 2 Self-Assessments will be extremely rare

Plan to achieve level 2 via 3rd-party assessment

January 2025

CLEARED
For Open Publication
Jan 17, 2025
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

January 15, 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing the Cybersecurity Maturity Model Certification (CMMC) Program: Guidance for Determining Appropriate CMMC Compliance Assessment Levels and Process for Waiving CMMC Assessment Requirements

The defense industrial base (DIB) is the target of recurrent and progressively sophisticated cyber attacks targeting Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) processed in, stored on, or transmitted over nonfederal unclassified information systems. These attacks threaten Department of Defense (DoD or Department) mission execution, reduce warfighting capabilities, weaken American technological superiority, and exfiltrate intellectual property and national security information. The Department is undertaking multiple efforts to reduce the risk of cyber attacks to DIB businesses.

Defense contractors and subcontractors are required to safeguard unclassified nonpublic information by applying specified network security requirements, as defined in DoD Instruction 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, which includes identified CUI and FCI that resides in or transits contractor unclassified information systems. Title 32 of the Code of Federal Regulations (CFR) § 2002 describes requirements for adequate safeguarding that, in the context of Defense contracts, are implemented through Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. This clause applies to contracts that require the processing, storing, or transmitting of CUI on contractor-owned information systems.

To enhance the security of DoD information and reduce the risk of cyber attacks to DIB businesses, the Department established the Cybersecurity Maturity Model Certification (CMMC) Program. The final CMMC Program rule was published to the *Federal Register* on October 15, 2024 and is codified in Title 32 CFR Part 170. The CMMC Program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding CUI or FCI. The CMMC Program will implement pre-award assessments of contractor compliance with the appropriate information safeguarding requirements. Title 32 CFR § 170 defines applicability of CMMC requirements and Title 48 CFR DFARS provisions and clauses will implement those requirements.

Upon publication of the final Title 48 CFR DFARS rule, 2019-D041, Program Managers and requiring activities shall include the need for CMMC assessments in procurement request and requirement documents in accordance with phase-in timelines described in Title 32 CFR § 170.3. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance to apply when determining the appropriate CMMC assessment level to include in each DoD solicitation and contract. Service and Component Acquisition Executives are authorized to waive inclusion of CMMC assessment requirements in DoD solicitations. Waivers are discussed in Attachment 2.

"CMMC Level 2 (Certification) is the minimum assessment requirement when the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI categorized under the National Archives CUI Registry Defense Organizational Index Grouping."

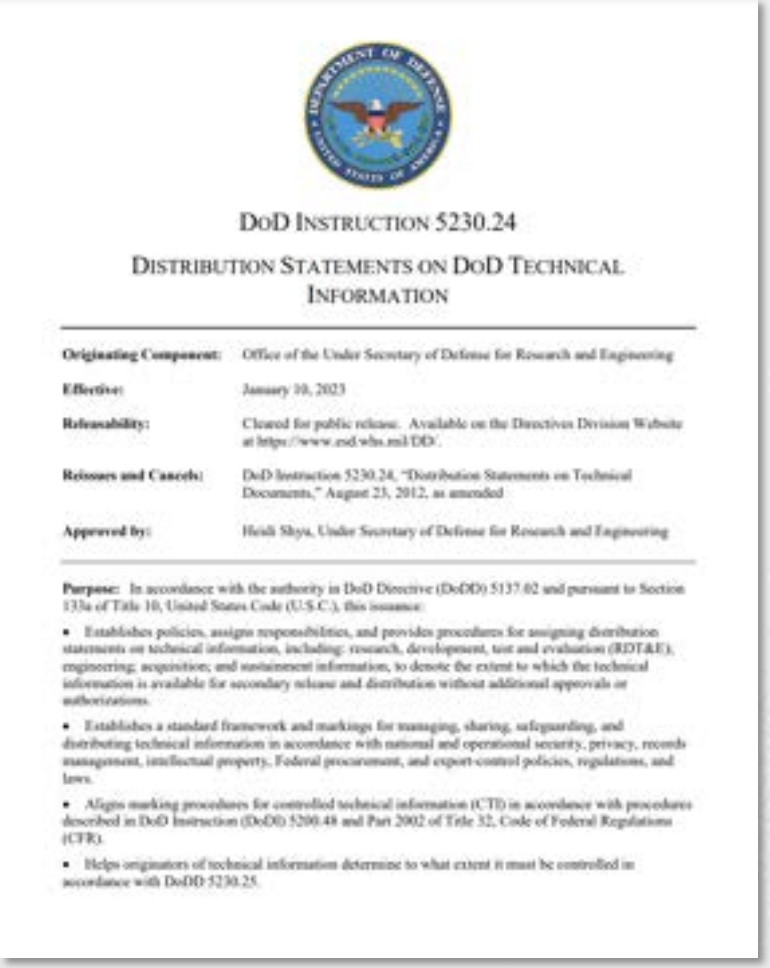
- **Controlled Technical Information**
- **DoD Critical Infrastructure Security Information**
- **Naval Nuclear Propulsion Information**
- **Privileged Safety Information**
- **Unclassified Controlled Nuclear Information - Defense**

