SIBC Supplier Days 2026

Cybersecurity: Your First Line of Defense - CMMC

March 3, 2026

Uncontrolled Unclassified Information

Agenda

- Introduction
- How we got here
- CMMC Levels
- CMMC Requirements
- CMMC Phased Implementation
- Applicability
- What can you the supplier do to prepare for CMMC
- Take - Aways
- CMMC Resources
- Questions?

Introduction

- Who we are:
  - Ashley Barton – Supply Chain Organization Compliance, Process Improvement, & Training Manager **(GDEB)**
  - David Tomko – Regulatory Compliance Analyst. Sr (Security Rep) **(GDEB)**
  - William Barnes – Chief Information Security Officer **(GDEB)**
  - Kendra Queeney – Director, Supply Chain Management **(HII)**

- Why we are here
  - Highlight what CMMC means for suppliers
  - Help you better understand how to prepare for CMMC

How we got here

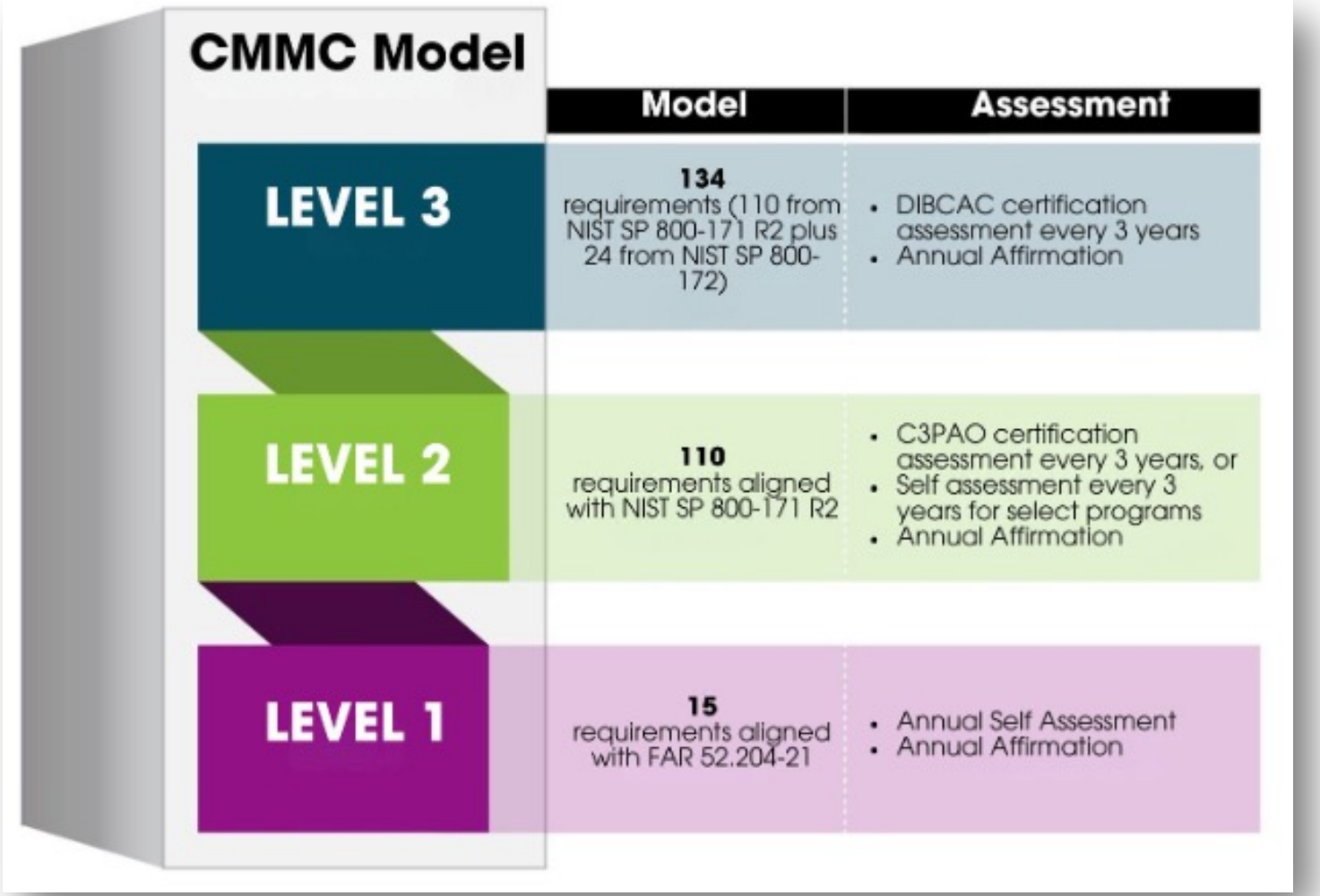
- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) - Aug 2015
- DFARS 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements) - Sept 2020
- DFARS 252.204-7020 (NIST SP 800-171 DoD Assessment Requirements) - Nov 2020
- DFARS 252.204-7021 (Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements) - Nov 2025

