

CMMC MODEL 2.0

MODEL

ASSESSMENT

LEVEL 3: EXPERT

110+
practices aligned with
NIST SP 800-171

Triannual government-
led assessments

LEVEL 2: ADVANCED

110
practices aligned with
NIST SP 800-171

Triannual third-party assessments for critical
national security information: Annual self-
assessment for select programs

LEVEL 1: FOUNDATIONAL

17
practices

Annual self-assessment

KEY CHANGES INCORPORATED UNDER THE CMMC 2.0 FRAMEWORK

With the implementation of CMMC 2.0, the Department intends to introduce the following changes to the CMMC Model relative to CMMC 1.0:

CMMC 1.0

LEVELS

- 5 increasingly progressive levels from Basic to Advanced
- Levels 2 and 4 intended as transition stages between Levels 1, 3, and 5

REQUIREMENTS AT EACH LEVEL

- Requirements include cybersecurity standards and maturity processes at each level
- Cybersecurity standards consist of certain requirements from NIST SP 800-171 as well as CMMC-unique standards

CMMC 2.0

- 3 increasingly progressive levels:
 - Foundational / Level 1 (same as previous Level 1)
 - Advanced / Level 2 (previous Level 3)
 - Expert / Level 3 (previous Level 5)
- Eliminates all maturity processes
- Eliminates all CMMC unique security practices:
 - Advanced / Level 2 will mirror NIST SP 800-171 (110 security practices)
 - Expert / Level 3 will be based on a subset of NIST SP 800-172 requirements