Cybersecurity Maturity Model Certification

Overview

February 2023

CMMC 2.0 Overview

Note: The information in this presentation reflects the Department's strategic intent with respect to the Cybersecurity Maturity Model Certification (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.

CMMC 2.0 Framework

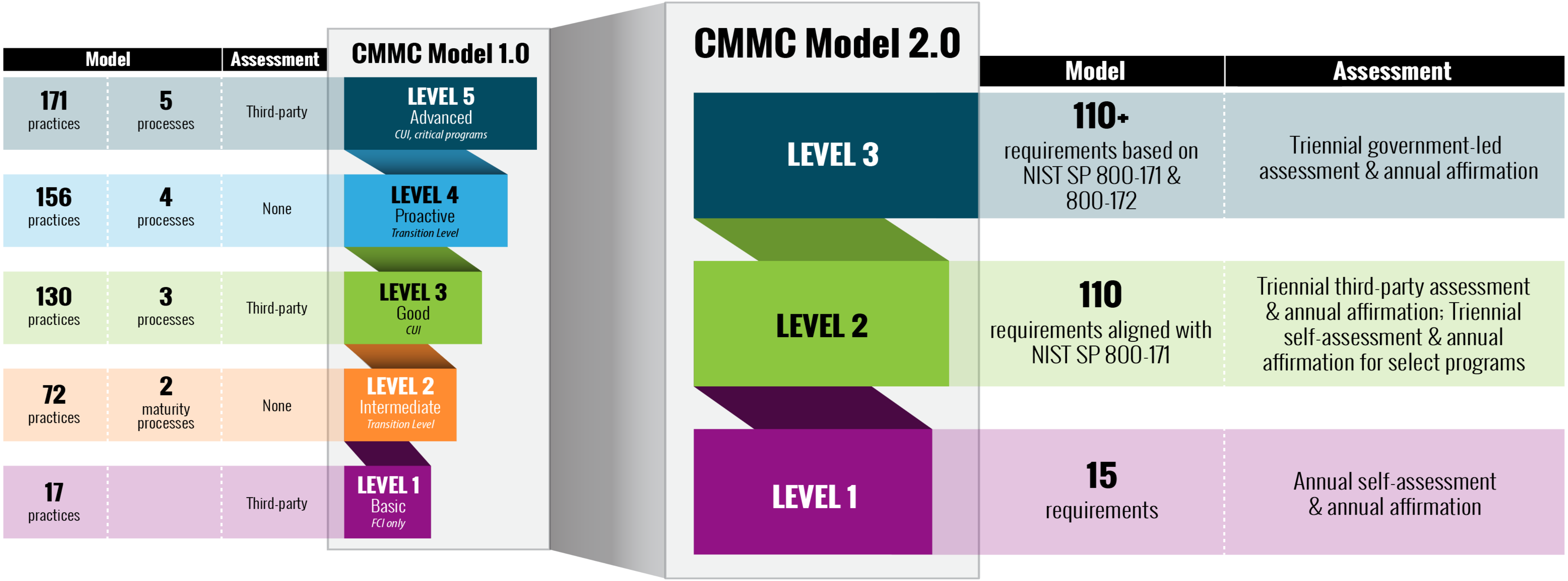
The CMMC Program provides a consistent methodology for DoD's pre-award assessment of a prospective contractor's implementation of required cybersecurity protections to enhance the cybersecurity posture of the Defense Industrial Base (DIB)

- DoD is migrating to the new CMMC framework as a requirement for contract award
- All DIB companies and subcontractors will need to comply with applicable CMMC requirements to conduct business with the DoD (excludes Commercial-Off-The-Shelf (COTS) procurements)

Origins

- NIST SP 800-171
- NIST SP 800-172

CMMC 2.0 Streamlines Overall Framework and Requirements



Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3	110+ requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171	Triennial third-party assessment & annual affirmation; Triennial self-assessment & annual affirmation for select programs
LEVEL 1	15 requirements	Annual self-assessment & annual affirmation

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.

CMMC 2.0 Assessments

CMMC Level 1

CMMC Level 1: will require DIB company self-assessments

CMMC Level 2

CMMC Level 2: may require either third-party or self-assessments, depending on the type of information processed, transmitted, or stored on non-federal information systems

- Requires third-party assessments for prioritized information: Companies will be responsible for obtaining an assessment and certification prior to contract award
- Requires self-assessments for other non-prioritized information: Companies will complete and report a CMMC Level 2 self-assessment and submit senior-official affirmations to the Supplier Performance Risk System (SPRS)

CMMC Level 3

CMMC Level 3: will require assessment by government officials

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

Post-Assessment Remediation and Waivers

❑ CMMC Program will allow limited use of POA&Ms

- **Strictly time-bound:** Contracting Officers can use normal contractual remedies to address a DIB contractor’s failure to meet their cybersecurity requirements after the defined timeline (TBD during rulemaking)
- **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

