CMMC Basics Training

Fall 2025

What, Why, and How?

What:

- A consistent pre-award assessment methodology to determine whether a prospective contractor has implemented cybersecurity protections necessary to adequately safeguard DoW information.

Why:

- To increase the cybersecurity posture of the DIB and better protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

How:

- All defense contractors and subcontractors will show compliance with applicable security requirements through self-assessment or independent assessment, prior to contract award (excluding Commercial-Off-The-Shelf(COTS) procurements).

CMMC Applicability

- CMMC Program requirements apply to all DoW solicitations and contracts for which a defense contractor or subcontract will process, store, or transmit FCI or CUI on its unclassified contractor information systems
  - New DoW solicitations
  - New DoW procurement instruments, including contracts, task orders, delivery orders and their associated option periods
  - As a condition to exercise an option period
  - Subcontractors are subject to flow-down requirements
- CMMC implementation will occur through new contracts awarded after the 48 CFR rule effective date of November 10, 2025.
- Incorporation in older contracts would require bilateral modification

The CMMC Program does not alter separately applicable requirements to protect FCI or CUI

FCI and CUI

FCI

Information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public or simple transactional information, such as necessary to process payments.

48 CFR 52.204-21

CUI

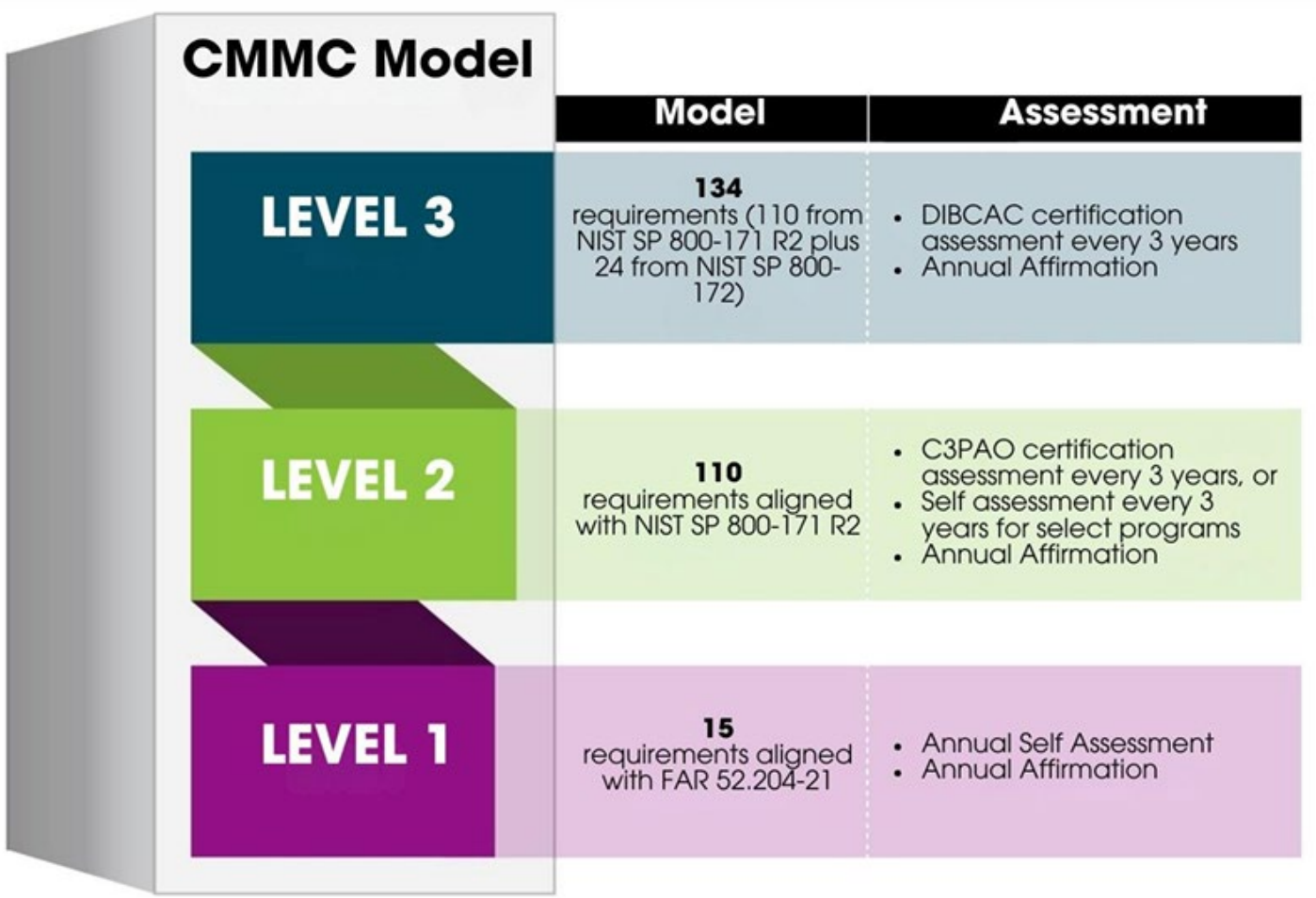
Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using **safeguarding or dissemination controls**.

