DLA
DEFENSE LOGISTICS AGENCY
*Established 1961*

The Nation's Combat Logistics Support Agency

# CMMC

Shivane Patel, DLA HQ (J72)
April 23-24, 2024

- What is CMMC?
- Background & History
- Current Related Requirements
- Published Rule(s)
- CMMC Requirements
- Timeline
- Compliance Steps
- DOJ – Civil Cyber Fraud Initiative
- Resources
- Q&A

# Cybersecurity Maturity Model Certification

- **What is CMMC?**
  - DoD's effort to increase the overall cybersecurity posture of the Defense Industrial Base (DIB) and supply chain
    - Cybersecurity framework concerned with how a contractor controls information on its IT systems/networks
  - Tiered Model
    - Cumulative maturity model - builds additional practices at each successive level
  - Assessment Requirements
    - Self assessments
    - Third-party (C3PAO) assessments
    - Government assessments
  - Implemented through contracts

- **What does this mean for contractors?**
  - CMMC compliance will be critical to winning business with DoD
  - Unified cybersecurity standard for all DoD contractors

- **2010** - The beginnings of CMMC started with Executive Order (EO) 13556
  - The intent of this EO was to establish an open and uniform program for managing unclassified information that requires safeguarding or dissemination controls
- **2019** - DoD announced the development of CMMC in order to move away from a "self-attestation" model of security
  - Interim rule became effective on 30 November 2020
  - Initially established a five-year phase-in period
  - In response to approximately 750 public comments on the CMMC 1.0 program DoD initiated an internal review of CMMC's implementation
- **2021** - In November DoD announced CMMC 2.0
  - Updated program structure and requirements designed to achieve the primary goals of the internal review
- **December 2023 – 2024** - CMMC 2.0 Proposed Rules (Title 32 & 48)

## Reminder of What is Still Required

- **DFARS 252.204-7012**
  - Implement NIST 800-171
  - Have NIST-conformant SSP
  - Work on POA&M
  - Obtain medium assurance certificate

- **DFARS 252.204-7019**
  - At a minimum conduct NIST 800-171 Basic (Self) Assessment in accordance with NIST 800-171A
  - Post Basic Assessment information to SPRS
  - Potential DIBCAC Medium & High Assessments

- **DFARS 252.204-7020**
  - Ensure applicable subcontractors also have results of a current assessment posted in SPRS prior to awarding a subcontract
  - Requires contractors to provide access to its facilities, systems, and personnel when necessary for DoD to conduct or renew a higher-level assessment

## Title 32 Part 170 of the Code of Federal Regulations (CFR)

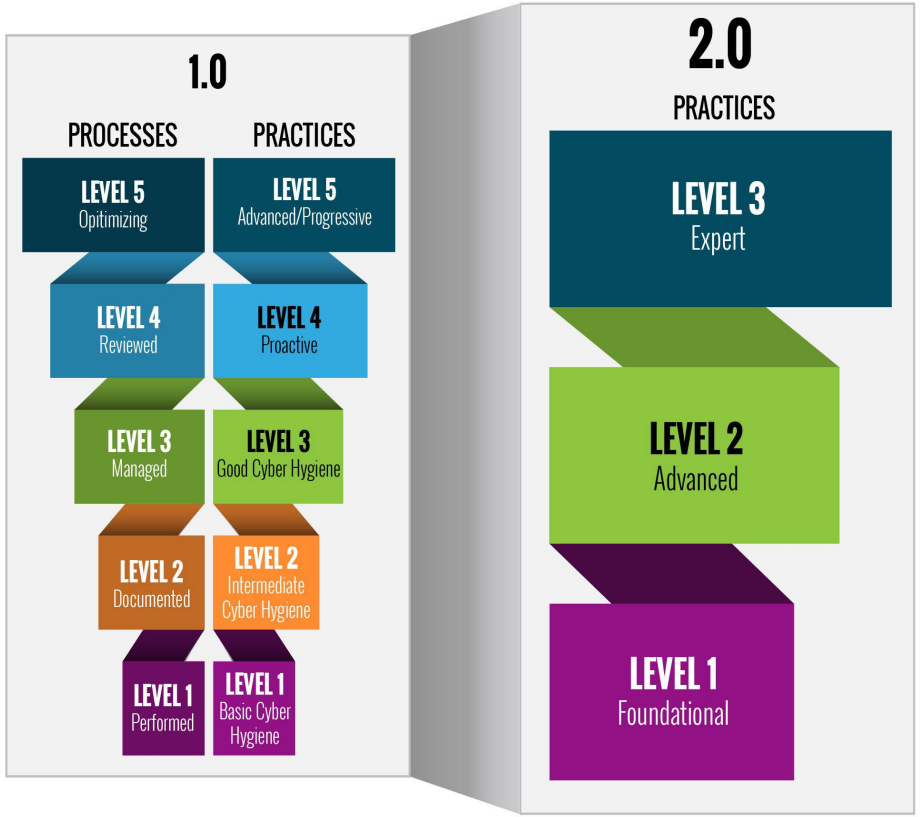
- Proposed Rule
  - Title - Cybersecurity Maturity Model Certification (CMMC) Program
  - Sets CMMC program requirements
  - Publication Date:  December 26, 2023

