CMMC 2.0 OVERVIEW

The **Cybersecurity Maturity Model Certification** (CMMC) Model was created by the U.S. Department of Defense (DoD) in January 2020. The Model and entire ecosystem were designed to provide assurance to the DoD of the protected posture of the **Defense Supply Chain** and to help DoD contractors that make up the **Defense Industrial Base** (DIB) protect sensitive information from malicious cyber activity like intellectual property theft.

The CMMC will be a single standard for all DoD contracts. Compliance with the CMMC will require DoD contractors to undergo a **comprehensive cybersecurity assessment**, which adds a certification element to verify the implementation of processes and practices associated with the achievement of *one of three certification levels* commensurate with the risk to the information within their care.

Earning CMMC certification will be central to DoD suppliers and to maintaining relevant contracts

CMMC 2.0 FRAMEWORK

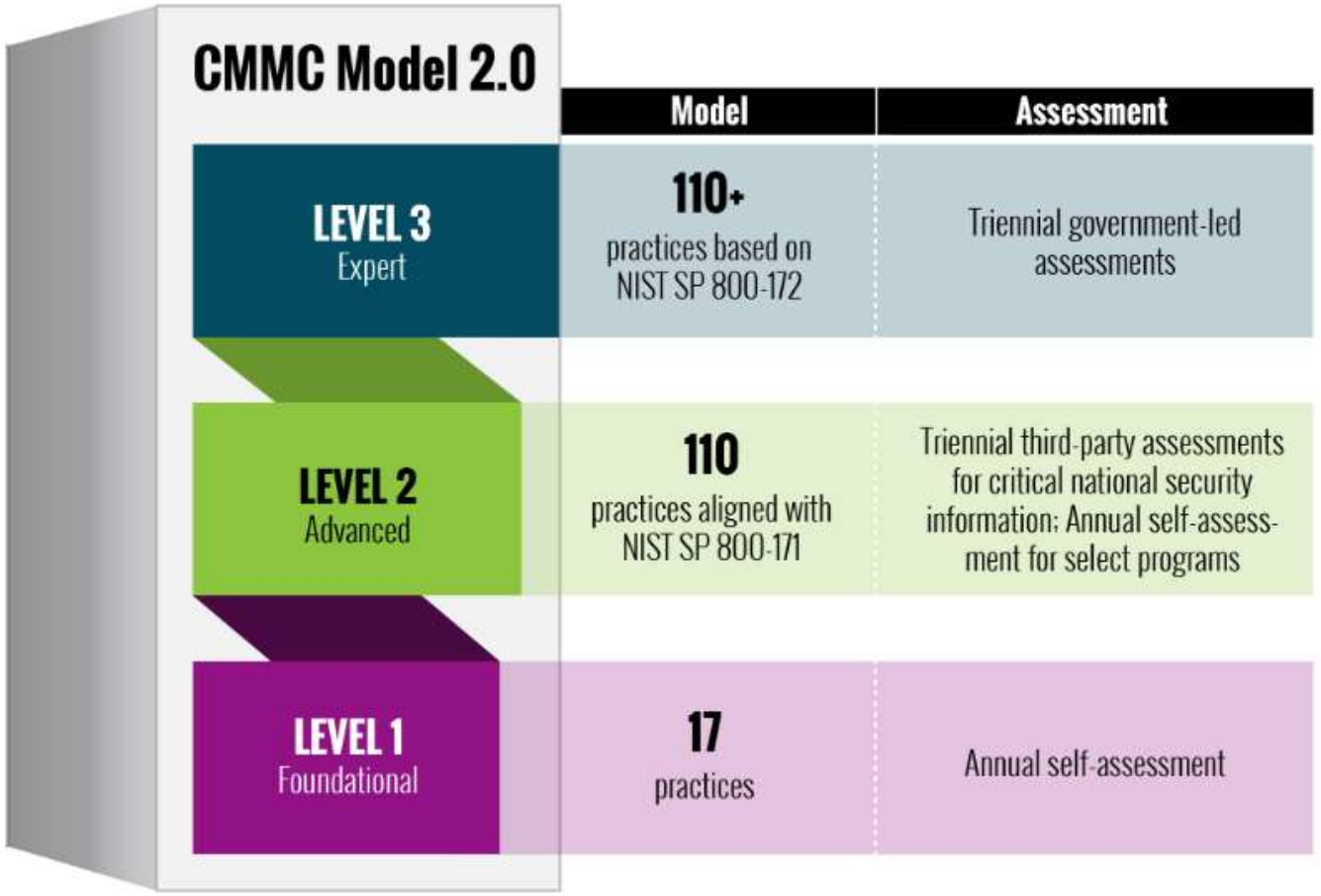
The CMMC framework consists of maturity levels **and cybersecurity best practices** organized into a set of 14 domains and mapped across 3 levels. Domains contain the progression of practices for a particular discipline. The practices are aligned to a set of capabilities within each domain to provide additional structure.

CMMC 2.0 retains three levels, directly linked to specific data types and existing regulations:

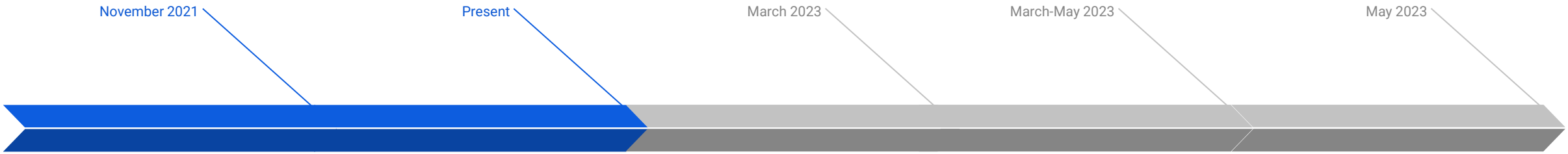
Level 1 – for companies with FCI only that must protect it per FAR 52.204-21**;** this information requires protection but is not critical to national security. **NIST SP 800-171**

Level 2 – for companies with CUI covered by the existing DFARS 252.204-7012/7019/7020 requirements. ***NIST SP 800-171***

Level 3 – for programs involving the most sensitive CUI, expected to be a very small subset of contractors. **NIST SP 800-172**



CMMC 2.0 TIMELINE



CMMC V2 Released

Initial DoD requirements

SPRS

Some NIST Requirements Starting to Appear in Solicitations

Rules Publication

Publication of Interim Final Rules

Comment Period

60 Day Comment Period for Rules

Requirements Start

Requirements Officially Appear in Contracts

Contractors must report their NIST SP 800-171 / 800-172 self-assessment scores to DoD's Supplier Performance Risk System (SPRS) to submit solicitor bids.

Contractors must pass third party CMMC assessments within the next 8 months to continue working with the DoD.