VIQTORY
CYBER

www.viqtorycyber.com

Are You Ready for CMMC?

CYBERSECURITY MATURITY MODEL
CERTIFICATION

Why CMMC?

In 2015, the Department of Defense (DoD) published the Defense Federal Acquisition Regulation Supplement (DFARS) to push private contractors to maintain cybersecurity standards according to the requirements the National Institute of Standards and Technology (NIST) outlined in NIST SP 800-171.

Created to ensure the protection of Confidential Unclassified Information (CUI), the standards outlined in DFARS and NIST SP 800-171 gave DoD contractors until December 31, 2017 to meet the requirements necessary to be compliant or risk losing DoD contracts.

To be classified as compliant, contractors merely had to attest to meeting the requirements or being in the process of satisfying them.

As a result, U.S. adversaries have been able to develop military equipment based on stolen data. For instance, the Chinese J-20 and J-31 stealth fighter jets suspiciously resemble the American F-35. According to the Pentagon, China may have accessed the F-35 design after an information breach in 2009.

The Cybersecurity Maturity Model Certification (CMMC) is a new certification model designed to verify that DoD contractors have sufficient controls to safeguard sensitive data, including Federal Contract Information (FCI) and Confidential Unclassified Information (CUI) .

- **Federal Contract Information (FCI)**: FCI is information provided by or generated for the Government under contract not intended for public release.

- **Controlled Unclassified Information (CUI)**: is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

The CMMC model uses the basic safeguarding requirements for FCI as the Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI as specified in NIST 800-171 / DFARS.

CMMC Levels

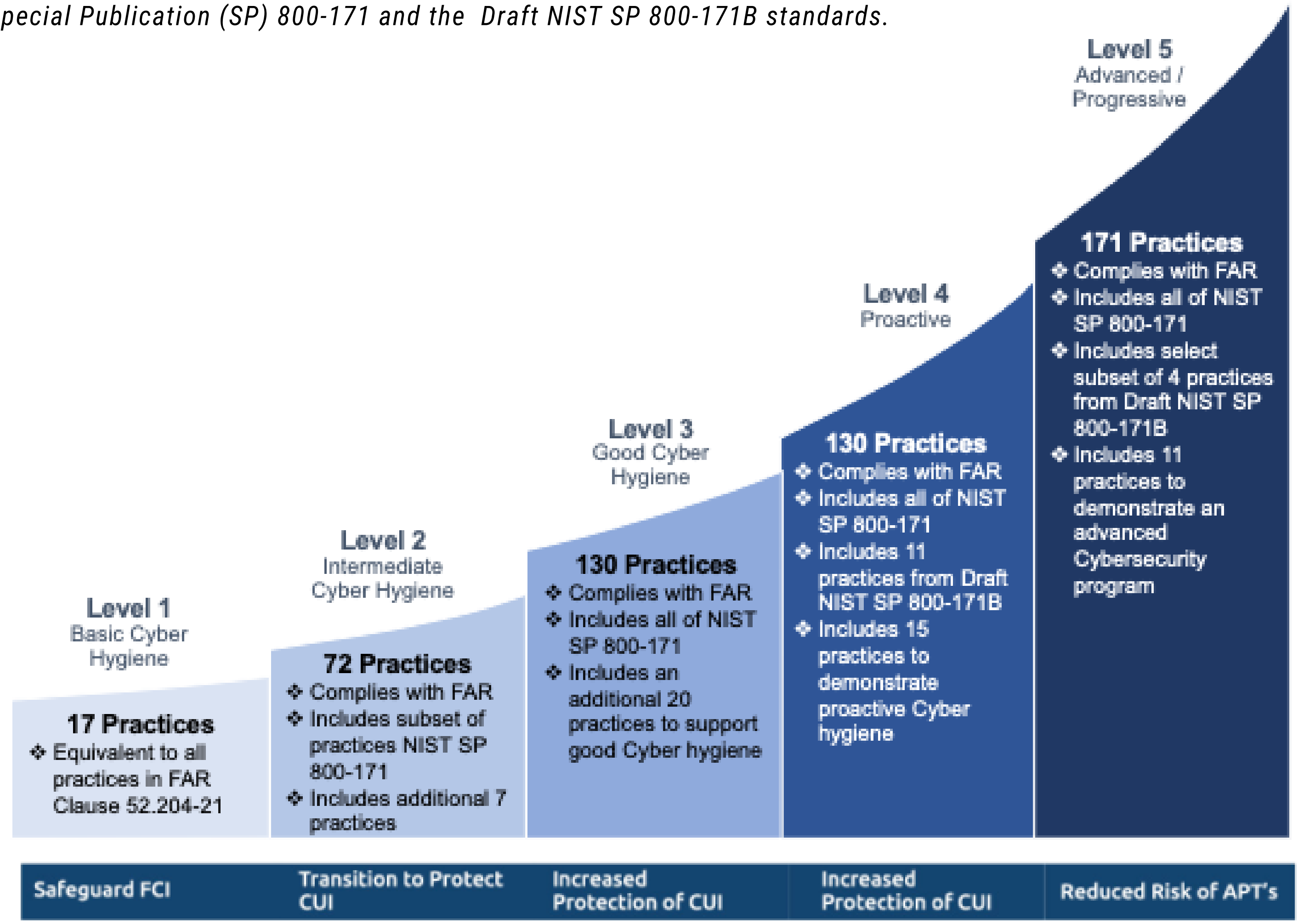
The CMMC acknowledges that not all information shares the same levels of sensitivity, and not all contact participants have the same clearance levels. Because of this, the Cybersecurity Maturity Model Certification measures processes and practices across five maturity levels.

