CYBER LANTERN

FAQ: WHAT YOU NEED TO KNOW ABOUT THE CMMC

There are currently over 1,000 open investigations by the FBI into intellectual property theft of US Technology by the Chinese. These investigations are often tied to the theft of intellectual property that is acquired from Defense Industrial Base (DIB), otherwise known as government contractors. To ensure the security of sensitive unclassified DoD information (CUI), the Department of Defense (DoD) has created the CMMC framework to ensure this data is safeguarded. We have compiled a list of frequently asked questions to help you become familiar with the CMMC and understand how to prepare for the certification.

What is the CMMC?

The CMMC is a comprehensive framework to enhance the cybersecurity of the U.S. DIB to address cybersecurity standards, regulations, metrics, ratings, and third-party certifications that prime contractors/ subcontractors must meet to successfully implement the current DFARS Clause 252.204-7012. This means the CMMC is essentially the guide and accreditation framework that safeguards DIB information systems.

Who needs this certification and how do I determine my required cert level?

Anyone who does business with the Department of Defense. This include companies who are NOT working in the cybersecurity/ information assurance fields. According to the CMMC Accreditation Board (CMMC AB), all DoD Suppliers will need to be CMMC Certified by 2025. DoD is to start incorporating the level of CMMC requirements within their initial Request for Information (RFIs) and follow-on Request for Proposals (RFPs) to give contractors a sense of what level of certification they should be at for submitting a proposal. Subcontractors may be allowed to certify at a lower level to their Primes, depending on the nature and intent of their work.

Can I certify myself?

You cannot certify yourself and this is the biggest difference between CMMC and the current DFARS and NIST requirements. You will need to request an assessment from a certified CMMC AB 3rd party accreditor. These assessors are currently undergoing training, as of August 2020. You can find more information on the CMMC AB here: https://www.cmmcab.org/c3pao-lp.

How is it different from NIST-800-171?

The NIST 800-171 compares to L3 compliance for CMMC. Since the CMMC framework was based on the NIST controls, matching your controls to NIST is a good way to begin preparing for the CMMC.

FAQ: WHAT YOU NEED TO KNOW ABOUT THE CMMC

Is it expensive, and can I be reimbursed?

Cost will depend on the following factors: Level of certification and level of NIST 800-171 maturity. The DoD has declared that certification costs are an ‘allowable expense’ under cost-reimbursement contracts, however it will depend on how the contract is structured and what contracting type is utilized. This may only cover the actual assessment, and not the ‘soft-costs’ associated with getting prepared for the audit. Some states such as Maryland are also providing financial support to pay for half of the process or up to $12k through DCAP.

How do I prepare for the certification process?

The CMMC AB suggests starting the certification process 6 months out or MORE; starting now could get your company certified within 6-18 months. To prepare, you can begin by getting a full assessment for your company. Next you will need to mitigate any issues identified in the assessment and obtain a separate compliance auditor to review the outcomes based on NIST 171 controls, on which the CMMC framework is based. Certifications are valid for **3 years**.

How can Cyber Lantern help you with CMMC?

Virtual CISO Services

Cyber Lantern can help you get certified by providing strategic guidance on how to apply the framework through our Virtual CISO services. Our team, is already in the process of preparing for our own CMMC accreditation through our DIB branch at Digital Lantern Federal. We can assist by identifying the proper controls and measures needed for your organization to reach the necessary level of CMMC accreditation and providing planning and implementation support so you can continue business as usual.

Detection and Response (XDR) Services

Cyber Lantern provides continuous detection and monitoring covering all areas of CMMC framework certification all for less than the cost of the assessment, mitigation, and audit:

- ✓ Asset Management
- ✓ Audit and Accountability
- ✓ Identification and Authentication
- ✓ Risk Management &Situational Awareness
- ✓ Incident Response Support
- ✓ System monitoring and protection