SERVICE SHEET

U.S. Department of Defense Cybersecurity Maturity Model Certification 2.0

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organization – your people, your operations, and your reputation.

Although the rulemaking process for Cybersecurity Maturity Model Certification (CMMC) 2.0 is currently pending, FTI Cybersecurity can help prepare for the upcoming changes to the CMMC program and ensure the protection of Controlled Unclassified Information (CUI), while also assisting with establishing compliance and attaining certification. In 2020, in an effort to protect CUI, the U.S. government released the CMMC program, aimed at confirming that cybersecurity controls were implemented for Department of Defense (DoD) contractors. In November 2021, the DoD announced an update to the CMMC program titled CMMC 2.0.

Major Changes from CMMC 1.0 to CMMC 2.0

- Reduced from 5 maturity levels to 3. Most contractors will be assessed at Level 2, which requires compliance with the 110 controls in NIST 800-171.
- CMMC specific practices (Δ20) are eliminated.
- All maturity processes are eliminated.
- Levels 1 and non-prioritized Level 2 contractors will only require annual self-assessments.
- Plan of Action & Milestones are allowed for certification with restrictions (currently undefined).
- Cybersecurity will be an allowable cost in DoD contracts. CMMC contractors can seek reimbursement from the government for the costs of certifications.

HOW WE CAN HELP

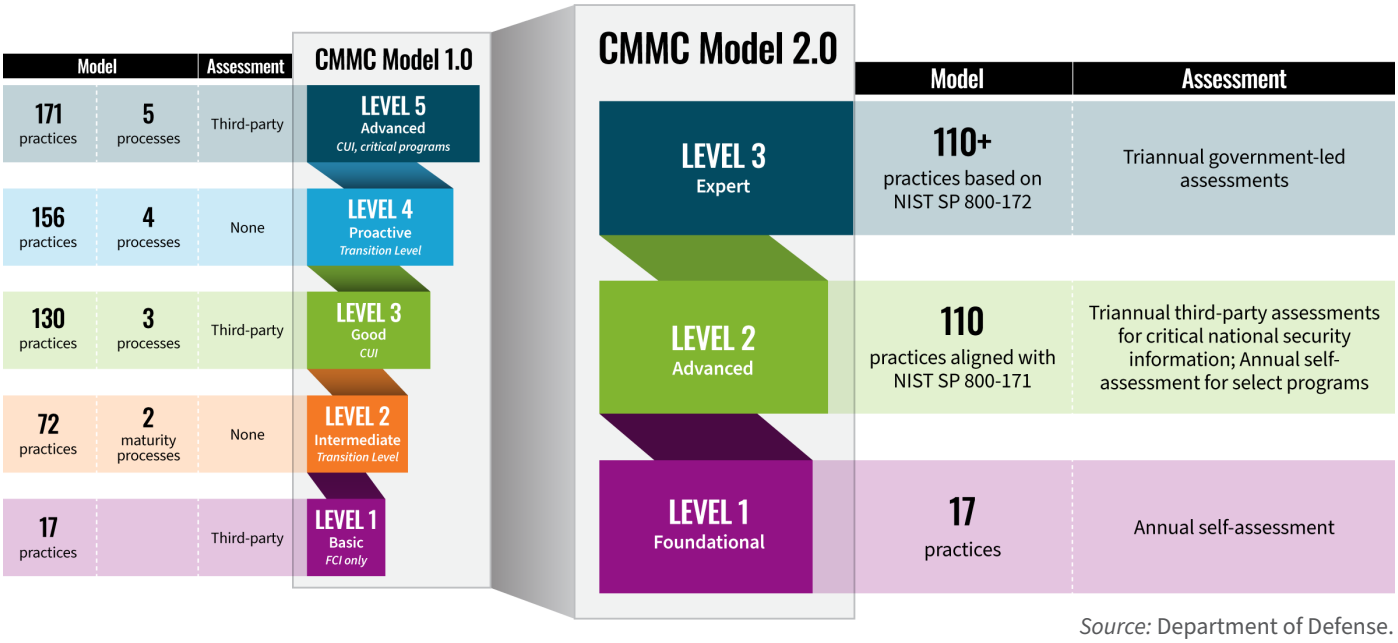
As authors of government cybersecurity policy, with extensive experience in government contracting requirements, FTI Cybersecurity helps DoD contractors implement the NIST framework and attain CMMC certification through a three-step process:

1. Pre-Certification Assessment and Gap Analysis
2. Pre-Certification Remediation, Implementation, and Transformation
3. Continuing Evaluations

FTI Cybersecurity can help navigate the complex CMMC certification process. In the competitive DoD contracting space, earning the required CMMC certification can serve as a business advantage, in addition to enhancing the cybersecurity posture of the contractor.

CMMC Levels

Contractors should begin evaluating and implementing any required changes now to ensure compliance and to maintain the ability to bid on DoD contracts. This can be accomplished by assessing current processes for how they compare to NIST 800- 171 controls and proactively closing any gaps. Depending on the CMMC level required in the specific proposal, the contractor must have a set number of NIST 800-171 security controls implemented, as well as NIST 800-172 for Level 3.



Source: Department of Defense.

CASE STUDY

Cybersecurity Compliance for a U.S. Defense Contractor

SITUATION

The Client conducts defense contracting and needed to ensure it was compliant with Defense Federal Acquisition Regulation Supplement (DFARS) and International Traffic in Arms Regulations (ITAR) within its relevant business units. We were engaged to conduct a full review of their network infrastructure to assess, plan for, and assist in the implementation of solutions to ensure DFARS and ITAR compliance.

OUR ROLE

We determined the scope of systems impacted by DFARS and ITAR compliance and conducted a gap analysis of systems to identify deficient controls. FTI Cybersecurity also developed or revised controls to ensure successful compliance, including with a focus on implementing cloud-based solutions. We conducted third party assessments of relevant vendors and offerings to meet the identified solutions and developed a roadmap for their implementation.

OUR IMPACT

We provided the Client timely feedback on the status of their cybersecurity program, as it related to compliance. We also worked closely with the Client to identify solutions to achieve compliance. The Client is now equipped to strengthen their cybersecurity posture.

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

1982

Year Founded and $5.4B equity market capitalization*

9/10

Advisor to 9 of the world's top 10 bank holding companies

7,000+

Employees

NYSE:FCN

Publicly traded

98/100

Advisor to 98 of the world's top 100 law firms

59

59 of Fortune Global 100 corporations are clients

**Number of total shares outstanding as of July 21, 2022, times the closing share price as of July 28, 2022.*

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA & APAC
Senior Managing Director
+44 7816 251410
david.dunn@fticonsulting.com

10062022 | VN02407-v02