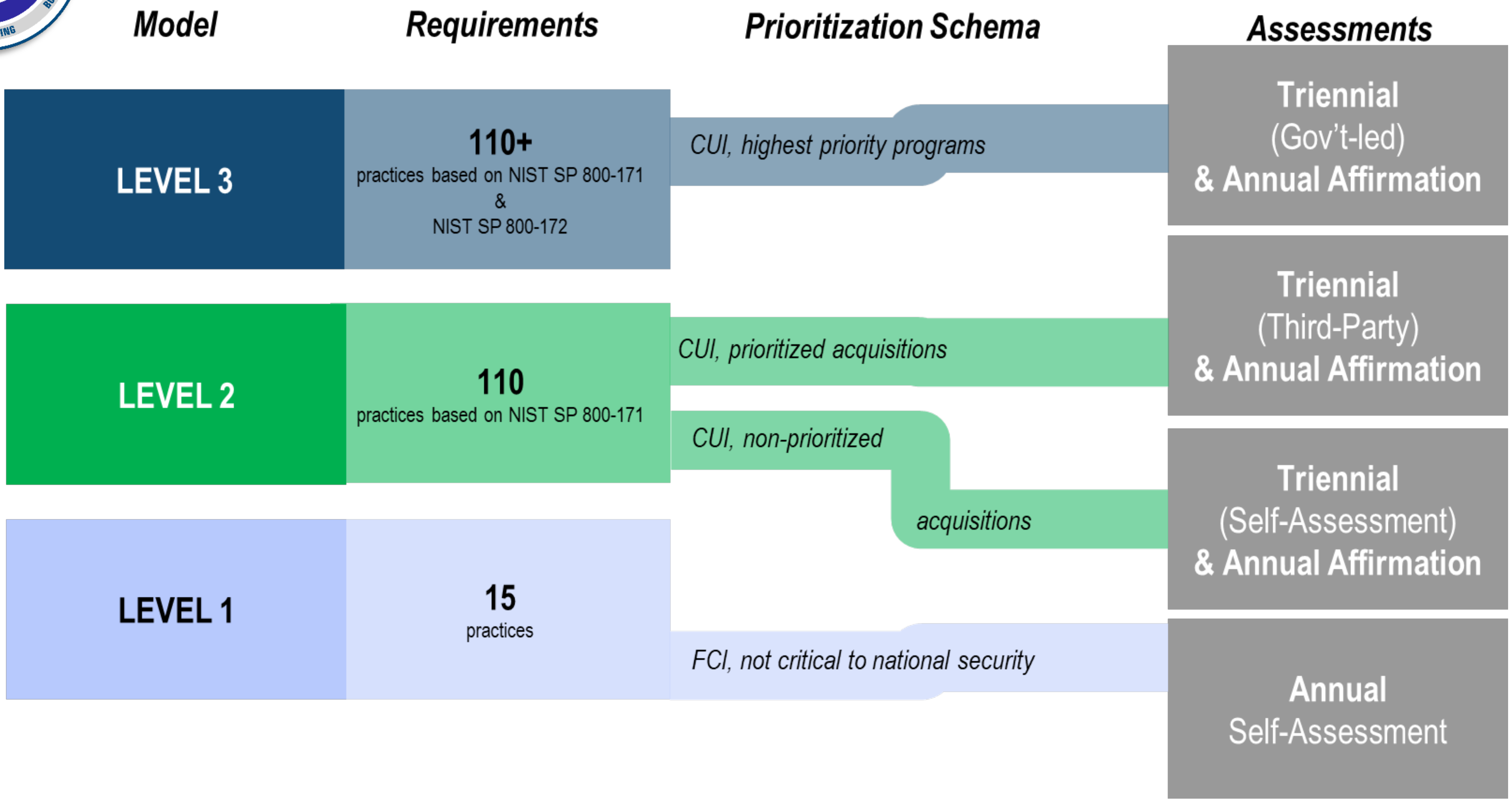
- **Only allowed in select mission-critical instances.** Government program offices will seek Service Acquisition Executive approval to exclude CMMC requirements from RFP
- **Will require senior DoD approval** to minimize potential misuse of the waiver process

Limited use of POA&Ms and waivers could allow the Department and DIB companies more flexibility to meet evolving threats

Questions?

Backup

CMMC Assessment Requirements Align to the Type of Information Being Handled



Model

Requirements

Prioritization Schema

Assessments

LEVEL 3

110+
practices based on NIST SP 800-171
&
NIST SP 800-172

CUI, highest priority programs

Triennial
(Gov't-led)
& Annual Affirmation

LEVEL 2

110
practices based on NIST SP 800-171

CUI, prioritized acquisitions

Triennial
(Third-Party)
& Annual Affirmation

CUI, non-prioritized
acquisitions

Triennial
(Self-Assessment)
& Annual Affirmation

LEVEL 1

15
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.

CMMC PMO