https://dodprocurementtoolbox.com/uploads/DOPSR_Cleared_OSD_Memo_CMMC_Implementation_Policy_d26075de0f.pdf

CMMC Level 2 Self-Assessments will be extremely rare

Plan to achieve level 2 via 3rd-party assessment

January 2023



DoD INSTRUCTION 5230.24

DISTRIBUTION STATEMENTS ON DoD TECHNICAL INFORMATION

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	January 10, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended
Approved by:	Heidi Shyu, Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02 and pursuant to Section 133a of Title 10, United States Code (U.S.C.), this issuance:

- Establishes policies, assigns responsibilities, and provides procedures for assigning distribution statements on technical information, including: research, development, test and evaluation (RDT&E); engineering; acquisition; and sustainment information, to denote the extent to which the technical information is available for secondary release and distribution without additional approvals or authorizations.
- Establishes a standard framework and markings for managing, sharing, safeguarding, and distributing technical information in accordance with national and operational security, privacy, records management, intellectual property, Federal procurement, and export-control policies, regulations, and laws.
- Aligns marking procedures for controlled technical information (CTI) in accordance with procedures described in DoD Instruction (DoDI) 5200.48 and Part 2002 of Title 32, Code of Federal Regulations (CFR).
- Helps originators of technical information determine to what extent it must be controlled in accordance with DoDD 5230.25.

https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/523024p.pdf

CTI: Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

- **Engineering drawings**
- **Configuration-management documentation**
- **Engineering data and associated lists**
- **Standards**
- **Specifications**
- **Technical manuals, reports, and orders**
- **Blueprints, plans, and instructions**

CMMC waivers are for *contracts*, not *contractors*

Waivers are determined prior to issuing a solicitation and will be extremely rare

January 2025

CLEARED
For Open Publication
Jan 17, 2025
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

January 15, 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing the Cybersecurity Maturity Model Certification (CMMC) Program: Guidance for Determining Appropriate CMMC Compliance Assessment Levels and Process for Waiving CMMC Assessment Requirements

The defense industrial base (DIB) is the target of recurrent and progressively sophisticated cyber attacks targeting Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) processed in, stored on, or transmitted over nonfederal unclassified information systems. These attacks threaten Department of Defense (DoD or Department) mission execution, reduce warfighting capabilities, weaken American technological superiority, and exfiltrate intellectual property and national security information. The Department is undertaking multiple efforts to reduce the risk of cyber attacks to DIB businesses.

Defense contractors and subcontractors are required to safeguard unclassified nonpublic information by applying specified network security requirements, as defined in DoD Instruction 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, which includes identified CUI and FCI that resides in or transits contractor unclassified information systems. Title 32 of the Code of Federal Regulations (CFR) § 2002 describes requirements for adequate safeguarding that, in the context of Defense contracts, are implemented through Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. This clause applies to contracts that require the processing, storing, or transmitting of CUI on contractor-owned information systems.

