What is the CMMC?

A Comprehensive Guide to the Cybersecurity Maturity Model Certification

UNITED TRAINING

A Brief History of DoD Cybersecurity Frameworks

Employees have always been the highest security risk for any organization and with the advent of the work from home and bring your own device models, they have become an even bigger target. Since the beginning of the COVID-19 lockdowns, cybercriminal attacks have increased dramatically.

Corporate leadership and executives have become rightly concerned about the security of their data. Not only are they concerned about their own organization's cybersecurity safeguards, but their concern also extends to the cybersecurity defenses of any partners and suppliers with whom they do business. If a partner or supplier has inadequate cybersecurity defenses in place, there is an increased danger that confidential customer and internal business data could be exposed to cybercriminals. It is that concern that led the largest employer in the world, the U.S. Department of Defense, to create the Cybersecurity Maturity Model Certification (CMMC) to ensure the protection of controlled unclassified information that contains data that is potentially critical to national security.

Why A Cybersecurity Framework Is Needed

Cybercriminals and malicious enemy state actors have always targeted cyberattacks against the Department of Defense (DoD), its supply chains, and the 300,000+ organizations that comprise the Defense Industrial Base (DIB) to gain some insight that can help them undermine our national security. The DIB is a ripe target because they help support our national defense infrastructure by providing services such as:

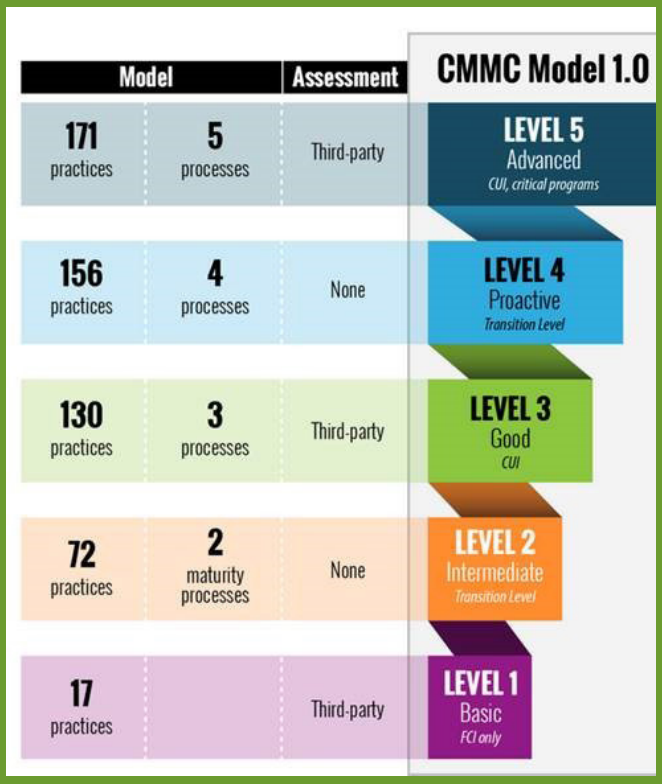
- **Research**
- **Engineering**
- **Development**
- **Acquisition**
- **Production**
- **Delivery**
- **Sustainment**
- **Operation of DoD systems, networks, installations, capabilities, and other services**

Losing our technological and logistical advantages negatively impacts our national security and our ability to deter the actions of our enemies. While there have always been strict controls for classified materials, there wasn't a framework in place to deal with federal contract information (FCI) or controlled unclassified information (CUI). CUI generated by the government and contractors, while not as sensitive as classified materials, can still give malefactors important insight that can be used to neutralize or reverse engineer our military advantages.

In 2017, a new requirement was added to the Defense Federal Acquisition Regulation Supplement (DFARS) for contractors and subcontractors that store, process, or handle CUI. It required they comply with the 110 security controls outlined in the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171). This was a step in the right direction; however, it was a flawed approach:

1. There wasn't a requirement that an organization meet all 110 controls immediately. To account for controls not met, an organization would submit a Plan of Action and Milestones (POA&M) document, but there was no requirement to produce a timeline for remediation.
2. An organization was allowed to self-assess and self-attest their NIST SP 800-171 compliance, but there was no verification audit by the DoD, nor any consequences for inaccuracies in the assessment report.

This system of security assessment and reporting became untenable, which led to the DoD to attempt correcting these issues with the creation of CMMC 1.0 in early 2020. This framework uses the processes and security implementation found in a variety of standards such as NIST, Federal Acquisition Regulation (FAR), and DFARS, and is used to determine the maturity level of an organization's cybersecurity posture. There were five levels of maturity progression, each more stringent than the previous, to meet 171 security practices (similar to NIST SP 800-171).



The CMMC 1.0 cybersecurity framework differed from the previous cybersecurity framework in three important ways:

