FLORIDA DEPARTMENT of ECONOMIC OPPORTUNITY

FloridaMakes PART OF THE MEP National Network™

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?

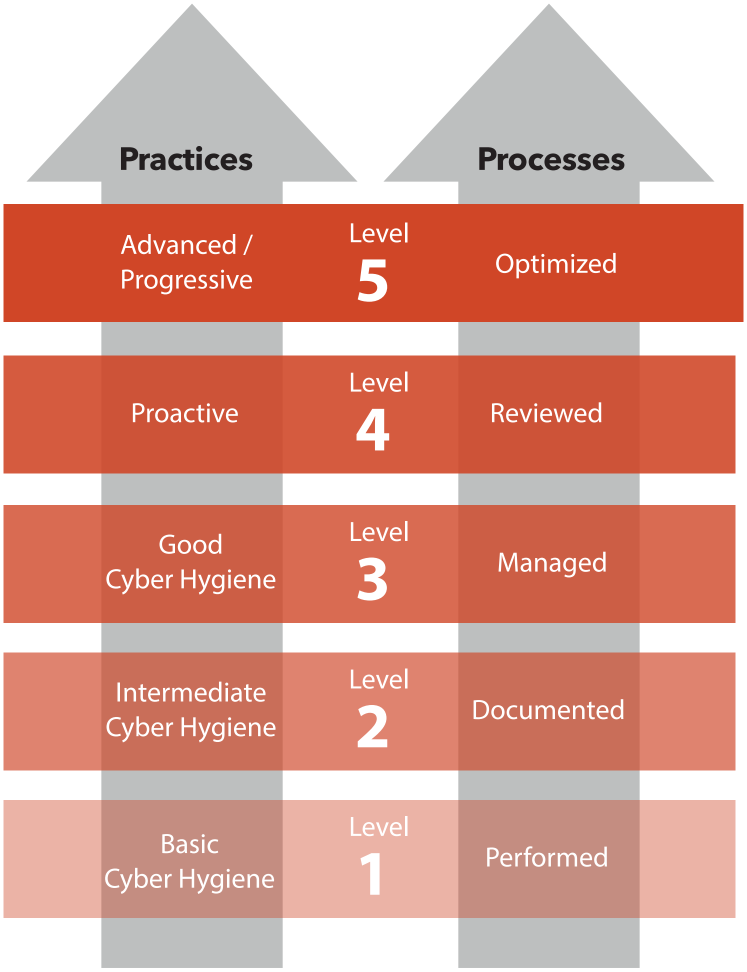
Manufacturers in DoD supply chains will be evaluated based upon the implementation of actual technical controls in addition to their documentation and policies. These evaluations will lead to a CMMC certification ranging from Level 1 "Basic Cyber Hygiene," through Level 5 "Advanced," as determined by third-party auditors. The CMMC level required in solicitations will be listed in 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?