To enhance the security of DoD information and reduce the risk of cyber attacks to DIB businesses, the Department established the Cybersecurity Maturity Model Certification (CMMC) Program. The final CMMC Program rule was published in the *Federal Register* on October 15, 2024 and is codified in Title 32 CFR Part 170. The CMMC Program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding CUI or FCI. The CMMC Program will implement pre-award assessments of contractor compliance with the appropriate information safeguarding requirements. Title 32 CFR § 170 defines applicability of CMMC requirements and Title 48 CFR DFARS provisions and clauses will implement those requirements.

Upon publication of the final Title 48 CFR DFARS rule, 2019-D041, Program Managers and requiring activities shall include the need for CMMC assessments in procurement request and requirement documents in accordance with phase-in timelines described in Title 32 CFR § 170.3. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance to apply when determining the appropriate CMMC assessment level to include in each DoD solicitation and contract. Service and Component Acquisition Executives are authorized to waive inclusion of CMMC assessment requirements in DoD solicitations. Waivers are discussed in Attachment 2.

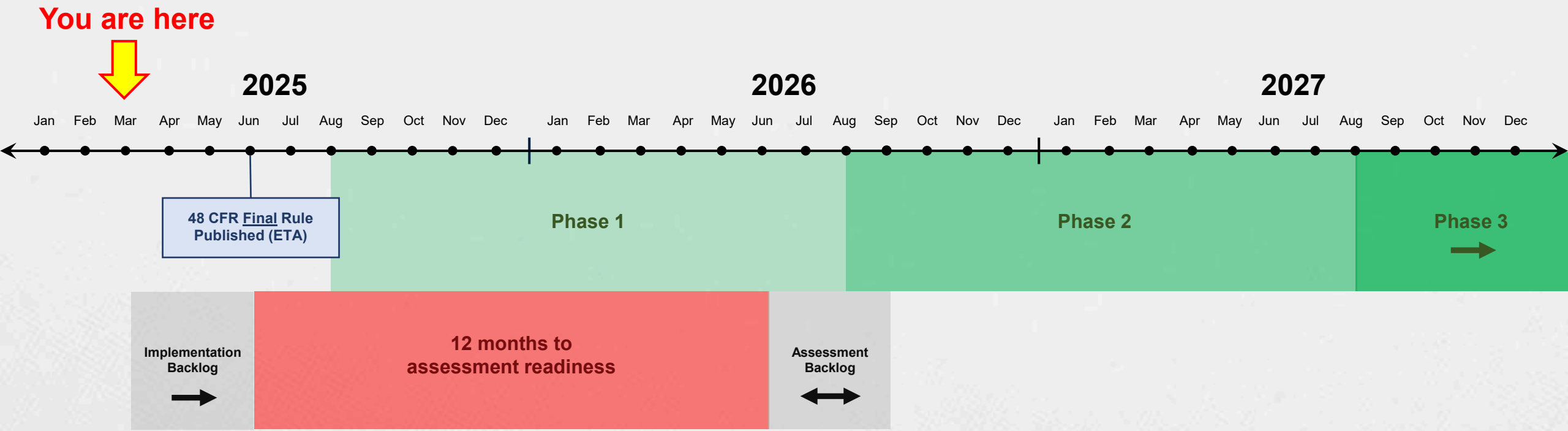
https://dodprocurementtoolbox.com/uploads/DOPSR_Cleared_OSD_Memo_CMMC_Implementation_Policy_d26075de0f.pdf

- All waiver requests go through component CIOs before service/component acquisition executive approval.
- CMMC waivers may be requested for individual procurements or classes of procurements.
- CMMC waivers do not affect the underlying security requirements in DFARS 7012, FAR 52.204-21.
- When market research indicates that including a CMMC assessment requirement may impede ability to generate robust competition or delay delivery of mission critical capabilities, the [acquisition executive] may approve requests to waive inclusion of CMMC assessment requirements.