32 CFR Part 2002

All CUI in possession of a government contractor or subcontractor is FCI, but not all FCI is CUI.

What are examples and what is required to receive the information?

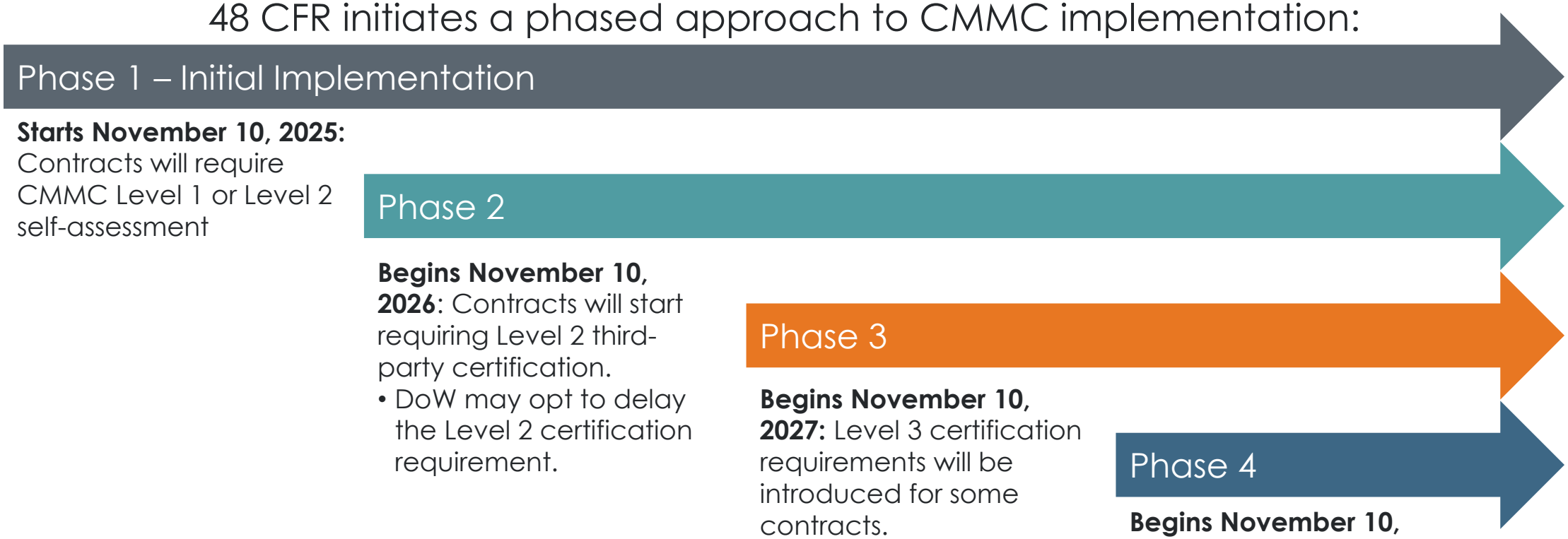
CMMC Model



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

Phased Implementation

48 CFR initiates a phased approach to CMMC implementation:



Starts November 10, 2025: Contracts will require CMMC Level 1 or Level 2 self-assessment

Begins November 10, 2026: Contracts will start requiring Level 2 third-party certification.

- DoW may opt to delay the Level 2 certification requirement.

Begins November 10, 2027: Level 3 certification requirements will be introduced for some contracts.

- DoW may opt to delay the Level 3 certification requirement.

Begins November 10, 22028: Full implementation will require CMMC certification for all relevant contracts as a condition of contract award.

Changes and Impact to Suppliers

	Non-compliance risks losing new contract opportunities		
	Covered contractor information systems with FCI	**Covered contractor information systems with CUI**	**Ongoing Responsibility**
Current State	FAR 52.204-21 requires no self-attestation	DFARS 252.204-7012 relied on self-attestation for required compliance with NIST SP 800-171 (Rev 2)	Maintain SPRS scores in accordance with DFARS 252.204-7019
Future State, CMMC 2.0 introduces tiers	Level 1 compliance; will require annual self-attestation	Level 2 certification; will require 3rd party assessment	Maintain compliance for Level 1; maintain certification for Level 2

While CMMC builds on DFARs, it significantly increases **enforcement** and **accountability**.

Note: This slide is intended as a snapshot overview of requirements does not negate compliance with any additional requirements outlined by the regulations. Suppliers must follow the required security controls based on their level, ensuring FCI and/or CUI protection.

Changes and Impact to Suppliers (cont'd)

The CMMC Program provides assessments at three levels, each incorporating security requirements from existing regulations and guidelines.

Level 1: Basic Safeguarding of FCI

- **Requirements**:
  - Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21. *(Changes to FAR clause 52.240-93 after FAR overhaul is finalized.)*

Level 2: Broad Protection of CUI

- **Requirements:**
  - Either a self-assessment or a C3PAO assessment every three years, as specified in the solicitation.
  - Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.
  - **Annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2.**

Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats

- **Requirements:**
  - Achieve CMMC Status of Final Level 2.
  - Undergo an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
  - **Provide an annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172.**