INSIGHTS FROM THE BDO GOVERNMENT CONTRACTING PRACTICE

NEW CMMC MODEL 2.0 IS RELEASED: Major Changes Ahead, Affecting DoD Contractors

THE TIMELINE OF CMMC EVOLUTION

In early 2020, we saw the fast incubation of the Cybersecurity Maturity Model Certification (CMMC) program, which was established by the Department of Defense (DoD) to enhance Defense Industrial Base (DIB) cybersecurity to meet evolving threats and safeguard the DoD-specific unclassified information that aids and enables our warfighters. In early 2020, CMMC Model 1.0 was released, offering a complex prescription for applying a mix of NIST 800-171 controls (already regulated by DFARS 252.204-7012), NIST 800-53 and CIS controls plus "Maturity Practices" that must be met to qualify certification. The CMMC model 1.0 was designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) shared with and handled by DoD contractors and subcontractors on non-Federal contractor information systems. This program requires a formal third-party certification process to assess a DIB contractor's compliance with the cybersecurity standards set forth in the CMMC Model.

In September of 2020, the Interim DFARS rule, DFARS Case 2019-D041, was released to implement three new clauses: DFARS 252.204-7019, 7020 and 7021. Effective November 30, 2020, the DFARS clause 252.204-7021 implemented DoD Contractor Compliance with the CMMC Level Requirement, which directed contractors to the CMMC 1.0 framework.

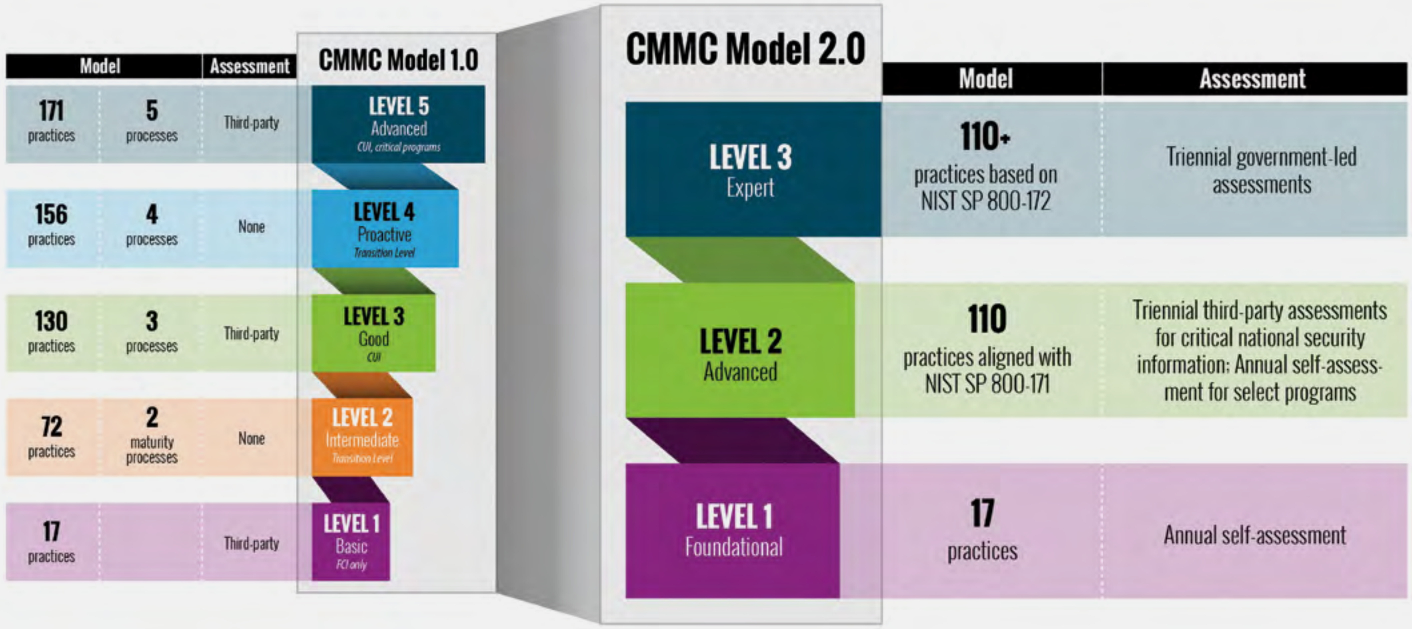
THE ORIGINAL DESIGN

The original design was five measured Maturity Levels, labeled Maturity Levels 1, 2, 3, 4 and 5. The only certifiable levels in the original program were 1, 3 and 5, leading to some confusion about what true purpose levels 2 and 4 served. In addition, CMMC didn't re-invent the wheel, but rather stuck to the original cyber framework inherited from DFARS 7012 – the 110 CUI-based NIST 800-171 controls, and added 20 controls on top of CMMC ML3 (totaling 130 controls). To reach Maturity Level 5, CMMC added NIST 800-172 (providing additional protections for Advanced Persistent Threats) on top of the NIST 800-171 controls.

TROUBLE AHEAD

Confused? So were many of the DIB contractors. Most notably, small and medium businesses (SMBs) complained that the scope was onerous, expensive and resource-intensive, and the design of the program lacked technical scoping and proper program-based definition for CUI.