## Title 48 CFR (DFARS Case 2019–D041)

- Proposed Rule
  - Publication Date: TBD (release pending)
  - Implementation of the CMMC program requirements through DFARS clause 252.204-7021 in DoD contracts

- DoD agencies (requiring activities & program office) will determine the applicable CMMC level for each procurement
- Based on the level required in the solicitation contractors will be required to obtain a CMMC certification prior to contract or subcontract award
- 3 increasingly progressive levels

## CMMC Model Structure



## Level 1

- Application:  Contracts involving Federal Contract Information (FCI) only
  - FCI involves information that is not marked as public or for public release
- Compliance:  FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems
  - This clause applies to most FAR based contracts
  - Mandates compliance with 15 security requirements (very basic cybersecurity hygiene)
- Contractors must fully meet all 15 security requirements
- No plan of action and milestones (POA&Ms) permitted
- Flow down to subcontracts that include FCI

## Level 2 Self Assessment

- Application:  Contracts involving Controlled Unclassified Information (CUI)
- Compliance: NIST SP 800-171 Rev 2 (110 security controls)
  - Mirrors existing contractor obligations to protect CUI under DFARS 252.204-7012
- POA&Ms permitted only on select controls
  - Must be closed within 180 days of the assessment
- Results of self-assessment will continue to be submitted into SPRS
- Flow down to subcontracts that include CUI

## Level 2 Certification Assessment

- Application:  Contracts involving CUI
- Compliance:  NIST SP 800-171 Rev2 (110 security controls)
  - Mirrors existing contractor obligations to protect CUI under DFARS 252.204-7012
- Verification of compliance through an authorized third party C3PAO
- POA&Ms are permitted for a very limited number of controls
  - Only permitted if a contractor achieves a particular assessment score
  - Must be closed within 180 days of initial assessment
- Certification valid for 3 years
  - Certification results will be entered by the third-party C3PAO into eMASS and will transmit the final results into SPRS
- Flow down to subcontracts that include CUI

# Level 3 Certification Assessment (Gov't & C3PAO)

- Application:  Contracts involving CUI
- Compliance:  NIST SP 800-171 Rev2 (110 security controls) & NIST SP 800-172
  - Requires a final CMMC level 2 certification assessment
- DCMA DIBCAC (Gov't) will perform level 3 assessment
- POA&Ms are permitted for a limited number of controls
  - Only permitted if a contractor achieves a particular assessment score
  - Must be closed within 180 days of initial assessment
- Conditional Certification Assessment vs. Final Certification Assessment (achievement of minimum score & no open POA&Ms)
- Level 3 certification assessment valid for 3 years
  - Certification results will be entered by the third-party C3PAO into eMASS and will transmit the final results into SPRS
- Flow down to subcontracts that include CUI

## Affirmations

- Required annually for each CMMC level
- Senior organization official must affirm that the organization is satisfying and will maintain the requirements of the specified CMMC level
- Submitted in SPRS
- A new affirmation is required at the time a new CMMC level is achieved
- See section 170.22 for full details on the affirmation procedure

- The proposed CMMC 32 CFR rule contemplates a phased implementation in which CMMC level requirements will be included in solicitations spanning 4 phases over a 3-year period
- **Initial Phase in Period**
  - The discretion to include the CMMC requirement in DoD solicitations and contracts given to the DoD agencies (requiring activities and program procuring offices)
- **Post Phase in Period**
  - After the phase in 3-year period the CMMC requirement will apply to ALL DoD FCI and CUI contracts

