SLIDES ONLY

NO SCRIPT PROVIDED

CLEARED
For Open Publication

Jan 21, 2025

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

CMMC Alignment to NIST Standards

How the Requirements Fit Into the Assessment Framework

February 2025

Agenda

- Overview of Cybersecurity Maturity Model Certification (CMMC) Program
- Alignment to National Institute of Standards (NIST) Special Publication (SP) 800-171 Revision (Rev.) 2
- Scoring in NIST SP 800-171 Rev. 2 (Including Multi-Factor Authentication (MFA) and Federal Information Processing Standards (FIPS) Partial Scores)
- NIST SP 800-172 Alignment and Organization-Defined Parameters (ODPs)
- Transition to NIST SP 800-171 Rev. 3
- Takeaways
- Q&A

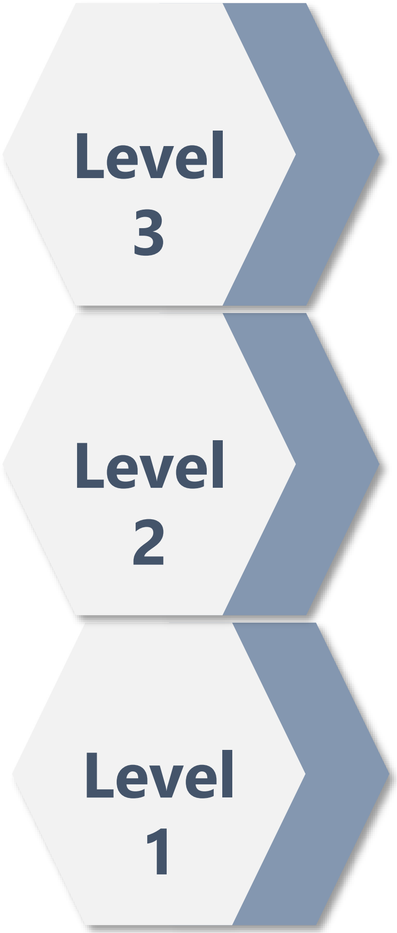
CMMC Overview

What is CMMC?

- A DoD framework ensuring protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Why Align to NIST Standards?

- Leveraging existing federal requirements, efficiency, and risk mitigation.