CMMC Levels

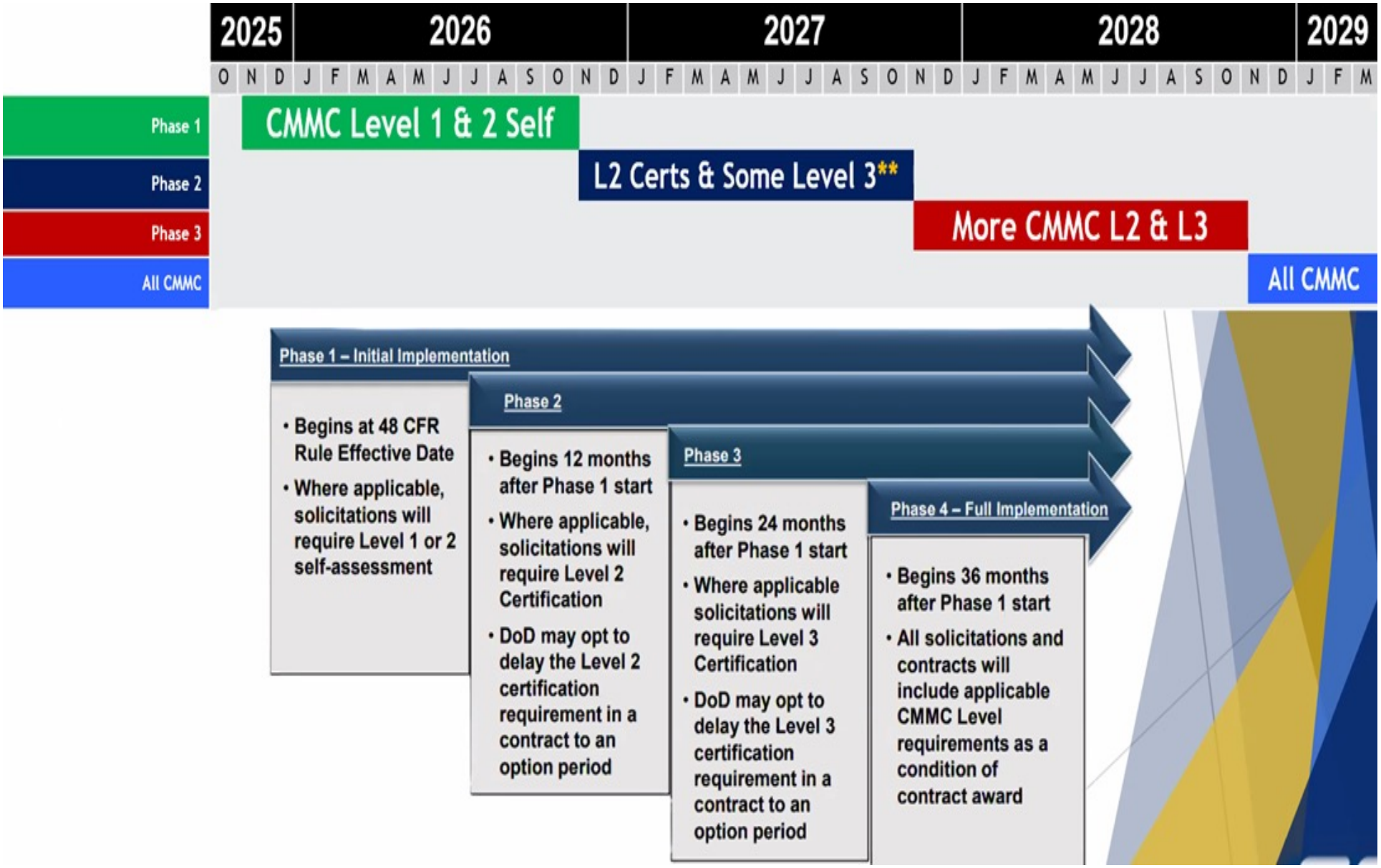
Tiered Model: Security requirements scale with sensitivity of data

