PERRY JOHNSON REGISTRARS, INC.

Your Partner for Quality Certification!

A new requirement for all United States Department of Defense suppliers and contractors, Cybersecurity Maturity Model Certification (CMMC) is a crucial part of ensuring national security!

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) is the latest verification method put in place by the United States Department of Defense (DoD). This certification is the Department's first attempt to set clear requirements for contractors when it comes to cybersecurity. The goal of the CMMC is to implement an appropriate level of cybersecurity across the supply chain of the Defense Industrial Base (DIB). The DIB supply chain includes more than 300,000 companies, all of which are responsible for protecting unclassified information (CUI) under the CMMC.

CMMC will define 5 levels of cybersecurity readiness, which all US DoD contracts will invoke on the DIB supply chain. It is estimated that over 300,000 DIB contractors will be affected throughout the 3-to-5-year roll-out, with most requiring a Level 1 through Level 3 certification.

What are the different CMMC levels?

There are five levels of CMMC certification, corresponding to different cyber security processes and practices. The five levels are:

- **Level 1: Basic Cyber Hygiene** – corresponds with the 17 basic cyber security processes that must be performed to protect FCI in NIST SP 800-171 Rev 2 and 48 CFR 52.24-21.
- **Level 2: Intermediate Cyber Hygiene** – corresponds to 72 cyber security requirements including all 17 Level 1 practices. Focus is on establishing and documenting practices and policies for compliance.
- **Level 3: Good Cyber Hygiene** – corresponds to 130 cyber security processes including all Level 1 and 2 requirements. The organization must demonstrate the ability to implement 800-171 requirements and manage ongoing policies and processes.
- **Level 4: Proactive** – corresponds to 156 cyber security practices including all Level 1, 2 and 3 requirements, which must be reviewed and measured for effectiveness. Adds ability to defend CUI from APT-style attacks. Adds controls from NIST SP 800-171B.
- **Level 5: Advanced/Progressive** – corresponds to 171 cyber security processes, including all Level 1, 2, 3 and 4 requirements. Focus is on the protection of CUI from APTs and the increased depth and sophistication of cyber security capabilities.

PJR ADVANTAGES

As a leader in the certification industry, PJR is focused on our clients' satisfaction and success! Our experienced auditors and dedicated schedulers give each client the individual one-on-one attention they deserve with detailed audit plans, flexible scheduling, and value-added auditing.

*Request a **FREE** quote today and see what a difference PJR can make!*

CALL (248) 358-3388 or EMAIL PJR@PJR.com

Revised: n/a | Rev. 1.0 | Issued: 5/21/2021 | Effective: 5/21/2021