CMMC Assessment Readiness Lead Time

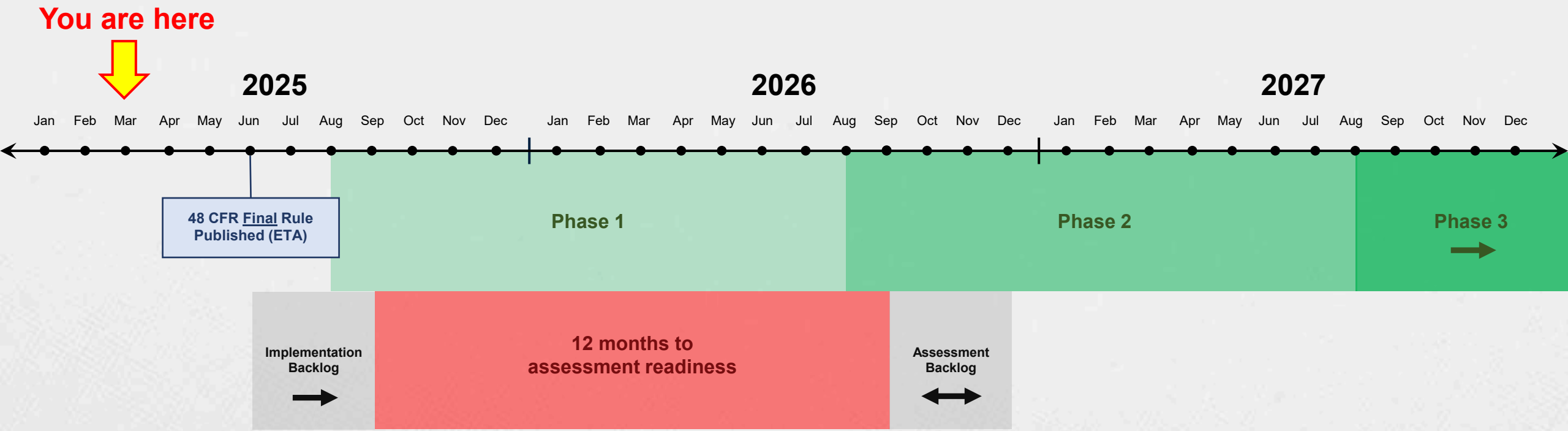
"CALT" – The longest pole in the tent

Delaying implementation until CMMC is in solicitations will halt new contract awards for 12+ months



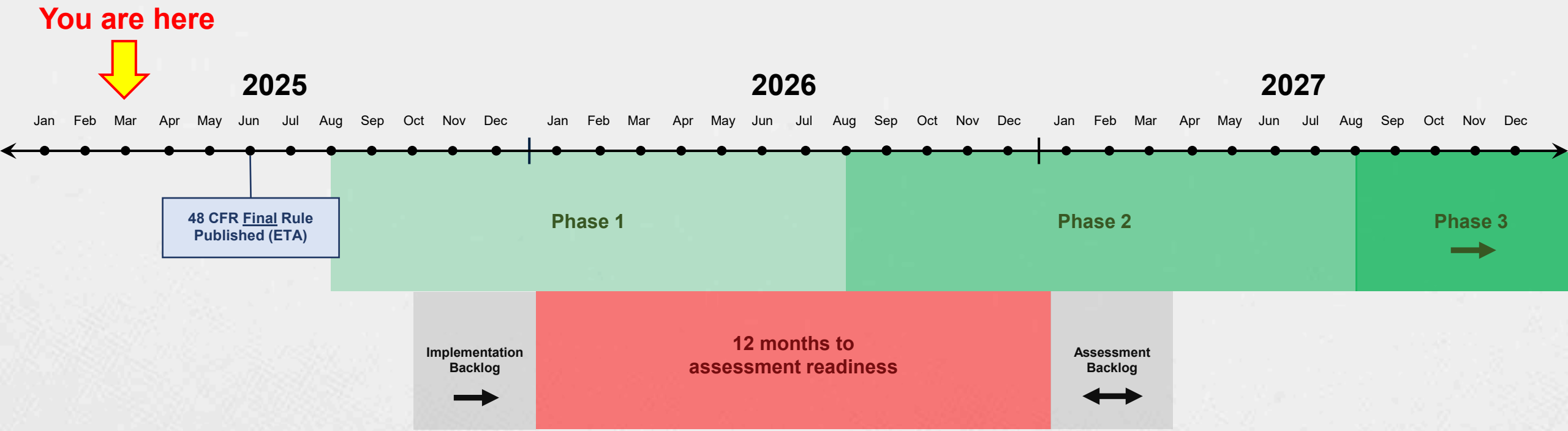
Starting from scratch in Q1 2025 = new award target Q4 2026