KEY FEATURES OF CMMC 2.0



CMMC Model 1.0

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

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

source: www.acq.osd.mil/cmmc/model.html

DOD REVIEWS THE CMMC PROGRAM…AND SIMPLIFIES THE IMPLEMENTATION

The DoD started a comprehensive review including over 850 public comments to the CMMC program in March of 2021. The direct result of this analysis has led to a radically different approach by the DoD in the release of CMMC Model 2.0. The DoD is approaching implementation of all changes through the rulemaking process, via the following CFRs: "*1) title 32 of the Code of Federal Regulations (CFR), to establish the CMMC 2.0 program; and 2) title 48 CFR, to implement any needed changes to the CMMC program content in 48 CFR.*" (2021-24160).

The new changes proposed are as follows:

- The complete elimination of the Maturity levels 2 and 4.
- Removing CMMC-unique practices (the delta 20 controls on top of NIST 800-171).
- Removing all maturity practices from the CMMC Model (leaving only the processes).
- Allowing annual **self-assessments** with an annual affirmation by DIB company leadership for CMMC ML 1 (read – **no certification required for ML 1**).
- Splitting CMMC Level 3 requirements between two types of DIB contractors.
    - **CMMC Formal Certification:** Identify prioritized acquisitions that would require independent assessment (via CMMC C3PAO formal assessment/certification and post to eMASS; re-certify every three years).
    - **Self-Attest Only:** Identify non-prioritized acquisitions that would require annual self-assessment and annual company affirmation (post score to Supplier Performance Risk System (SPRS) every year).
- CMMC Level 5 requirements are still under development.
- Development of a time-bound and enforceable plan of action and milestone (POA&M) process (POA&M items were previously disallowed, but now are accepted for package approval, as long as the POAM items are rectified within a set timeframe).
- Development of a selective, time-bound waiver process, if needed and approved.

HOW DOES THIS AFFECT YOUR ORGANIZATION?

Note that your original requirement of NIST 800-171 as specified by DFARS 252.204-7012 does not change. In fact, the streamlining of this program to provide two paths for validating a contractor's compliance to the NIST framework is being solidified. The two paths are as follows:

1. **Via CMMC ML3 Certification with C3PAO formal certification and package upload to eMASS or**
2. **Via CMMC self-attestation and score reporting to SPRS.**

The requirement for the safeguarding of CUI within an approved environment has not changed and must be fully compliant to the security controls as prescribed in NIST 800-171.

HOW WILL YOU KNOW IF YOUR ORGANIZATION IS A PRIORITIZED ACQUISITION OR A NON-PRIORITIZED ACQUISITION?

Your organization's status is to be determined. Once CMMC 2.0 goes into effect, the DoD will specify the required CMMC level in solicitations and applicable Requests for Information (RFIs).

WILL PRIME CONTRACTORS AND SUBCONTRACTORS BE REQUIRED TO HOLD THE SAME CMMC LEVEL?

Yes and no. If contractors and subcontractors are handling the same type of FCI and CUI, then yes. In scenarios in which the prime only flows down select information, the subcontractor may abide by a lower level CMMC.

OVERVIEW OF CMMC ASSESSMENTS:

Assessment requirements are tiered by the sensitivity of information shared with the contractor. Under CMMC 2.0, "CMMC 2.0 implements tiered assessment requirements based on the sensitivity of the information shared with a contractor. Upon implementation of CMMC 2.0:"

- Contractors who do not handle information deemed critical to national security (Level 1 and a subset of Level 2) will be required to perform annual cybersecurity self-assessments.
- Contractors responsible for information critical to national security (a subset of Level 2) will be required to undergo cybersecurity assessments conducted by a third party.
- Contractors responsible for highest priority, most critical defense programs (Level 3) will be required to undergo government-led assessments.

WILL MY ORGANIZATION NEED TO BE CERTIFIED IF IT DOES NOT HANDLE CUI?

That depends. Under CMMC 2.0, if a DIB company does not process, store or transmit CUI on its unclassified network, but does process, store or handle FCI, then it must perform a CMMC Level 1 self-assessment. The company is required to submit the results into SPRS with an annual affirmation by a senior company official.

PLAN OF ACTIONS AND MILESTONES (POA&MS)

Companies can receive contract awards with a **Plan of Actions and Milestones** (POA&M) in place to complete CMMC requirements under CMMC 2.0. The Department will outline a minimum number of requirements that must be met prior to contract award to enable a remaining subset to be addressed in a POA&M within a clearly defined timeline. The Department also intends to specify a small subset of requirements that cannot be on a POA&M for organizations looking to achieve CMMC certification.

WAIVERS

The Department will allow a limited waiver process to exclude CMMC qualifications from acquisitions for select mission-critical requirements. Waiver requests will require senior DoD leadership approval and will be subject to limited duration. Specifics to come.

MORE INFORMATION TO COME…

Once in effect, the proposed overhaul of CMMC promises SMBs a clearer and more attainable path to cybersecurity compliance. While limited information has been released as of the publication of this insight, BDO anticipates that much more information is to come in the near-term.
You may reference the Office of the Under Secretary of Defense's (OUSD) proposed changes to CMMC Model 2.0 at **www.acq.osd.mil/cmmc**.

People who know Government Contracting, know BDO.

www.bdo.com/**government-contracting**

CONTACT:

CHRISTINA REYNOLDS
Industry Specialty Services Director
creynolds@bdo.com

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 70 offices and over 750 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 91,000 people working out of more than 1,650 offices across 167 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.