Assessments: Verifies compliance through independent review

Contracts: Certification required to win and hold work



CMMC Phased Implementation



Applicability

- **All** DoD solicitations and contracts when a contractor or subcontractor will process, store, or transmit FCI or CUI on unclassified contractor information systems
- Required for **BOTH** Domestic and Foreign Suppliers
- CMMC Status will be specified by DoD in the solicitation and contract
- Exceptions
  - Contracts exclusively for commercially available off-the-shelf (COTS) items
  - Does not apply to Federal information systems operated by contractors or subcontractors on behalf of the Government

What can you do to prepare for CMMC?

- Review the 110 NIST controls
- Validate you have closed out your POAM
- Compile OQE to validate NIST compliance for C3PAO audit
- Potentially engage with outside consultants
- Begin scheduling your C3PAO audit
- Continue to monitor CMMC news

Take-Aways

- NIST requirements should not be new
- Full compliance with NIST 800-171 Rev 2 should be a priority
  - 110 security requirements
- Primes are responsible for ensuring subcontractor/supplier CMMC certification or self-assessment compliance prior to subcontract award
- Initial and annual affirmations of continuous compliance will be required
- CMMC requirements in solicitations and contracts will start November 10, 2025

Any Questions?

Thank you

Provided, Not Presented

CMMC Resources

Resources

- **DIB SCC CyberAssist CMMC**
  - DIB SCC CyberAssist CMMC is an extension of the CyberAssist program, specifically focused on helping DIB companies achieve CMMC Levels 1-3. It offers resources and support for companies to prepare for and achieve CMMC compliance.

Services you can engage with

- **Apex Accelerators**
  - Apex Accelerators are a technology accelerator that provides resources and support to help small businesses CMMC compliance. Please note that Apex Accelerators is not a CMMC certification body, but rather a partner that can help small businesses prepare for and achieve CMMC compliance.
- **Project Spectrum**
  - Project Spectrum is a DoD initiative aimed at improving the security and management of Controlled Unclassified Information (CUI). It provides a framework and tools to help DoD agencies and contractors manage CUI.
- **DoD CUI Program**
  - The DoD CUI Program is a DoD initiative that governs the handling and management of Controlled Unclassified Information (CUI) within the DoD. It establishes policies and procedures for CUI classification, marking, and declassification, but it is not directly related to CMMC compliance.

CMMC Asset Categories

You need an **accurate inventory** of your assets before you can work on protecting it.

Asset categorization is the **foundation** of CMMC readiness

CUI Assets: Systems, devices, or tools that process, store, or transmit CUI. Think of them as the places where sensitive contract-related data lives. (*e.g., a virtual or physical workstation used by authorized personnel to access CUI related to a government contract*)

Security Protection Assets (SPAs): Systems or tools that protect CUI assets, like firewalls, antivirus software, or authentication systems. (*e.g., a firewall that prevents unauthorized access to a server holding CUI*)

Contractor Risk Managed Assets (CRMAs): Company-owned systems that don't touch CUI directly but still connect to your network. You decide how to manage the risk they pose. (*e.g., a company-issued laptop used by a project manager to access internal business systems which is on the same enterprise network, but doesn't process, store, or transmit CUI*)

Specialized Assets: Non-traditional devices like smart sensors or industrial machines that are hard to secure using standard methods. (*e.g., a CNC machine connected to a network that can't run antivirus software*)

Out-of-Scope Assets: Assets that have no connection at all to CUI or the systems that protect it. They're completely outside of the CMMC boundary (*e.g., a visitor check-in kiosk located in the building lobby*)

Provided, Not Presented

CMMC Requirements

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	• Conducted by Organization Seeking Assessment (OSA) annually • Results entered into the Supplier Performance Risk System (SPRS)	• Not permitted	• After each assessment • Entered into SPRS
Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 2 (C3PAO)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by DIBCAC every 3 years • Results entered into CMMC eMASS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS

Protecting Sensitive Information

It is everyone's responsibility to protect sensitive information. Three common forms of information distributed or received by NNS are:

- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)
- Unclassified Naval Nuclear Propulsion Information (U-NNPI)

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

U-NNP

Unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.

NNPI is a sub-set of CUI with stricter requirements, as outlined in OPNAV N9210.3.