Keynote Presentation of Robert Metzger
October 30, 2024

Robert S. Metzger
Rogers Joseph O'Donnell PC

rmetzger@rjo.com | +1.202.777.8951

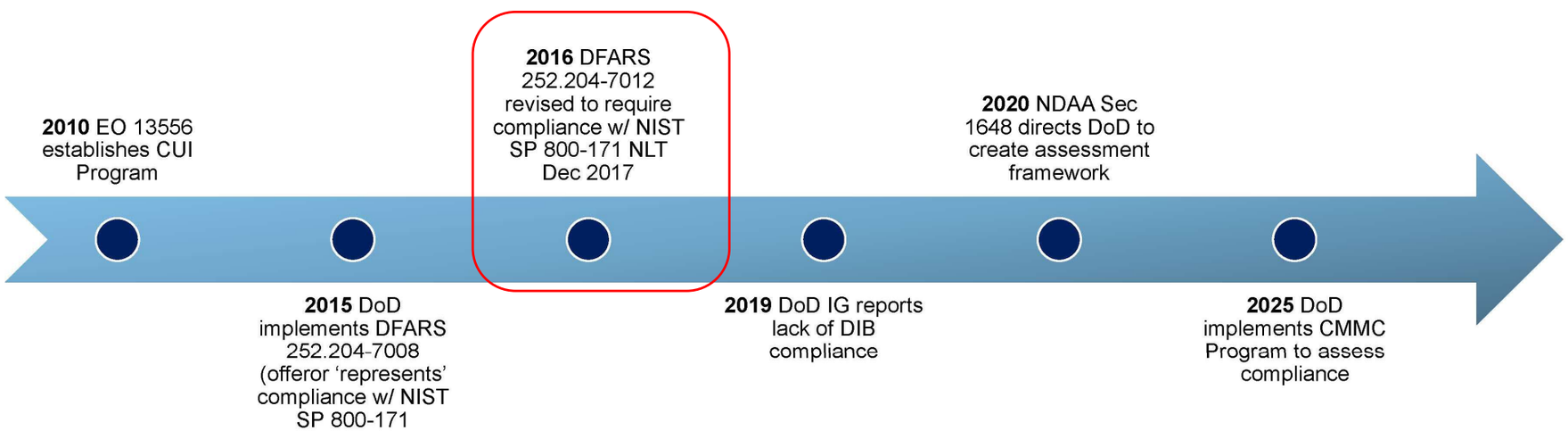
What is CMMC?

- CMMC is a cybersecurity compliance framework that applies to organizations with contracts with the Department of Defense.
  - CMMC has three Levels. We focus on Level 2 (CUI).
  - Level 2 applies to 80,000 companies 2; 90% of these must pass a certification assessment.
  - DFARS 252.204-7012 has required cyber protection of CUI since 12/31/2017.
  - NIST SP 800-171 Rev. 2 establishes 110 cyber controls in 14 security families.
  - When actualized, each of 320 "Assessment Objectives" in SP 800-171A (June 2018) must be MET of found NOT APPLICABLE for the overall security requirement to be scored as MET.
- CMMC enforces cyber compliance. The Program DFARS Rule (32 CFR Pt. 170) is now final. Rollout of certification requirements begins when the companion Contract DFARS Rule (48 CFR) is final – expected by end Q2 2025.

