CMMC 2.0: Our Take

The CMMC-AB is supportive of the changes proposed in CMMC 2.0

- There is now a defined way forward for CMMC
- DoD employed a risk-management approach and addressed the issues they said they would
- CMMC 1.0 had formidable implementation challenges
- CMMC 2.0 supports an incentivized interim, voluntary program during Federal rulemaking
- DoD reaffirmed the CMMC Accreditation Body's role
- **There is still tremendous business opportunity for RPs and RPOs within CMMC**
- **The CMMC-AB needs to be more active in enabling all professions within the CMMC Ecosystem for success**

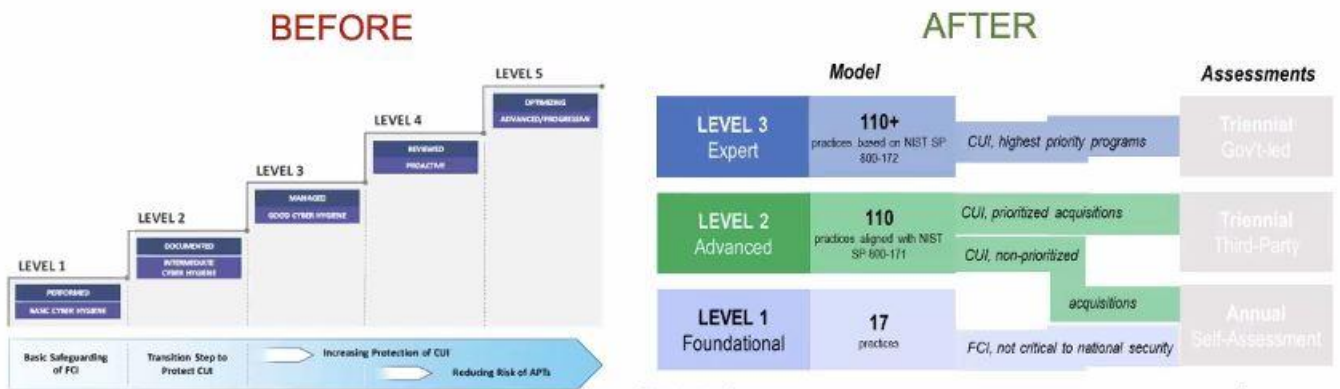
CMMC 2.0 Drivers

On November 4th, DoD announced major changes to the CMMC program following a six-month internal program review driven by four (4) general objectives

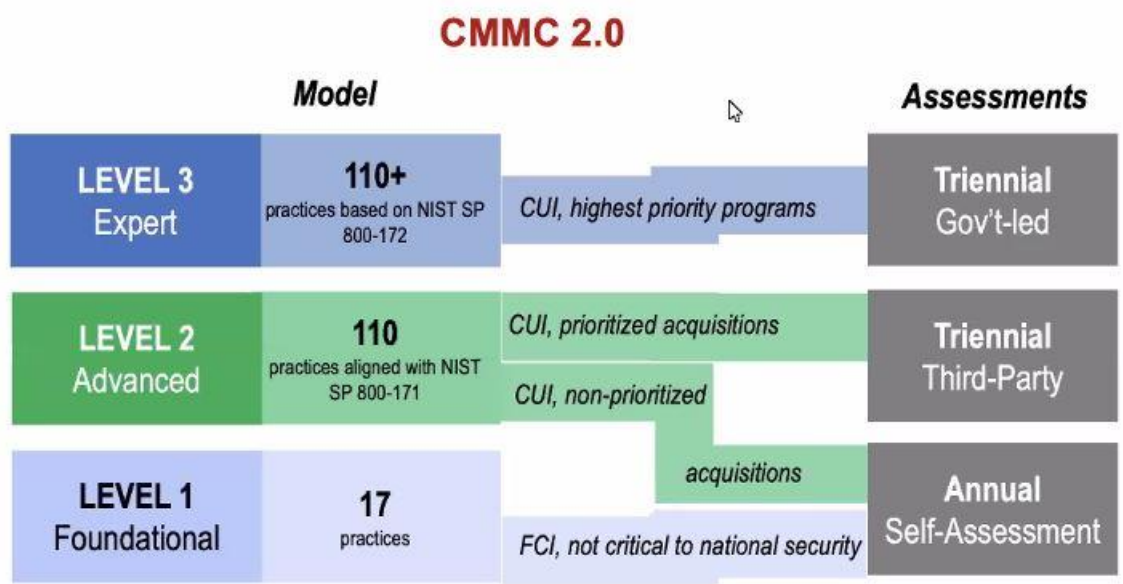
- Clarify and streamline the CMMC model and make it more accessible
- Ease the cost burden of CMMC to industry, especially to small and medium-sized businesses
- Address CMMC Ecosystem scalability
- Instill greater trust and confidence in the CMMC Ecosystem

