US Department of Defense

Cybersecurity Maturity Model Certification (CMMC)

Moving Toward Certification Success

Introduction

To reduce the risk of cyberattacks on the United States' confidential and vital information, the US Department of Defense (DoD) has developed a certification program. It is aimed at assessing and enhancing the cybersecurity posture of the Defense Industrial Base (DIB), particularly as it relates to Controlled Unclassified Information (CUI) within the supply chain. With ongoing supply chain vulnerabilities and attacks, it is clear to see that self-reported security assessments are no longer adequate.

Sue Gordon, a former deputy director of national intelligence

"Criminal hacking, by crooks and nation states, is "a global commodity now, everyone can cause harm. Formerly just the province of great powers, now it is available to anyone. In a digitally connected world, one need not travel great physical distance or expend great resources to achieve malign outcome."

How to Prepare for a CMMC Certification

Before undertaking a formal CMMC certification assessment, organizations can ensure that the process is completed quickly and successfully by performing the following steps in advance. The ultimate objective of CMMC Certification is to further the security maturity of the United States Defense Industrial Base (DIB) sector and to validate the protection of Controlled Unclassified Information (CUI). Obtaining or maintaining government contracts prioritizes for those organizations that have and maintain CMMC certification. Taking these recommended steps is not just a one-time exercise, but should be incorporated with every major change to your organization's infrastructure or any digital alterations to your business.

TECH LOCK®
A RevSpring Company

320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083
info@techlockinc.com
847.245.3727

How to Prepare for a CMMC Certification

Step 1:
Document all System Security Plan Policies, Procedures, and Actions

Organizations need to fully document their current System Security Plans (SSPs). NIST 800-171 requirement 3.12.4 states that the contractor must develop, document, periodically update, and implement system security plans for organizational information systems. These plans must describe the security requirements in place or planned for the systems. Section 3.12.2 of NIST 800-171 also requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate any vulnerabilities in their systems. A documentation review before engaging with a C3PAO certification will uncover issues and will ultimately save money. Having clear documentation, the less your staff will have to fill in the blanks with auditor questions.

Perform a thorough review of your System Security Plan (SSP) to understand the who/what/when/where/how/why of your CUI environment.

Assess your Plan of Action & Milestones (POA&M) to understand what controls are not addressed (if applicable) and how your compensating controls can remediate the risk of non-compliance for a certain control aspect.

Evaluate your policies, standards, and procedures to see if those line up with the SSP and if that documentation supports all the requirements of NIST 800-171/CMMC.

Step 2:
Review Operations and Security Controls against Compliance Guidance

In preparing for CMCC certification, a review of security operations and controls to ensure they are aligned to the guidance and your documentation is recommended. Organizations should ensure that they can:

Identify, remediate, and report all cybersecurity incidents within the required 72-hour reporting period.

Have a formal procedure in place to ensure that all subcontractors and suppliers meet the organization's compliance requirements.

Have a structure in place to update plans as the business and IT infrastructure evolve over time.

Map the ways the organization achieves the appropriate level of security controls:

- CMMC Level 1: 17 Controls
- CMMC Level 2: 72 Controls (includes Level 1 controls)
- CMMC Level 3: 130 Controls (includes Level 2 controls)
- CMMC Level 4: 156 Controls (includes Level 3 controls)
- CMMC Level 5: 171 Controls (includes Level 4 controls)

320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083 info@techlockinc.com 847.245.3727

Step 3:
Plan for a Security Assessment and Gap Analysis

Perform a thorough assessment of the organization's current operations and identify any gaps in coverage or documentation. The initial assessment should cover all 14 families and 110 security requirements of the NIST regulations. The assessment can be performed in-house by the company's own security operations team. But, with the CMMC eliminating the option of self-certification, building a relationship with a third-party service provider is now recommended. Individuals have been going through the CMMC training processes. There are assessors that have established their CMMC-PA provisional status as organizations are in queue to be C3PAO Certified to provide the third-party CMMC Assessments for DoD contractors.

Obtain More Value from a CMMC Assessment

Performing all these steps before the certification process is started will ensure that the formal CMCC process is quick, efficient, comprehensive, and successful.

The CMMC experts at TECH LOCK have an extensive understanding of cybersecurity, NIST SP 800-171/172 and NIST 800-53, ISO 27001/27002. THE TECH LOCK team also has the ability to provide PCI-QSA, PCI-ASV, and HITRUST Certifications. Our unique security focused experience delivers streamlined services that not only go beyond just compliance assessments, but help to achieve cyber resiliency and data security that fulfill multiple standards and compliance guidlines.

TECH LOCK provides organizations with a personalized path to success from beginning to end. Pre-certification assessments, to managing and implementing security controls, and providing compliance maintenance we help DoD contractors easily achieve their desired CMMC maturity level quickly.

About TECH LOCK Inc.
TECH LOCK enables organizations to navigate, detect, and respond to today's modern cybersecurity and compliance challenges. Our full spectrum security-centric approach delivers value to our clients through defined and measurable outcomes combined with independent cyber research, specialized skills, and premium customer support and service.

320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083 info@techlockinc.com 847.245.3727