Delaying implementation until CMMC is in solicitations will halt new contract awards for 12+ months



Kickoff from 48 CFR final rule publication = new award target Q1 2027

Delaying implementation until CMMC is in solicitations will halt new contract awards for 12+ months

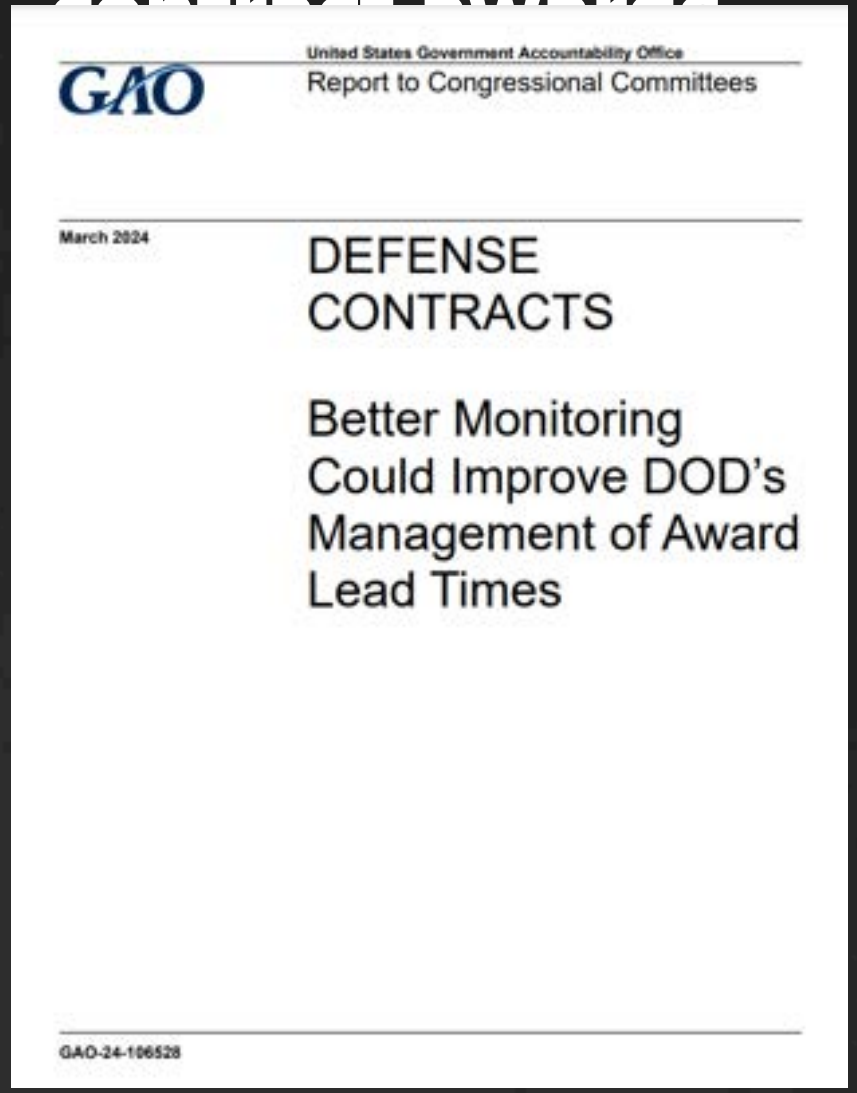


Q4 2025 implementation kickoff = new award target Q2 2027

Procurement Administrative Lead Time

"PALT" – The most important metric behind your CMMC strategy

If your total CMMC implementation + assessment time is longer than your customer's PALT, then you will miss contract awards


