AITHERAS

5 FACTS TO KNOW to prepare for CMMC CERTIFICATION

The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing cybersecurity across DoD contractors. It is a new framework for ensuring that companies in the defense industrial base (DIB) supply chain are protecting sensitive defense information.

1

THE CHANGE IT BRINGS

DoD contractors must now need to undergo external security audits by certified independent 3rd party organizations to inform risk. Contractors will remain responsible for implementing cybersecurity requirements. What kinds of things are examined in a security audit?

- VERIFY SECURITY STRATEGY
- HARDWARE/ SOFTWARE FLAWS
- SECURITY TRAINING EFFECTIVENESS
- NEW TECHNOLOGY VULNERABILITIES

Information SECURE

2

THE 5 CMMC LEVELS AND FRAMEWORK

5. Advanced Progressive

The CMMC defines 30 extra security controls – over level four – These largely relate to the ability of organizations to respond to changing threat landscapes through auditing and managerial processes, over extra technical requirements.

4. Proactive

These audit processes involve looking at historical data on the threats you have been exposed to, and how your organization proactively responded to them.

3. Good Cyber Hygiene

This level is based on an extension of the NIST 800-171 r2 standards. To be fully compliant with this level, organizations must have in place 47 security controls. In order for your organization to be accredited, you will need to document the security procedures you already have in place.

2. Intermediate Cyber Hygiene

This level introduces a new type of data called Controlled Unclassified Information (CUI). CUI is defined by the DoD as "any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls," but does not include certain classified information.

1. Basic Cyber Hygiene

The first level is for organizations to put in place "basic cyber hygiene" practices. These include using antivirus software and providing staff training to ensure that passwords and other authentication details are secure.

3

HOW TO PREPARE

There is no self-certification in CMMC. Your organization will coordinate directly with an accredited and independent third-party commercial certification organization to request and schedule a CMMC assessment.

The 17 TECHNICAL REQUIREMENTS

Access Control
Asset Management
Audit and Accountability
Awareness and Training
Configuration Management
Identification and Authentication
Incident Response
Maintenance
Media Protection
Personnel Security
Physical Security
Recovery
Risk Management
Security Assessment
Situational Awareness
Systems and Communications Protection
System and Information Integrity

4

DOCUMENT YOUR PRACTICES

A critical part of proving your cybersecurity maturity is to be able to present the DoD with exhaustive, detailed plans of the cybersecurity tools, processes, and systems you already have in place. Early preparation of this type could result in a more efficient assessment with positive end results.

START NOW AND GET HELP

5

ENGAGE WITH THE DOD

Though the requirements of the CMMC are likely to be a burden – at least initially – for many organizations, it's also worth recognizing that the DoD knows this. The advantage of the "maturity" model contained in the CMMC is that it allows firms to work toward maturity levels in consultation with the DoD, and starting this relationship early is crucial.

FEEDBACK is key with DOD

source: https://www.varonis.com/blog/cmmc-compliance/

www. aitheras.com
inquiry@aitheras.com