Level 3

NIST SP 800-172
24 Additional Security Requirements

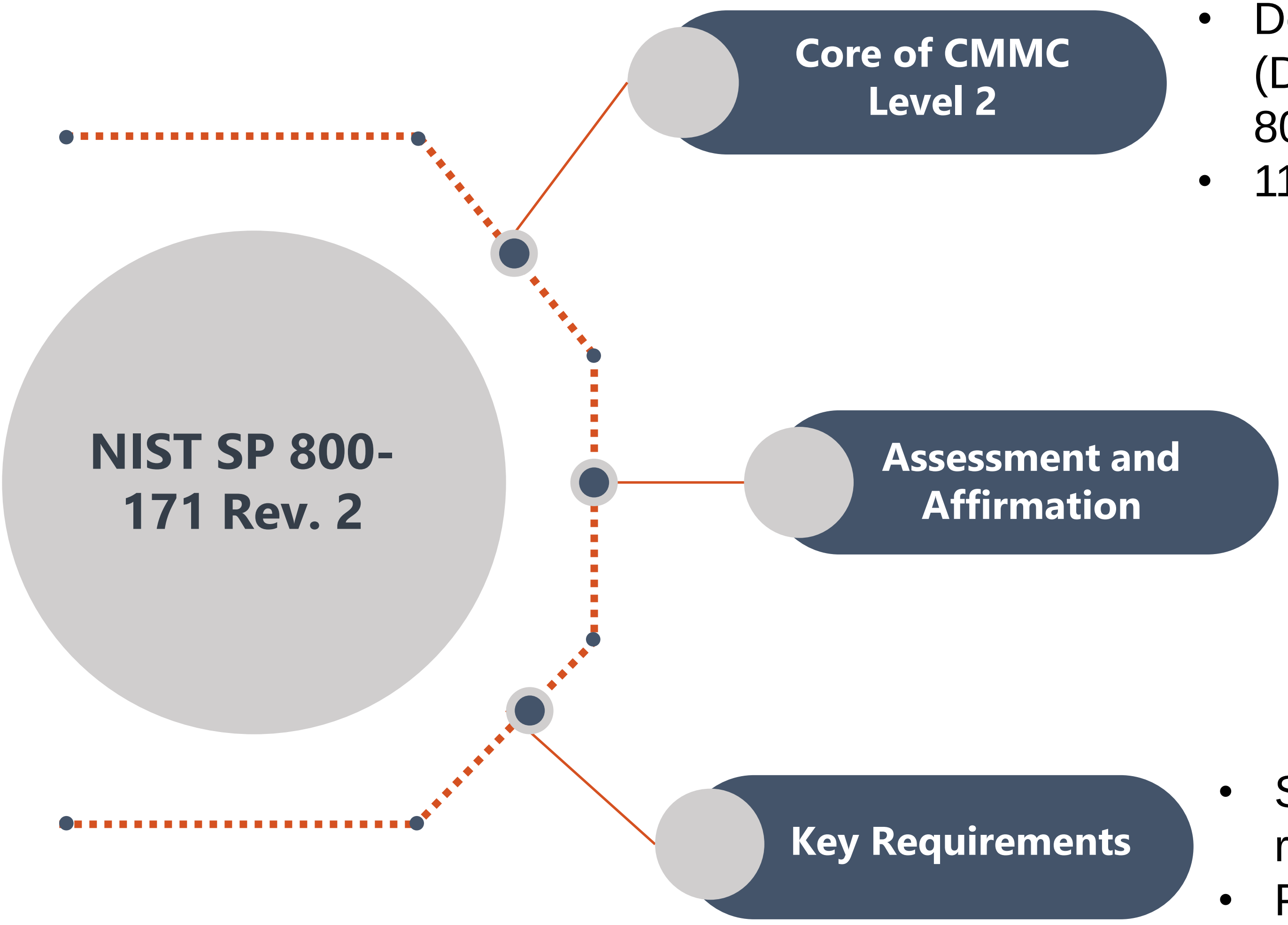
Level 2

NIST SP 800-171 Rev 2
110 Security Requirements

Level 1

FAR 52.204-21
15 Security Requirements

Alignment to NIST SP 800-171 Rev. 2



Core of CMMC Level 2

- Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 requires NIST SP 800-171 Rev. 2.
- 110 Security Requirements across 14 families.

Assessment and Affirmation

- Ensures consistent baseline implementation of safeguards for protecting CUI.
- Self-assessments and third-party assessments (C3PAOs) validate compliance.

Key Requirements

- System Security Plan (SSP): How security requirements are met.
- Plan of Action & Milestones (POA&M): Addressing gaps (conditional compliance).

NIST SP 800-171 Rev. 2 Scoring and Partial Scores

- **Scoring System**
  - Based on DoD Assessment Methodology, assessing NIST SP 800-171A objectives.
  - Maximum score: 110 points.
  - Deductions for unmet requirements (critical requirements must be fully met).
  - Security requirements are valued 1, 3, or 5 points with a range of -203 to 110, with a minimum passing score of 88. Partial credit is allowed for two requirements:
    - MFA: 5 points deducted from overall score of 110 if MFA is not implemented or implemented only for general users and not remote and privileged users;
    - MFA: 3 points deducted if MFA is implemented for remote and privileged users but not implemented for general users;
    - FIPS: 5 points deducted from overall score of 110 if no cryptography is employed;
    - FIPS: 3 points deducted if cryptography is employed but not FIPS validated.

Alignment to NIST SP 800-172 and ODPs

- **CMMC Level 3**
  - 24 Enhanced Security Requirements derived from NIST SP 800-172.
  - Targets Advanced Persistent Threats (APTs).
  - CMMC Level 3 first requires CMMC Status of Final Level 2 (CMMC Third-Party Assessment Organization)
- **Organization-Defined Parameters (ODPs)**
  - ODPs allow organizations to tailor specific security values to meet mission needs.
  - Flexibility for organizations while meeting the intent of the security controls.
- NIST SP 800-172 supplements and enhances NIST SP 800-171 Rev. 2.

Transition to NIST SP 800-171 Rev. 3

- **Rulemaking Process for NIST SP 800-171 Rev. 3**
  - DoD will formally adopt Rev. 3 through future rulemaking.
  - DFARS 7012 Class Deviation: Assessments remain against Rev. 2 until Rev. 3 is officially adopted.
  - A new scoring methodology will be developed.

- **Voluntary Transition to Rev. 3**
  - Organizations can proactively implement Rev. 3.
  - Key Condition: Must still meet Rev. 2 requirements for compliance and assessments.

- **Key Changes in Rev. 3**
  - Added flexibility via ODPs.
  - Increased focus on resilience and advanced threat protections.

Practical Guidance for Transitioning to Rev. 3

- **Preparation Steps:**
  - Review gap analysis between Rev. 2 and Rev. 3.
  - Update SSPs and security controls accordingly.
  - Maintain current compliance with Rev. 2 while aligning systems with Rev. 3.

Key Takeaways

- CMMC Level 2 aligns fully with NIST SP 800-171 Rev. 2.
- Scoring includes partial credit for MFA and FIPS implementation.
- CMMC Level 3 incorporates NIST SP 800-172 and uses ODPs for flexibility.
- Transition to Rev. 3 will occur via rulemaking.
- Continuous compliance with current requirements is critical.

DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER

Questions?

DOD CHIEF INFORMATION OFFICER
FULCRUM
IT ADVANCEMENT STRATEGY