A Long History As Prelude

CMMC Program Overview and History

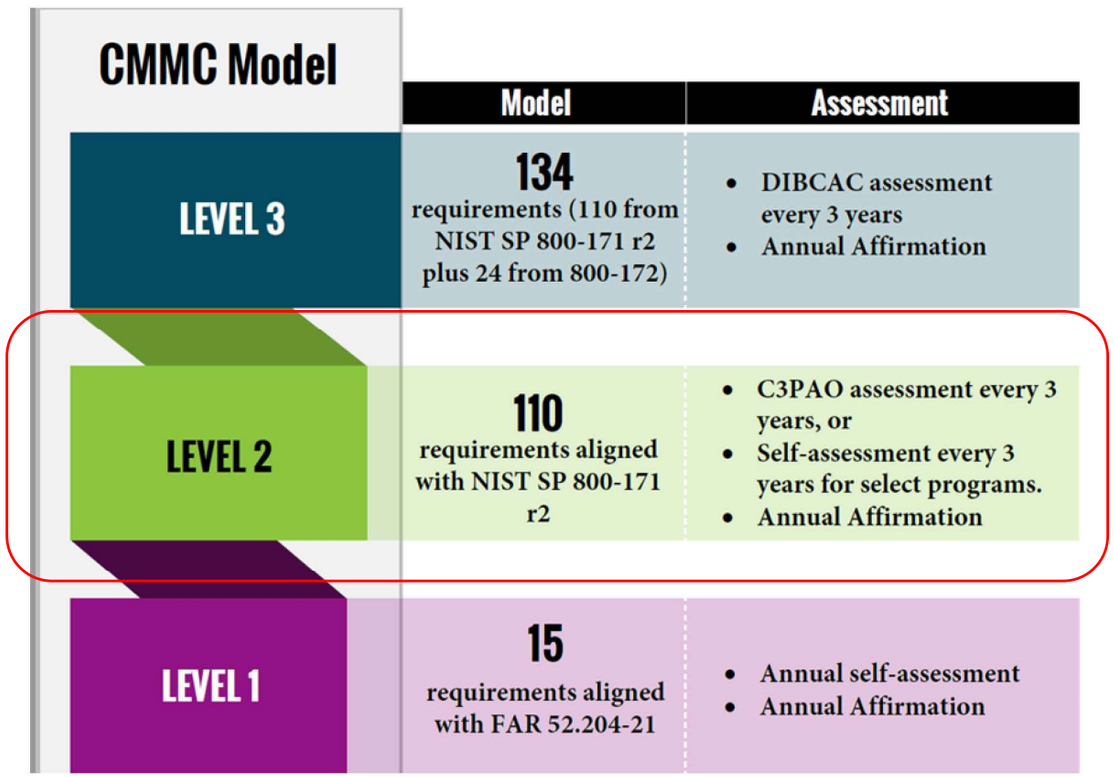
The CMMC Program helps ensure that DoD contractors and subcontractors comply with DoD requirements to safeguard FCI and CUI.