- **Phase 1** (**0-6 Months)** - Begins when DFARS 252.204-7021 is finalized as part of the Title 48 Rule DFARS Case 2019–D041
  - DoD will include level 1 Self-Assessment or CMMC Level 2 Self-Assessment requirements as a condition of contract award and *may* include such requirements as a condition to exercising an option on an existing contract
  - DoD may also include CMMC level 2 Certification Assessment requirements as it deems necessary for applicable solicitations and contracts
- **Phase 2 (6-18 Months)** - Begins 6 months after the start date of Phase 1 and will last for 1 year
  - DoD will include CMMC level 2 Certification Assessment requirements as a condition of contract award for applicable contracts involving CUI and may include such requirements as a condition to exercising an option on an existing contract
  - DoD may also include CMMC level 3 Certification Assessment requirements as it deems necessary for applicable solicitations and contracts

- **Phase 3 (18-30 Months)** - Begins 18 months after the start date of Phase 1 and will also last for 1 year
  - DoD intends to include CMMC level 3 Certification Assessment requirements for all applicable DoD solicitations and contracts as a condition of contract award, but DoD may delay inclusion of these requirements to an option exercise as it deems appropriate

- **Phase 4 Full Implementation (30+ months)** - Begins 30 months after the start date of Phase 1
  - Involves the inclusion of all CMMC program requirements in ALL DoD solicitations and contracts that contain CUI or FCI including option periods

# Compliance Steps


- **Step 1 - Education and Analysis**
  - Educate all stakeholders in your organization AND across the supply chain
  - Executives must understand impacts
  - Perform CUI data analysis
    - Understand the CUI you are working with
    - How CUI is being received, stored, processed, and shared
    - Who has access to CUI
    - Conduct gap analysis at the requirement level (110 items)
- **Step 2 - Develop a compliant SSP and POA&M based on analysis**
  - Follow NIST CUI SSP template at a minimum, including all sections in NIST 800-171
  - Align with assessment/certification evidence required (based on NIST 800-171A for Basic (self) assessment score)
- **Step 3 - Submit NIST 800-171 Basic (self) assessment score report to SPRS** (update when status changes)

# Compliance Steps (Continued)


- **Step 4 – POA&M Mitigations**
  - Implement any required mitigations according to the POA&M, including all necessary documentation and prioritizing your implementations around the requirements that bring the greatest reduction in security risk
- **Step 5 - Gather evidence needed to conduct NIST 800-171 Security Controls Assessment**
  - Complete all 320 assessment objectives to validate compliance with NIST 800-171
- **Step 6 - Obtain CMMC certification** at the required level (plan as if you expect a third-party assessment)

- DOJ has announced new Civil Cyber Fraud Initiative
- Government will use False Claims Act (FCA) to prosecute DoD contractor cybersecurity misrepresentations
- May lead to increase in whistleblower and bid protest actions

*"The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."*

*- Department of Justice, Office of Public Affairs, October 6, 2021*

- FAR - Federal Acquisition Regulation: https://www.acquisition.gov/browse/index/far
- DFARS - Defense Federal Acquisition Regulation Supplement: https://www.acquisition.gov/dfars
- Title 32 Rule: https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program
- DoD NIST SP 800-171 Assessment Methodology Rev 3: https://csrc.nist.gov/pubs/sp/800/171/r3/fpd
- CMMC - Cybersecurity Maturity Model Certification: https://dodcio.defense.gov/CMMC/
- CMMC Proposed Rule Overview Video: https://www.dvidshub.net/video/912871/cybersecurity-maturity-model-certification-cmmc-proposed-rule-overview
- CMMC-AB - CMMC Accreditation Body: https://cmmcab.org/
- Project Spectrum is a nonprofit effort funded by the DoD Office of Small Business Programs to help educate the Defense Industrial Base (DIB) on compliance with this requirement: https://www.projectspectrum.io/
- PTAC: https://www.dla.mil/SmallBusiness/PTAP/

- DoD CUI registry, training, and resources: https://www.dodcui.mil
- DoD Instruction 5200.48 for CUI: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF
- NIST 800-172: https://csrc.nist.gov/publications/detail/sp/800-172/final
- SPRS - Supplier Performance Risk System: http://www.sprs.csd.disa.mil
- PIEE - Procurement Integrated Enterprise Environment: https://piee.eb.mil
- DC3 - Defense Cyber Crime Center: https://www.dc3.mil/
- DIBNet - Defense Industrial Base Network: https://dibnet.dod.mil/portal/intranet/
- FCA – False Claims Act - see DOJ Announcement at: https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

# Questions?