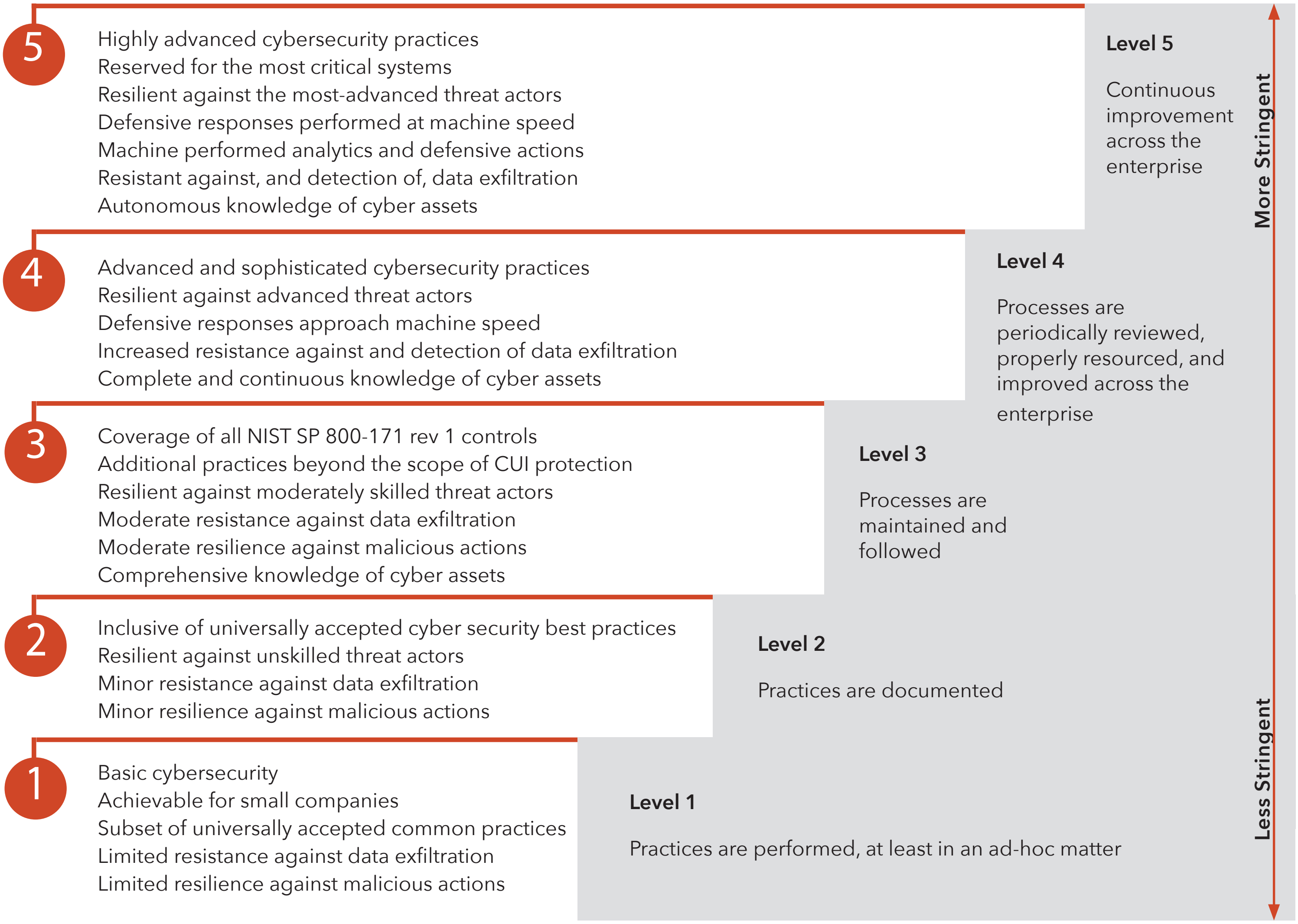
- Establish a System Security Plan and Plan of Action. Implementation of NIST SP 800-171 cybersecurity requirements will continue to be the starting place.
- Configure existing environments or build new environments to address the NIST SP 800-171 cybersecurity requirements.
- Address items in Plans of 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



Practices		Processes
Advanced / Progressive	Level 5	Optimized
Proactive	Level 4	Reviewed
Good Cyber Hygiene	Level 3	Managed
Intermediate Cyber Hygiene	Level 2	Documented
Basic Cyber Hygiene	Level 1	Performed

CMMC Model Level Descriptions



Description of Practices

Description of Processes

5

Highly advanced cybersecurity practices
Reserved for the most critical systems
Resilient against the most-advanced threat actors
Defensive responses performed at machine speed
Machine performed analytics and defensive actions
Resistant against, and detection of, data exfiltration
Autonomous knowledge of cyber assets

Level 5

Continuous improvement across the enterprise

4

Advanced and sophisticated cybersecurity practices
Resilient against advanced threat actors
Defensive responses approach machine speed
Increased resistance against and detection of data exfiltration
Complete and continuous knowledge of cyber assets

Level 4

Processes are periodically reviewed, properly resourced, and improved across the enterprise

3

Coverage of all NIST SP 800-171 rev 1 controls
Additional practices beyond the scope of CUI protection
Resilient against moderately skilled threat actors
Moderate resistance against data exfiltration
Moderate resilience against malicious actions
Comprehensive knowledge of cyber assets

Level 3

Processes are maintained and followed

2

Inclusive of universally accepted cyber security best practices
Resilient against unskilled threat actors
Minor resistance against data exfiltration
Minor resilience against malicious actions

Level 2

Practices are documented

1

Basic cybersecurity
Achievable for small companies
Subset of universally accepted common practices
Limited resistance against data exfiltration
Limited resilience against malicious actions

Level 1

Practices are performed, at least in an ad-hoc matter

DoD released Version 1.0 of the CMMC framework in January 2020 and has stated it intends to 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.

FloridaMakes Network

FloridaMakes is a statewide, industry-led, public-private partnership operated by an alliance of Florida's regional manufacturers associations with the sole mission of strengthening and advancing Florida's economy by improving the competitiveness, productivity and technological performance of its manufacturing sector, with an emphasis on small and medium-sized firms. FloridaMakes is the official representative of the MEP National Network in the State of Florida.

For More Info:

Contact your local Business Advisor for assistance navigating NIST SP 800-171, DFARS and CMMC. FloridaMakes cybersecurity experts can help with DFARS compliance and CMMC certification.

☎ 407-450-7206 ✉ info@floridamakes.com