



What Does The CMMC Mean For DoD Contractors?

The Cybersecurity Maturity Model Certification (CMMC) is the next step in the Department of Defense (DoD) efforts to protect U.S. defense manufacturing supply chains from cyberthreats. The CMMC in its final form will incorporate the requirements of National Institute of Standards and Technology Special Publication (NIST SP) 800-171 and will establish a new framework for defense contractors to become certified as cybersecurity compliant. The higher a company certifies, the more contracts a company can bid.

How Will Contractors Be Evaluated?

Manufacturers in DoD supply chains will be evaluated based upon the implementation of actual technical controls in addition to their documentation and policies. These evaluations will lead to a CMMC certification ranging from Level 1 "Basic Cyber Hygiene," through Level 5 "Advanced," as determined by third-party auditors. The CMMC level required in solicitations will be listed the solicitation's sections L and M and will be a "go/no-go decision."

DoD contracting authorities will still require a System Security Plan (SSP) and Plan of Action as demonstration of compliance to DFARS 252.204-7012.

How Can Contractors Prepare For CMMC?

- Establish a System Security Plan and Plan of Action. Implementation of NIST SP 800-171 cybersecurity requirements will continue to be the starting place.
- Configure existing environments or build new environments to address the NIST SP 800-171 cybersecurity requirements.
- Address items in Plans of Action.
- Flow down the DFARS cybersecurity requirements to subcontractors and suppliers.
- Increase level of cybersecurity maturity by formalizing cybersecurity practices and processes across the company.

Capabilities Assessed for Practice & Process Maturity

	Processes
Level 5	Optimized
Level	Reviewed
Level ne 3	Managed
e Level ne 2	Documented
Level ne 1	Performed
	Level 3 Level 2 Level

CMMC Model Level Descriptions

Description of Practices

Description of Processes

Highly advanced cybersecurity practices Level 5 Reserved for the most critical systems Continuous **More Stringent** Resilient against the most-advanced threat actors improvement Defensive responses performed at machine speed across the Machine performed analytics and defensive actions enterprise Resistant against, and detection of, data exfiltration Autonomous knowledge of cyber assets Level 4 Advanced and sophisticated cybersecurity practices Resilient against advanced threat actors Processes are periodically Defensive responses approach machine speed reviewed, properly Increased resistance against and detection of data exfiltration resourced, and improved Complete and continuous knowledge of cyber assets across the enterprise Coverage of all NIST SP 800-171 rev 1 controls Level 3 Additional practices beyond the scope of CUI protection Resilient against moderately skilled threat actors Processes are maintained Moderate resistance against data exfiltration and followed Moderate resilience against malicious actions Comprehensive knowledge of cyber assets Inclusive of universally accepted cyber security best practices Level 2 Resilient against unskilled threat actors Minor resistance against data exfiltration Practices are documented Minor resilience against malicious actions Less Stringent Basic cybersecurity Achievable for small companies Level 1 Subset of universally accepted common practices Practices are performed, at least in an ad-hoc matter

DoD has stated that it intends to release Version 1.0 of the CMMC framework by as early as January 2020 and will begin including these certification requirements in new DoD solicitations starting in the Fall of 2020. Like the DFARS Cybersecurity Clause, the CMMC level requirement will also flow down to all subcontractors. Future Requests for Proposals (RFPs) may require a CMMC level even if handling of Controlled Unclassified Information (CUI) is not included in the contract.

The MEP National Network

Limited resistance against data exfiltration Limited resilience against malicious actions

The MEP National Network is a unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

For More Info:

Contact North Carolina Manufacturing Extension Partnership for assistance navigating NIST SP 800-171, DFARS and CMMC. NCMEP cybersecurity experts can help with DFARS compliance and CMMC certification.





info@ncmep.org