Source: DoD Cybersecurity Maturity Model Certification Program Overview

The Three Levels of CMMC

Revised CMMC Framework Requirements

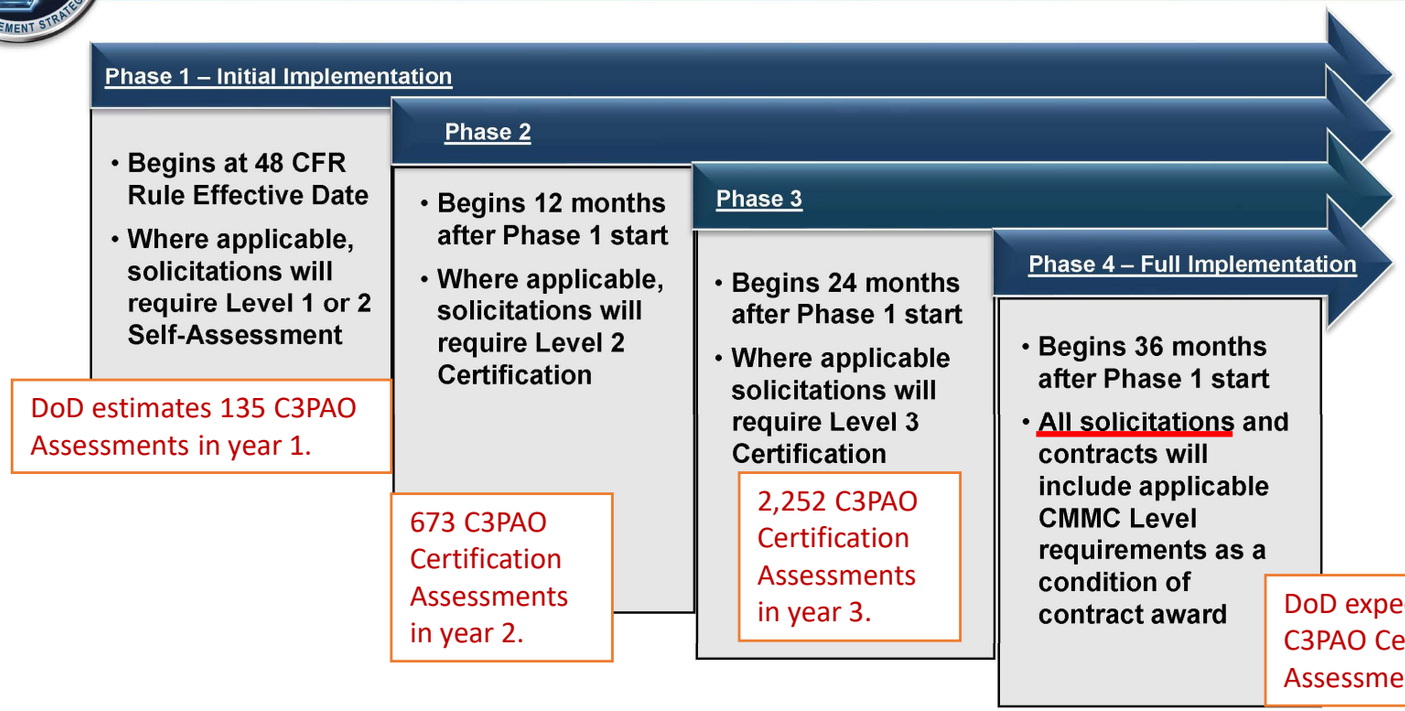


Source: DoD Cybersecurity Maturity Model Certification Program Overview

When specified in a solicitation, all CMMC requirements must be met prior to award

The 4-Year Implementation Plan

Phased Implementation of CMMC Requirements



In some procurements, DoD may implement CMMC requirements in advance of the planned phase

Applicability Estimates – 32 C.F.R. § 170.3(b)

- Applicable to small businesses and to commercial products
- "Pure" COTS excluded
- Universities excluded if solely engaged in fundamental research (w/o FCI or CUI)
- Flow Down "throughout the supply chain at all tiers"
- Applies to international primes and subs "regardless" of where operated
- Certification lasts 3 years
- Affirmations required annually
- Waiver authority very limited
- No apparent "safety valve" for companies that cannot meet

Level	Small	Other Than Small	Total
1 Self-Assessment	103,010	36,191	139,201
2 Self-Assessment	2,961	1,039	4,000
2 C3PAO Assessment	**56,689**	**19,909**	**76,598**
3 DIBCAC Assessment	1,327	160	1,487
Total	163,987	57,299	221,286

10 Key Take-Aways From the Final 32 CFR Rule

1) DoD is committed to the CMMC program.
2) CMMC is threat-driven. The threat environment is worsening.
3) CMMC enforces security obligations where self-attestation failed.
4) Before, companies could "rest" on low SPRS scores. No longer.
5) Small businesses are subject to CMMC obligations – without relief.
6) NIST SP 800-171 Rev. 2 controls are the present baseline for security.
7) DoD now facilitates the use of enclaves and Managed Service Providers.
8) Prime contractors will pressure their suppliers to comply early.
9) A Level 2 "Final certification assessment" will be required for new awards.
10) The Final CMMC Program Rule is effective Dec. 16, 2024.

Regarding the Proposed 48 CFR Rule

- Required notification of "any lapses or changes" to contractor information systems or "when CMMC compliance status changes."
- Primes must "ensure" their subs have the appropriate CMMC level, prior to subcontract award, but cannot access suppliers' SPRS (or eMASS) scores.
- DoD has declined to provide any "tailored accommodations" for small contractors or other special circumstances.
- Criteria absent as to who/how/when decisions will be made as to which programs, or contracts, will be subject to which CMMC requirements.
- POA&Ms limited to only 1/3 of the 110 NIST -171 requirements (only 1-point items).
- Continuing obligations for monitoring and reporting.
- Companies must anticipate continuing adjustment and validation of security.

