Cybersecurity Maturity Model Certification

Version 2.0

Overview Briefing

December 3, 2021

Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

DISTRIBUTION A. Approved for public release

CMMC 2.0 Model

CMMC 2.0 model is streamlined to three versus five levels

- **Eliminates CMMC 1.0 Levels 2 and 4:** Developed as transition levels and never intended to be assessed requirements
- **Establishes three progressively sophisticated levels, depending on the type of information:**
  - Level 1 (Foundational) – for companies with FCI only; information requires protection but is not critical to national security
  - Level 2 (Advanced) – for companies with CUI
  - Level 3 (Expert) – for the highest priority programs with CUI

Requirements will mirror NIST SP 800-171 and NIST SP 800-172

- **Eliminates all CMMC unique practices and maturity processes:** Work with NIST to address identified gaps in the NIST SP 800-171
- **Aligns Level 2 with NIST SP 800-171**
- **Level 3 will use a subset of NIST SP 800-172 requirements**

Simplifies the CMMC standard for companies, while safeguarding critical Department information

DISTRIBUTION A. Approved for public release

CMMC 2.0 Assessments

CMMC Level 1 (Foundational) will require DIB company self-assessments

CMMC Level 2 (Advanced) may require third-party or self-assessments, depending on the type of information

- **Requires third-party assessments for prioritized acquisitions:** Companies will be responsible for obtaining an assessment and certification prior to contract award
- **Requires self-assessments for other non-prioritized acquisitions:** Companies will complete and report a CMMC Level 2 self-assessment and submit senior official affirmations to SPRS

CMMC Level 3 (Expert) will be assessed by government officials

Eases assessment requirements for companies not handling information related to prioritized acquisitions

DISTRIBUTION A. Approved for public release

Allowance of POA&Ms and Waivers

CMMC 2.0 will allow limited use of POA&Ms

- **Strictly time-bound:** Potentially 180 days; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Limited use:** Will not allow POA&Ms for highest-weighted requirements; will establish a "minimum score" requirement to support certification with POA&Ms

Waivers will be allowed on a very limited basis, accompanied by strategies to mitigate CUI risk

- **Only allowed in select mission critical instances:** Government program office will submit the waiver request package including justification and risk mitigation strategies
- **Strictly time bound:** Timing to be determined on a case-by-case basis; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Will require senior DoD approval** to minimize potential misuse of the waiver process

Limited use of POA&Ms and waivers could allow the Department and DIB companies flexibility to meet evolving threats and make risk-based decisions

DISTRIBUTION A. Approved for public release

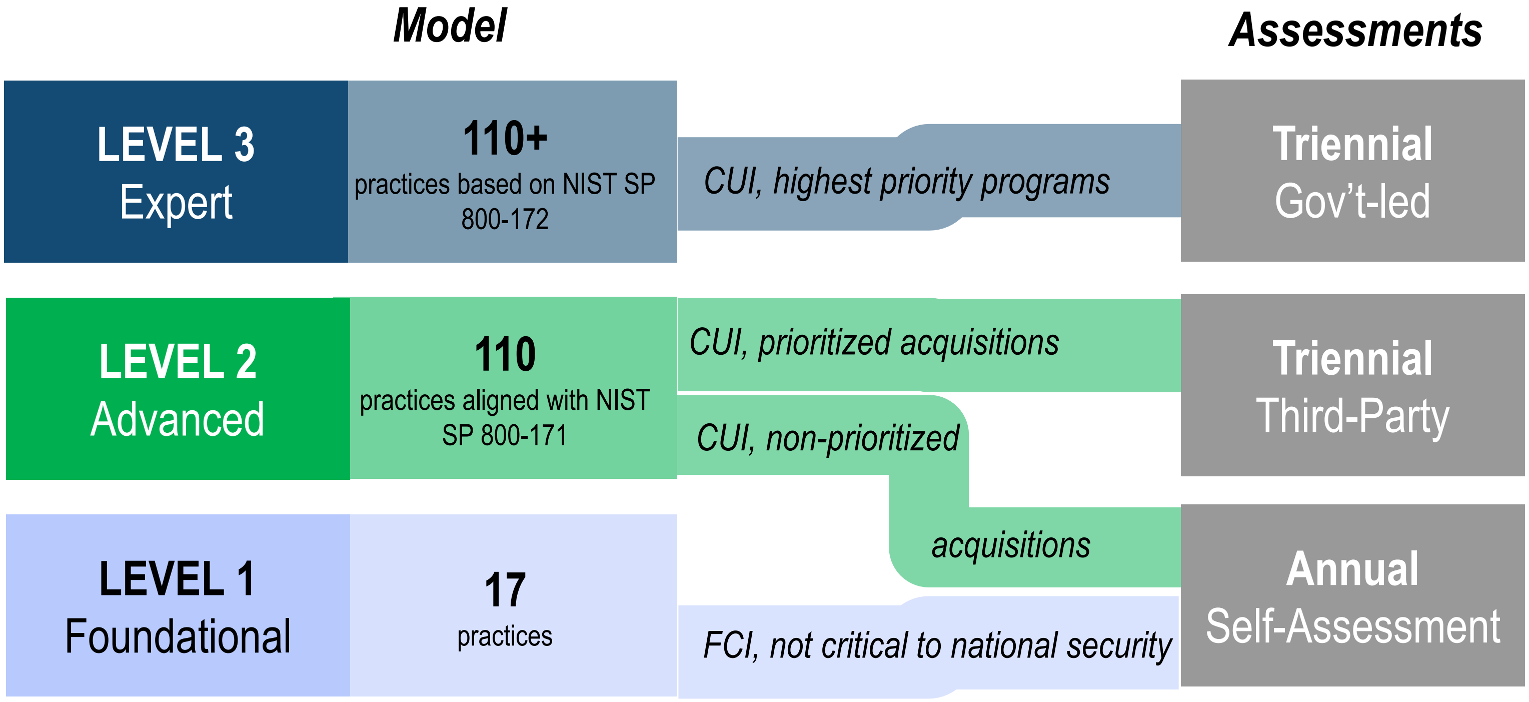
Rulemaking – Codifying CMMC 2.0

Changes will be released through a interim rule. A 60-day public comment period and concurrent congressional review will be included prior to the rule becoming effective

- DoD has **mandatory rulemaking obligations** for CMMC that must be addressed as part of the CMMC 2.0 implementation
  - Rulemaking under 32 CFR is required to establish the CMMC program
  - Rulemaking under 48 CFR is required to update the contractual requirements in the DFARS to implement the CMMC 2.0 program
  - The DoD is suspending the CMMC Piloting effort and mandatory CMMC certification
- Timeline to complete all rulemaking requirements will be 9 to 24 months; includes a mandatory 60-day public comment period and concurrent congressional review
  - The DoD will continue to encourage the DIB sector to enhance their cybersecurity posture during the interim period
  - The Department is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC 2.0 Level 2 certification in the interim period
  - Until rulemaking formally implements CMMC 2.0, the DIB's participation in CMMC will be voluntary

DISTRIBUTION A. Approved for public release

CMMC 2.0 tailors model and assessment requirements to the type of information being handled



Model

Assessments

LEVEL 3 Expert

110+ practices based on NIST SP 800-172

CUI, highest priority programs

Triennial Gov't-led

LEVEL 2 Advanced

110 practices aligned with NIST SP 800-171

CUI, prioritized acquisitions

Triennial Third-Party

CUI, non-prioritized acquisitions

LEVEL 1 Foundational

17 practices

FCI, not critical to national security

Annual Self-Assessment

Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

DISTRIBUTION A. Approved for public release

Questions?