United States Government Accountability Office

GAO

Report to Congressional Committees

March 2024

DEFENSE CONTRACTS

Better Monitoring Could Improve DOD's Management of Award Lead Times

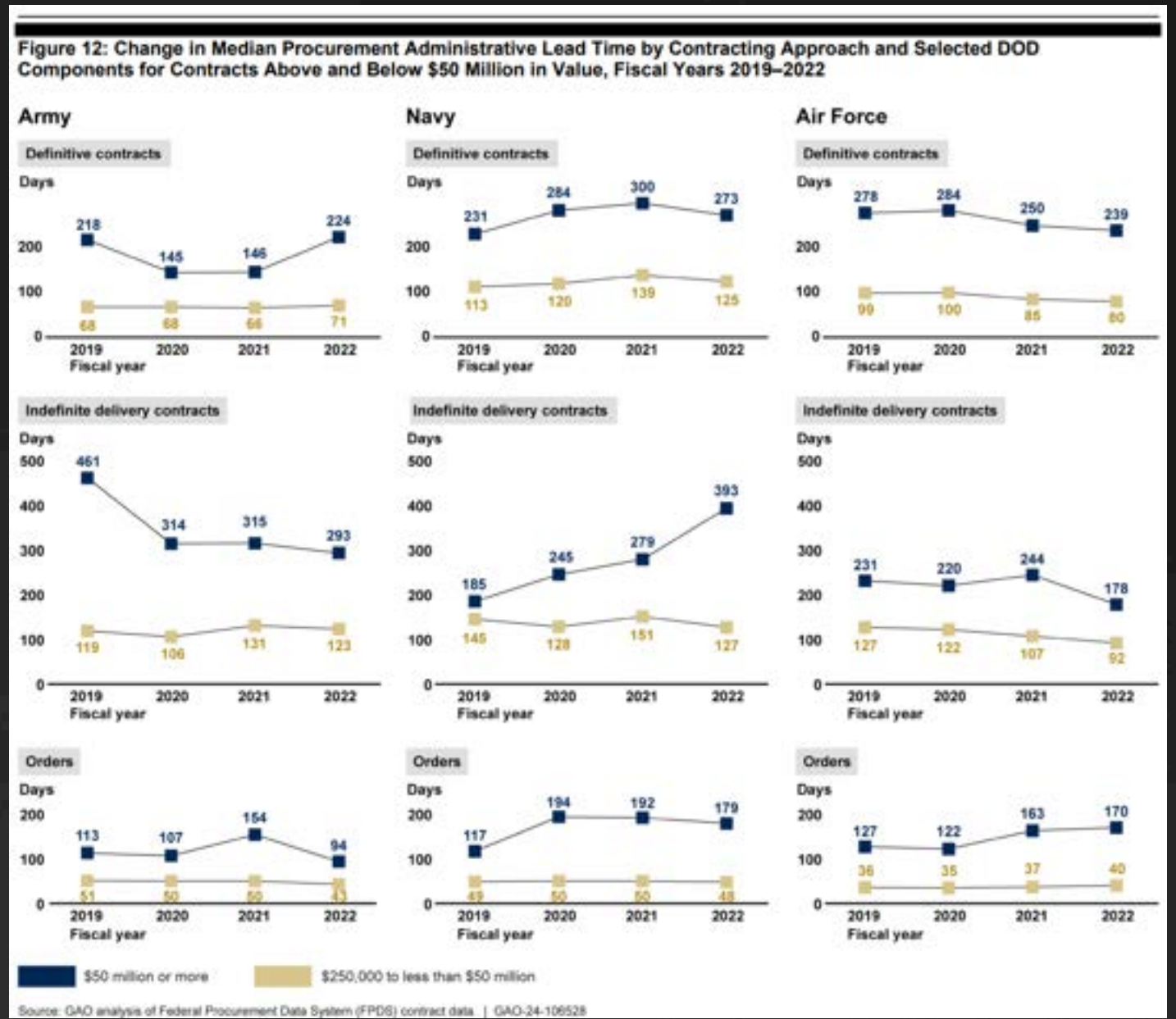
GAO-24-106528

https://www.gao.gov/products/gao-24-106528

