IMEC

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 incorporates the requirements of National Institute of Standards and Technology Special Publication (NIST SP) 800-171 and establishes 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?

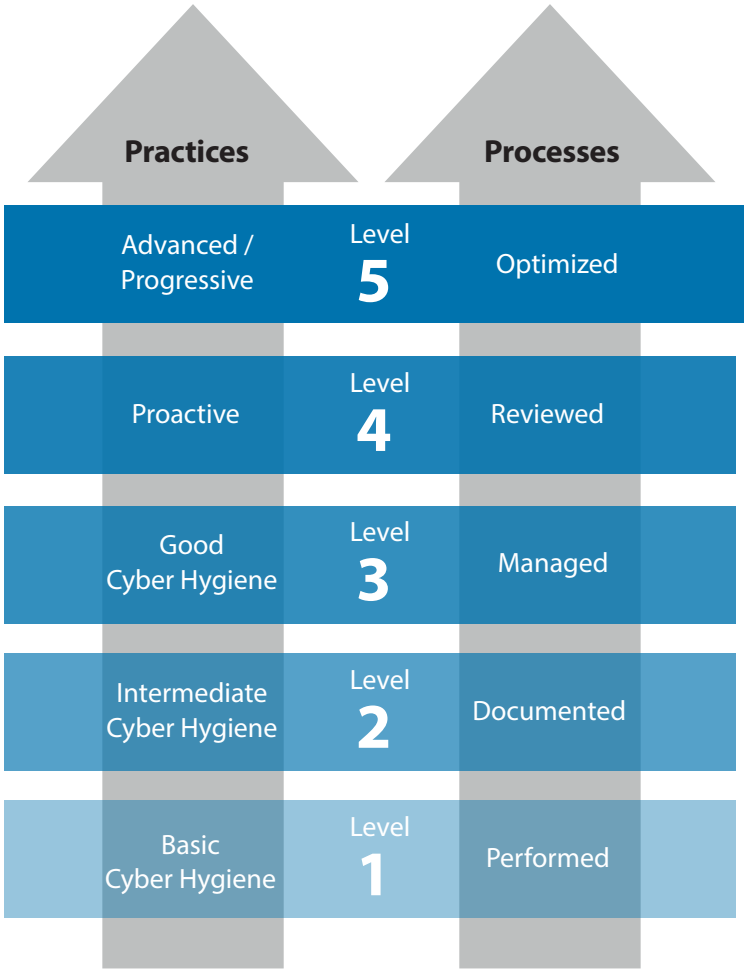
Manufacturers in DoD supply chains will be evaluated based upon the implementation of actual technical controls in addition to their documentation and policies. These evaluations will lead to a CMMC certification ranging from Level 1 "Basic Cyber Hygiene," through Level 5 "Advanced," as determined by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

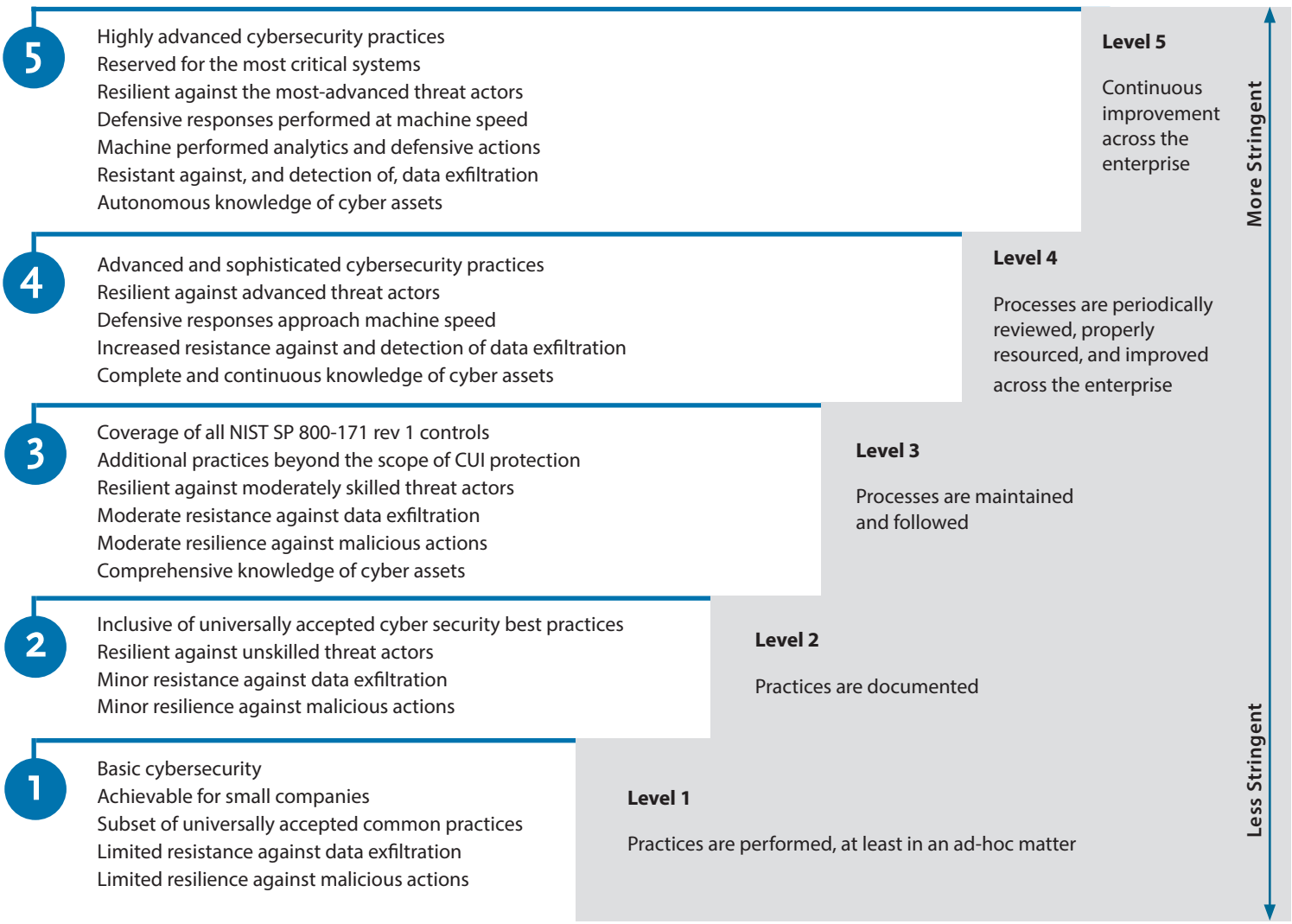
How Can Contractors Prepare For CMMC?

- 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



CMMC Model Level Descriptions



DoD has released Version 1.0 of the CMMC framework 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

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 IMEC for assistance navigating NIST SP 800-171, DFARS and CMMC. MEP cybersecurity experts can help with DFARS compliance and CMMC certification.

888.806.4632

info@imec.org

IMEC PART OF THE MEP National Network™

WWW.IMEC.ORG