CMMC 2.0: Primary Proposed Changes

- **CMMC Model:** Previously five (5) levels, now three (3) levels
- **Level 1:** Self-attestation by DIB companies; third-party assessments eliminated
- **Level 2:** Will be "bifurcated" as a prioritization measure
  - Higher-Priority Level 2 contracts will require certification by third-party assessment organizations (C3PAOs)
  - Lower-Priority Level 2 contracts may only require DIB self-attestation
- **Level 3:** Anticipating Level 2 C3PAO Assessment + DIBCAC NIST SP 800-172 Assessment



The Revised Model



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: Primary Proposed Changes (cont'd)

- **CMMC Model: Eliminates all CMMC-unique practices and maturity processes**
  - DoD will work with NIST to address identified gaps in the NIST SP 800-171
- **Limited use of Plans of Action & Milestone (POA&Ms) will now be allowed**
  - **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**
  - **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

The Interim Program

Since the timeline to complete the Federal rulemaking process may be anywhere from 9 to 24 months, an interim voluntary program has been authorized

- Until rulemaking formally implements CMMC 2.0, the DIB's participation in CMMC will be voluntary
- The DoD will continue to encourage the DIB sector to enhance their cybersecurity posture during the interim period
- DIB companies will be able to engage C3PAOs for CMMC Level 2 certification
- The Department is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC 2.0 Level 2 certification in the interim period

CMMC 2.0 Opportunities

In some respects, CMMC 2.0 may introduce additional opportunity for RPs and RPOs than existed in CMMC 1.0

Self-Attestation for Level 1 and Level 2

- Self-attestation will still be made through SPRS, but will require that only senior company officials (*e.g.*, CEO, CFO, etc.) make the attestation
- Company decision-makers (*i.e.*, C-suite and Boards of Directors) will be compelled to engage in CMMC
- Whistleblower notification and False Claims Act violations are potentially in play
- Assistance from RPs and RPOs is an effective risk-mitigation measure prior to self-attestation

CMMC alignment with NIST SP 800-171

- Positions CMMC as more easily adoptable by Federal civilian executive branch agencies
- Positions CMMC as more easily adoptable by international allies
- NIST 800-171 Appendix E tailoring action for "Policies and Procedures"
- *CMMC Assessment Guide* and *CMMC Assessment Process* are still expected to be controlling documents for DIB CMMC assessments

Way Forward

The CMMC Accreditation Body will be working more actively to support your successful engagement in CMMC

- Active promotional support by stressing the value of RPs and RPOs
- Developing a DIB culture of CMMC certification as a market differentiator
- CMMC 2.0 “delta training” modules for RPs *(free of charge)*
- Re-vamped and more secure RP and RPO digital credentials
- “Advanced RP” designation offerings
- More frequent RP and RPO engagement events
- New CMMC-AB website with a improved online CMMC Marketplace

In addition, we are open to your ideas in how to make CMMC a more successful pursuit for you