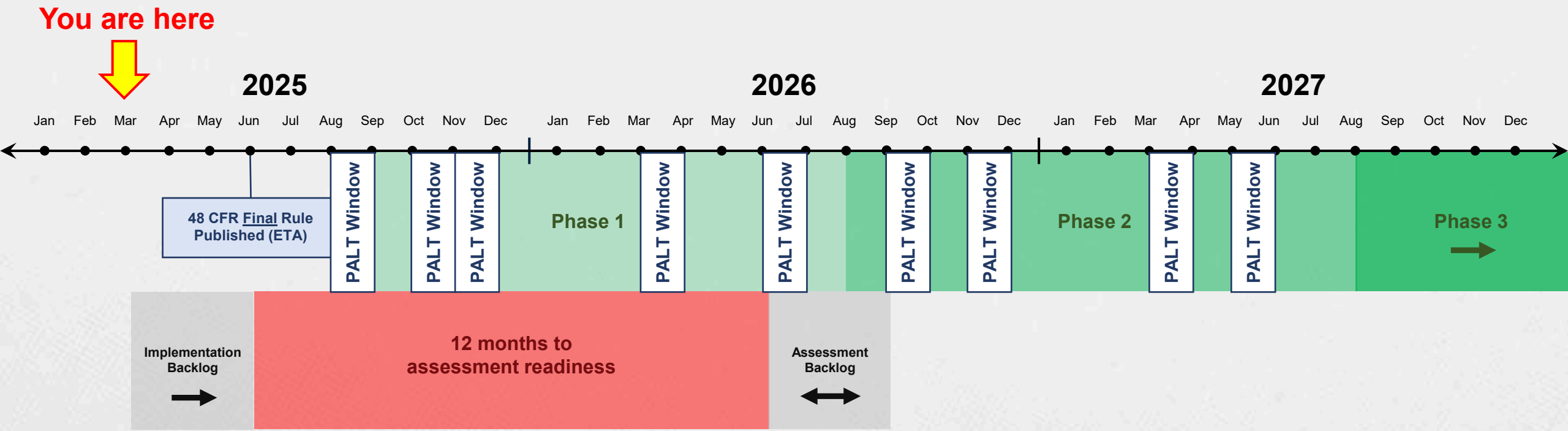
Procurement Administrative Lead Time (PALT)

The length of time between when an agency solicits offers from potential contractors and the date it awards a contract.

FY19 – FY20: DOD-wide median PALT has decreased by more than 20%, from 41 days to just 32 days

