Defense Shield®
CMMC & MSSP Solutions

www.viqtorycyber/defense-shield.com

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

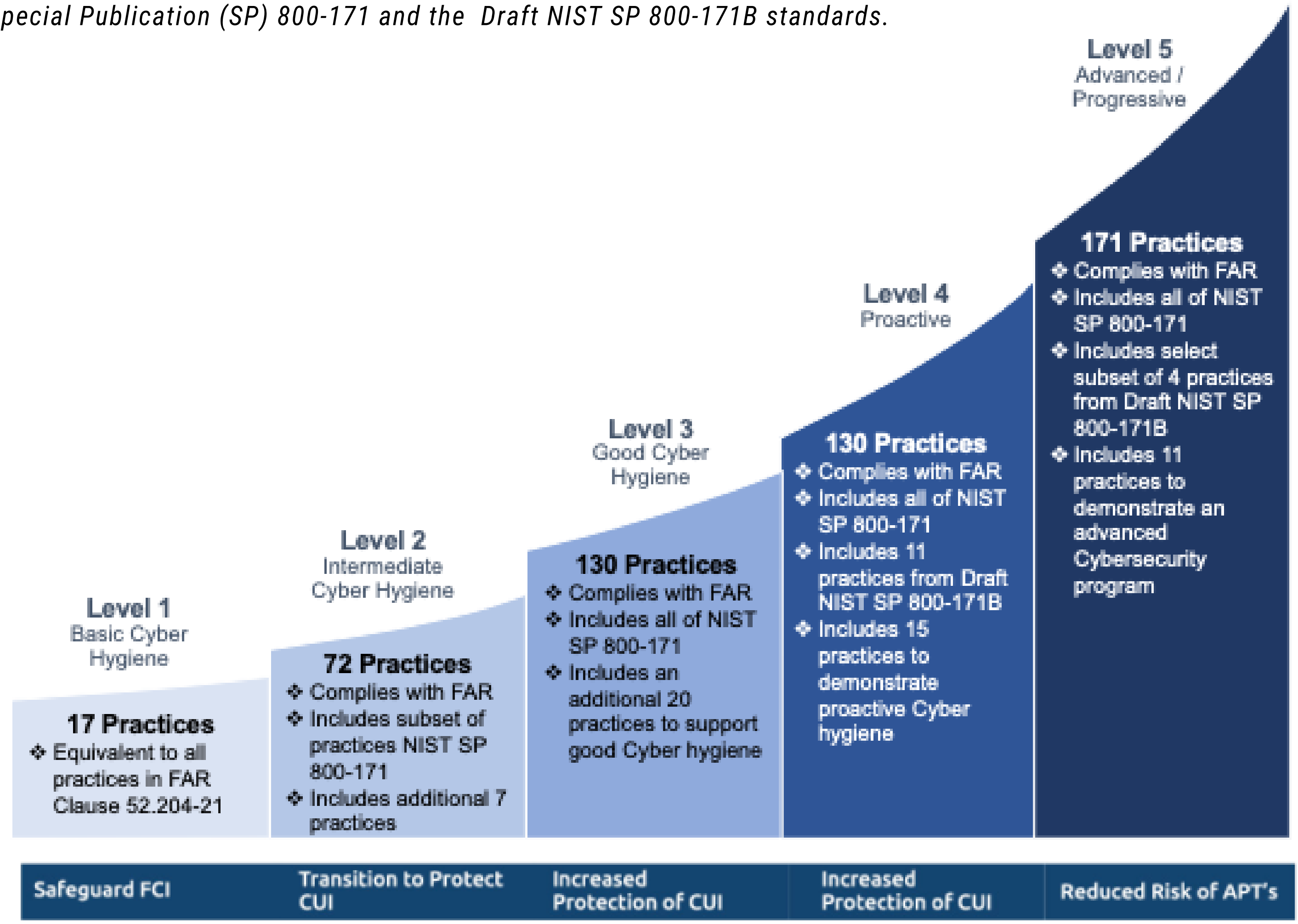
The CMMC acknowledges that not all information shares the same levels of sensitivity, and not all contact participants have the same clearance levels. Because of this, the Cybersecurity Maturity Model Certification measures processes and practices across five maturity levels.

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