Cyber**Security**

VESTIGE
Digital Investigations

CMMC Preparation

How DoD Contractors Can Prepare For CMMC

As part of DoD contracts, Primes and Subcontractors are subject to the flowdown rules contained in the Federal Acquisition Regulation (FAR) as well as the Defense Federal Acquisition Regulation Supplement (DFARS). In an effort to continue to improve cybersecurity and prevent the loss of intellectual property and other sensitive information, this government-led effort is being implemented to protect the U.S. Defense Supply Chain (DSC) from foreign and domestic cybersecurity threats, and reduce the overall security risk of the sector.

Since the adoption of DFARS 252.204-7012 in 2016, over 300,000 US DoD Contractors have been scrambling to understand and implement NIST SP 800-171 standards within their companies in order to be compliant with the regulation. Some have had the internal resources to become compliant themselves, while others have outsourced the task to professionals, such as Vestige, who help DoD suppliers comply with their cybersecurity mandates – and yet, others have ignored or failed to implement such requirements.

Due to this slow adoption rate of the DFARS 252.204-7012 regulation, the Department of Defense has released the **Cybersecurity Maturity Model Certification (CMMC)**. CMMC is designed to ensure appropriate levels of cybersecurity controls and the processes are adequate and in-place to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). CMMC 2.0 outlines three compliance maturity levels that range from Basic Cybersecurity Hygiene (Maturity Level 1) to Advanced Cybersecurity Practices (Maturity Level 3). When implemented, adherence to the CMMC will reduce the risk of hostile agents breaching a supplier's cybersecurity defenses.

Unlike in the past (NIST 800-171) where a supplier was able to "self-assess" conformance with the standard, CMMC 2.0 requires that to be awarded prioritized contracts at Level 2 and all contracts at Level 3, the organization needs to undergo a thorough, evidence-based, external audit performed by a Certified Third Party Assessor Organization (C3PAO), (Level 2), or from DIBCAC (Level 3).

For those organizations that can self-assess, a senior officer of the company will need to attest that the controls are in place and working as designed.

Compliance is required in order to be awarded a DoD contract. Depending on a supplier's requirements and current state, the CMMC Accreditation Body (CMMC-AB) has advised that obtaining certification to the CMMC program will likely take a minimum of 6 months. Vestige's experience with similar frameworks (and our deep knowledge on both NIST 800-171 and CMMC) would indicate that organizations may need a minimum of 12 months.

Is Your Program Ready?

If you currently have a lucrative DoD Contract that you want to maintain, passing the new CMMC is crucial. If you aren't 100% certain you'll pass — Vestige has a solution that is a perfect fit for you!

Why Vestige?

- Vestige is a **CMMC Registered Provider Organization (RPO)**
- Vestige employs **CMMC Registered Practitioners (RP)**
- **20 years** of Information Security/Cybersecurity experience
- **Expertise in NIST 800-171**, the predecessor to the CMMC
- **Focus on small and mid-size enterprises** / organizations
- **A proven formula** from going from assessment to secure

THE CYBER AB
CMMC CERTIFICATION
REGISTERED PRACTITIONER ORGANIZATION
RPO

OVER

Here Is Our 4-Phase CMMC Process:

1. Pre-CMMC Cybersecurity Assessment

We assess your network to see if it matches up with the upcoming guidelines. We'll come in, just as if we were running the certification audit, and look at both Design and Execution.

With the results from this, we'll provide a complete Gap Analysis Roadmap showing where your organization currently stands in regard to passing CMMC, current maturity level, and the path forward to obtaining the desired/required maturity level.

2. Remediation

In Phase 2, we take the roadmap from Phase 1 and help you implement those controls. We can be as involved or not as involved during this phase, based on your preference for assistance for remediating the gaps. With our expert advice, we help your IT put the controls in place with all the supporting requirements for turnkey execution, so there will be no issues when a third party assessor is certifying you.

3. Coordination, Guidance & Advocacy during the formal CMMC Assessment

Vestige will work with you during the actual CMMC Assessment itself to make the process as smooth as possible. We act as an advocate, negotiator and liaison between your organization and your Certified 3rd Party Auditing Organization (C3PAO) – helping deliver success for your CMMC.

4. On-Going Compliance Services

In Review, Our Services Include:

- **Pre-CMMC Cybersecurity Assessment** – Vestige will critically assess your organization's environment as if we are the C3PAO assessing your environment for certification. In this manner you obtain a realistic understanding of your ability to pass the certification assessment and obtain a roadmap of changes that need to be implemented to pass.
- **Remediation** – We provide a roadmap, policies and turnkey implementation for you and your IT to ensure there will be no issues when it's time for the third party assessor certifying your organization.
- **Expert Guidance** – Our RPs offer expert guidance throughout the actual 3rd party CMMC Assessment to assure the process is smooth and pain-free for your organization.
- **On-Going Compliance Services** - to maintain your Cybersecurity Maturity Model Certification.

Take Proactive Steps Today

Contact Vestige today so that you are prepared for this update and can smoothly transition to this latest effort by the DoD to enhance the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Vestige Digital Investigations

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com