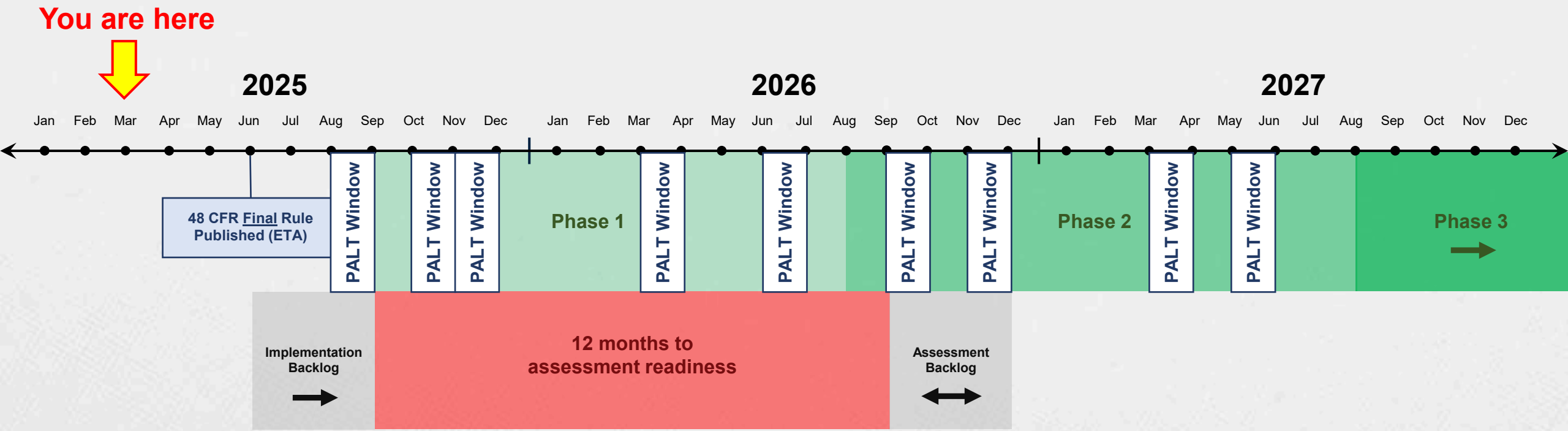


Delaying implementation until CMMC is in solicitations will halt new contract awards for 12+ months



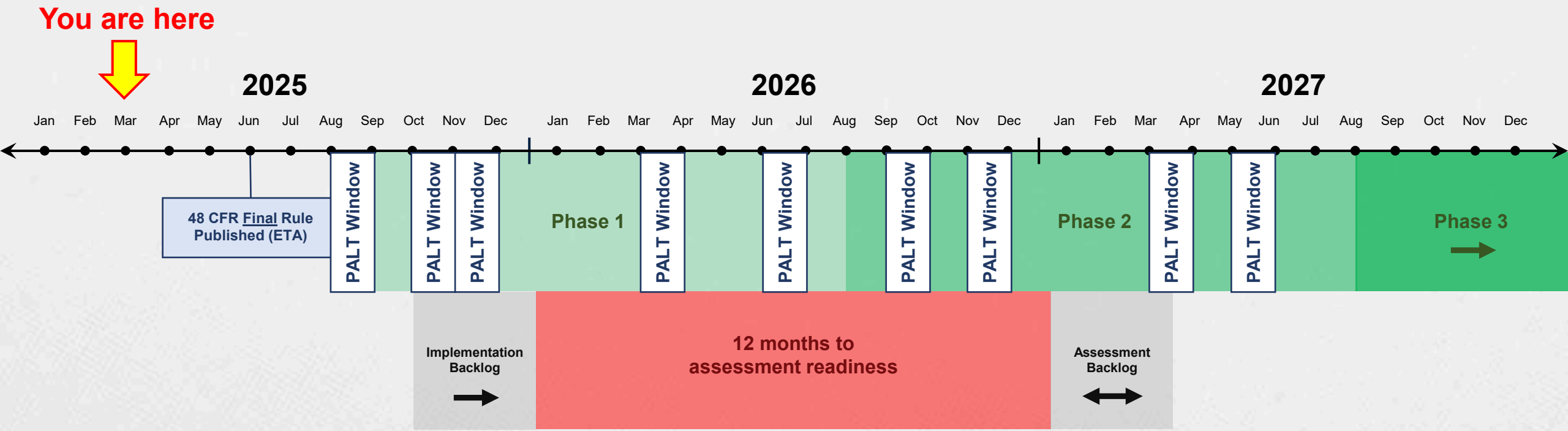
Starting from scratch in Q1 2025 = new award target Q4 2026

Delaying implementation until CMMC is in solicitations will halt new contract awards for 12+ months



Kickoff from 48 CFR final rule publication = new award target Q1 2027

Delaying implementation until CMMC is in solicitations will halt new contract awards for 12+ months



Q4 2025 implementation kickoff = new award target Q2 2027

SUMMIT7

THANK YOU

Contact

jacob.horne@summit7.us 256.585.6868 linkedin.com/company/jacob-evan-horne