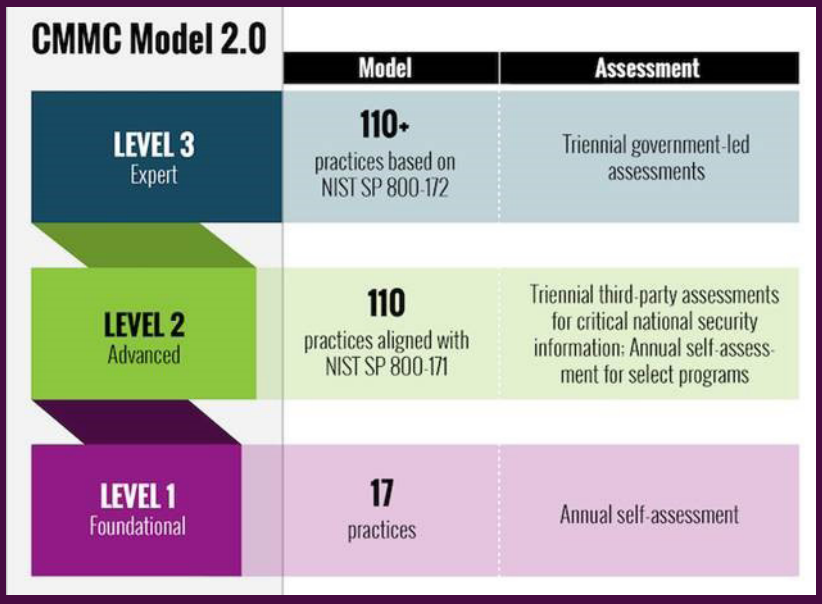
- **All 300,000+ companies that have contracts with the DoD, whether directly as a primary contractor or as a subcontractor, had to meet these standards, even if they did not possess or create CUI.**
- **Organizations were no longer allowed to self-assess and self-attest their compliance—their maturity level certification was assigned based on an independent audit by a DoD approved third-party assessor.**
- **Organizations were no longer allowed to submit a Plan of Actions and Milestones (POA&Ms)—an organization either met the requirements for a maturity level or they did not.**

While well-intentioned, CMMC 1.0 was too high a bar for small and mid-sized organizations, as well as organizations that did not handle CUI. These organizations comprise a majority of the DIB and if they could not meet CMMC 1.0 requirements they could no longer perform DoD work. The DoD realized that if there was a dramatic reduction in the size of the DIB, it would lead to a loss of innovation for the sake of no overall improvement in information security. CMMC 1.0 was tweaked twice to fix the issues (v1.1 and v1.2), but there was a realization that CMMC 1.0 needed to be reworked to simplify it while ensuring high levels of cybersecurity.

CMMC: The Next Generation

Over the course of 2021, the DoD, working with industry, simplified and streamlined the CMMC 1.0 framework and issued the **new CMMC 2.0 framework** in November 2021.

CMMC 2.0 is meant for organizations that currently, or wish to, do business with the DoD. The framework applies to primary contractors, subcontractors, and any supplier that works with them. The CMMC 2.0 framework will apply to DIB organizations' unclassified networks that process, store, or transmit FCI or CUI.



CMMC 2.0 is an outline of the best cybersecurity practices which are segmented into CMMC 2.0 controls. Previously, CMMC 1.0 had five levels of cybersecurity maturity—CMMC 2.0 reduced that number to three:

- Entry level, basic cybersecurity practices
- No documentation required
- 17 practices
- Applies to organizations that process FCI data not critical to national security
- Organization does not create, store, or receive CUI
- Annual self-assessment

- Advanced cybersecurity practices
- Documentation of practices is required
- 14 domains and 110 security controls in alignment with NIST SP 800-171 Rev. 2
- Applies to primary contractors and subcontractors that handle the same type of CUI
- Subcontractors may only need to meet a lower level if they only receive select information from the primary contractor
- Triennial third-party assessment for contractors working with prioritized acquisitions with data critical to national security
- Annual self-assessment for contractors working with CUI non-prioritized acquisitions with data not critical to national security

Level 3 Expert

- Highest level with advanced cybersecurity practices
- Extensive documentation required—organizations must establish, maintain, and resource plans to manage all activities necessary for cybersecurity practices implementation
- Overall reduction in system vulnerability to advanced persistent threats (APTs)
- 14 domains and 110 security controls in alignment with NIST SP 800-171 Rev. 2 plus an additional subset of controls in alignment with NIST SP 800-172 (the additional subset of controls will be released later)
- Triennial government-led assessments for contractors working with CUI highest priority programs with data critical to national security

The 14 domains from NIST SP 800-171 that apply to Level 2 and Level 3 certification are:

- Access Control (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (CA)
- System & Communications Protection (SC)
- System & Information Integrity (SI)

In addition to the above, contractors can create a POA&M process, but contrary to the past, this process would be set to a defined timeline along with accountability if the goals are not met. Additionally, security breaches that bring misrepresentation of self-assessment readiness to light can cause an organization to face substantial fines and/or jail time for those responsible for signing off on an organization's readiness assessment.

A Final Word

Protecting sensitive data is important for any organization, including one as large as the DoD. In the DoD's case, the information they are protecting is vital to our national security. To ensure that controlled unclassified data is secure across the vast number of organization's that work either directly or indirectly with the DoD, a generalized framework for cybersecurity needed to be constructed. Over time, an initial framework was created, was changed, and evolved to eventually become CMMC 2.0. This framework can also benefit organizations that do not do any business with the DoD, as it provides a roadmap to increase the protection of sensitive data.

Cybersecurity Certifications

If you are interested in working for an organization that does business with the DoD, the list below shows certifications that will give you the knowledge necessary to protect sensitive data and strengthen cybersecurity:

CompTIA: Security+, CASP+, CySA+

EC-Council: CSCU, CND, CTIA, CSA, ECIH, EDRP, CHFI, CCISO

ISACA: CISA, CRISC, CISM

ISC2: CISSP, CCSP

If you want to help ensure that organizations handling sensitive data with national security implications, there are certifications you can attain to become a **CMMC Professional and a CMMC Assessor.**

The Cyber AB Certified CMMC Professional (CCP)

The Cyber AB Certified CMMC Assessor (CCA)

Certification is through The Cyber AB, the official accreditation body of the CMMC Ecosystem and sole authorized non-governmental partner of the DoD in implementing and overseeing the CMMC conformance regime.

Let United Training help you start down the path of cybersecurity certification.

unitedtraining.com