Summary: Your Challenge, Your Choices

- CMMC is real and now.
- Compliance and security serve both enterprise and the national interest.
- Security comes at a cost (independent of CMMC) and costs will continue.
- The new reality: build security costs into the business model of DoD suppliers.
- Companies have choices for security solutions.
- "Waiting and watching" is bad business. Most need 6 – 18 months for readiness.
- Level 2 CMMC Assessments after Dec. 16, 2024, count for rule compliance.
- There is advantage in early achievement of a Final Certification Assessment.
- Companies should not count on POA&Ms to postpone compliance.
- Not being ready when required risks highly adverse business consequences.

About the Presenter

Robert S. Metzger

Bob Metzger is an attorney in private practice with Rogers Joseph O'Donnell, PC, a boutique law firm. He heads the firm's office in Washington, D.C.

After graduating from Georgetown Law, where he was an Editor of *The Georgetown Law Journal,* Bob was a Research Fellow at what is now the Harvard Belfer Center for Science & International Affairs, where he concentrated on U.S.-Soviet issues and European security.

Bob has been recognized as a thought leader on cybersecurity and government contracts. In 2024, he was honored in Lawdragon's inaugural 500 Leading Global Cyber Lawyers guide and was named a "Top Voice" by LinkedIn. Chambers USA has recognized RJO's work, and it is the only boutique firm ranked in its exclusive Government Contracts: The Elite (USA - Nationwide) list. Bob has garnered Band 1 recognition from Chambers in USA Government Contracts: Cybersecurity (USA — Nationwide), the highest Chambers ranking an attorney can receive, and has been ranked for Government Contracts (USA – Nationwide) for 14 consecutive years.

Bob was a 2016 "Federal 100" awardee, recognized for his "ability to integrate policy, regulation and technology." As a Special Government Employee of DoD, Bob was on the Defense Science Board task force that produced the April 2017 "Cyber Supply Chain Report." He also is a co-author of influential August 2018 MITRE "Deliver Uncompromised" Report and has been a consultant to MITRE on several other projects involving cyber and supply chain security, software assurance, ransomware, digital asset crimes, and other subjects.

ROBERT METZGER
Shareholder
Rogers Joseph O'Donnell PC
rmetzger@rjo.com
https://www.linkedin.com/in/robertmetzger/
202-777-8951

Supplemental Chart

The Long History Leading to CMMC

November 2010:	Executive Order 13556 establishes a program to protect "Controlled Unclassified Information"
November 18, 2013:	Final Rule: "Safeguarding Unclassified Controlled Technical Information" (includes "-7012")
May 8, 2015:	NARA Proposed Rule (Controlled Unclassified Information)
June 19, 2015:	NIST SP 800-171: (Final)
August 26, 2015:	Interim DFARS: "Network Penetration Reporting and Contracting for Cloud Services"
December 30, 2015:	Amended Interim Rule: "Network Penetration …" (defers cyber obligation to 12/31/2017)
September 14, 2016:	NARA Final Rule, "Controlled Unclassified Information"
August 2018:	MITRE publishes "Deliver Uncompromised" Report
September 29, 2020:	CMMC Interim Final Rule (IFR) Published; Effective Nov. 30, 2020
November 2021:	CMMC 2.0 announced (5 levels compressed to 3; SP 800-171 baseline)
December 2021:	DoD publishes Level 1 and Level 2 Scoping Guidance & Assessment Guides
March 22, 2023:	Final Rule, Use of Supplier Performance Risk System (SPRS) Assessments (-7019, -7020)
December 26, 2023:	Proposed Rule 32 CFR Part 170 (CMMC 2.0) (Comments Closed Feb. 26, 2024)
May 14, 2024:	NIST SP 800-171 Rev. 3 Final
August 15, 2024:	Proposed 48 CFR Rule (CMMC contractual implementation) (Comments due Oct. 15, 2024)
October 15, 2024:	*DoD Publishes Final 32 CFR Part 170 Rule, 89 Fed. Reg. 83092*
December 16, 2024:	32 CFR Part 170 Effective Date

CMMC 2.0 Implementation Likely to Begin by Mid-2025.