The achievement of higher CMMC levels enhances the ability of an organization to protect CUI. For Levels 4-5, it also reduces the risk of advanced persistent threats (APTs), which are often executed via multiple incursions, including cyber, physical, and deception.

Here is a synopsis of the five CMMC levels and their respective requirements:

What level Makes Sense for Your Company?

The CMMC (Cybersecurity Maturity Model Certification) levels are a non-linear function that demonstrate increasingly more advanced "Cyber hygiene" practices based most notably on the NIST Special Publication (SP) 800-171 and the Draft NIST SP 800-171B standards.



Level 1
Basic Cyber Hygiene

17 Practices
- Equivalent to all practices in FAR Clause 52.204-21

Level 2
Intermediate Cyber Hygiene

72 Practices
- Complies with FAR
- Includes subset of practices NIST SP 800-171
- Includes additional 7 practices

Level 3
Good Cyber Hygiene

130 Practices
- Complies with FAR
- Includes all of NIST SP 800-171
- Includes an additional 20 practices to support good Cyber hygiene

Level 4
Proactive

130 Practices
- Complies with FAR
- Includes all of NIST SP 800-171
- Includes 11 practices from Draft NIST SP 800-171B
- Includes 15 practices to demonstrate proactive Cyber hygiene

Level 5
Advanced / Progressive

171 Practices
- Complies with FAR
- Includes all of NIST SP 800-171
- Includes select subset of 4 practices from Draft NIST SP 800-171B
- Includes 11 practices to demonstrate an advanced Cybersecurity program

Safeguard FCI | Transition to Protect CUI | Increased Protection of CUI | Increased Protection of CUI | Reduced Risk of APT's

Our Approach to CMMC Compliance

1
DISCOVERY

Our team conducts a series of Interviews and a network audit to determine data access and usage.

2
GAP ANALYSIS

A Gap Analysis Identifies the missing pieces necessary to achieve compliance.

3
REMEDIATION

A remediation plan Is put forth and executed with action steps towards compliance based on priority level.

4
MONITOR

Monitors systems and processes and provides the service and support to maintain compliance.

Getting you started on your journey toward CMMC compliance.

1. Determine what level of maturity your organization needs to (or would like to) achieve.
2. Review the CMMC framework to understand the practices and processes your organization would need to comply with for the level of maturity desired.
3. Interview key stakeholders and audit data usage.
4. Conduct a **GAP ANALYSIS** – work with a third party or with your team to identify technical gaps in existing vs. required practices.
5. Develop a **REMEDIATION PLAN** to implement practices that are found to be non-existent (or fixes for those determined weak) based on the results of the assessment.
6. Deploy technical solutions where needed.
7. Remediate other process gaps as identified in the preparedness assessment.
8. Identify/select a CMMC Third-Party Assessor Organization (C3PAO) firm for your CMMC audit.
9. Obtain your desired CMMC level maturity certification based on the audit.

Timeline

A landmark effort by the Department of Defense to shore up cybersecurity across its 300,000+ contractor base has managed to stay mostly on schedule despite the coronavirus pandemic.Here are some key milestones:

- DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. EFFECTIVE Nov 30, 2020.
- A DoD supplier or contractor should plan for at least a 6-month preparation and certification period.
- The first contract awards to certified suppliers or contractors are expected to take place in the first quarter of 2021.
- The CMMC certification is valid for a 3-year period.

Why Viqtory?

Jan Killmeyer

Cybersecurity Risk Management Consultant

- Since 2018, performed DFARS and NIST SP 800-171 compliance assessments and program development to ensure the confidentiality of Controlled Unclassified Information (CUI) for a number of DIB clients.
- Performed Security Maturity Assessments using the FFIEC Cybersecurity Assessment Tool (CAT), NIST Cybersecurity Framework, and ISO 27001/27002, measuring the maturity of process implementation against the Carnegie Mellon University Capabilities Maturity Model (CMM).
- Worked at the senior management level with over 20 years of experience providing IT Security and Privacy Management to the government, finance and manufacturing industries.
- Served active duty as a Colonel in the US Army where holding positions as the Inspector General, Director of Audit and Investigations, and the Chief, Enterprise Solutions in the Information Operations Division for the Defense Logistics Agency.
- Served as the Deputy Chief of Staff for Information Management, a CIO equivalent, for the Northeastern United States with the US Army Reserve Command.
- Assisted a $4B manufacturing company in performing Sarbanes Oxley IT assessments of newly acquired subsidiaries internationally to determine current state of security and provide remediation assistance and process improvement.

Paul Kriebel

Cybersecurity Risk Management Consultant

- Over 25 years risk management and Cybersecurity consulting experience.
- Nearly 10 years with Big 4 firms Deloitte & Touche and PWC, performing Cybersecurity assessments and program implementations for commercial sector companies, including financial services, life sciences & healthcare, and technology & telecommunications sectors.
- Over 10 years experience working in the federal government sector, including DoD, VA, and the White House.
- Over 10 years working in Governance, Risk, and Compliance (GRC) technologies and program development.
- Experienced Chief Information Security Officer (CISO), having established and matured a formal Cybersecurity program for a Medicare and Medicaid healthcare insurance provider.
- Developed and managed Cybersecurity audits of IT departments at a larger financial services sector.
- Developed a managed identity services business for a global financial services organization.
- Established Cybersecurity and identity management businesses.
- Speaker at several overseas conferences.

EMAIL:
info@viqtorycyber.com
CALL : 412-334-1115

Service Disabled Veteran Owned Small Business
SDVOSB
cVE

Viqtory Is a service disable veteran-owned small business