**Cybersecurity Maturity Model Certification (CMMC)**

**Introduction**

The Cybersecurity Maturity Model Certification (CMMC) is a new certification standard introduced by the Department of Defense (DoD) to ensure security of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB). Starting 1 OCT 25, certification is mandatory for all DIB contractors and is a key component of DoD's push to protect sensitive information from cyber threats.

**Background**

The CMMC was established in response to rapidly accelerating cyber-attacks across the DIB. To address these new threat vectors and protect sensitive Government information, DoD implemented various regulations and guidelines, including the National Institute of Standards and Technology (NIST) Special Publication 800-171. The CMMC certification operationalizes concepts of the National Cyber Strategy and DIB Cybersecurity Strategy, by providing a standardized framework for assessing and certifying cyber hygiene levels and the cybersecurity maturity of the industrial base.

**Key Points**

1. **Mandatory Certification**: For all DoD contractual instruments > the $10k micro-purchase threshold, (Awards, Orders, Calls, Agreements, Government Purchase Card transactions), CMMC certification is mandatory with the exception of Commercial Off the Shelf (COTS) purchases.
2. **FCI/CUI Protection**: CMMC is designed to protect FCI and CUI, which includes sensitive information related to government contracts, national security, defense, infrastructure, and other critical areas. The DoD CUI Registry includes 112 categories of CUI across 17 index groups.
3. **NIST Scores**: Contractors must achieve a minimum NIST score to be eligible for contract awards, as required by DFARS 252.204-7012.
4. **Implementation Timeline**: CMMC will follow a phased implementation.

FY26 = Level 1 only, irrespective of whether the acquisition includes CUI.

FY27 = Levels 1 (acquisition has FCI only) & Level 2 (acquisition has FCI and CUI). FY28 = Levels 1 (FCI only), 2 and 3 (CUI is present); CMMC fully implemented. Beginning 1 OCT 25, applicable awards require Level 1. No cert = No award.

1. **Certification Levels**: The CMMC certification has three levels. Level 1s is considered the Basic level of cyber hygiene. It is designed to protect FCI, and only requires DIB self-certification. Level 2 is the Intermediate level of cyber hygiene, designed to protect FCI and CUI, with two versions depending on CUI category. Level 2s only requires DIB self-certification. Level 2c requires DIB self-certification with verification by a Certified Third-Party Assessor Organization (C3PAO). Level 3c is the Advanced level of cyber hygiene. It is designed for FCI and the most sensitive types of CUI. Certification requires Level 2c as a pre-requisite, followed by verification by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

**Key Benefits**

1. **Enhanced Security**: The CMMC certification will enhance the security of CUI and protect against cyber threats.
2. **Competitive Advantage**: Contractors who achieve CMMC certification will have a competitive advantage in the market.
3. **Compliance**: The CMMC certification will ensure compliance with DoD regulations and guidelines, reducing the risk of non-compliance.

**USACE Implementation**

In coordination with CIO/G6 and Engineering & Construction (E&C), the Directorate of Contracting (DoC) is on point to lead a cross-functional CMMC Tiger Team charged with full implementation of CMMC and the underlying CUI. The primary forcing function will be issuance of a HQ OPORD directing activities of subordinate units. In addition, DoC will host rolling webinars, industry engagements, brown bags, as well as recurring Special Notice postings on SAM.gov, the primary Government Point of Entry (GPE) for the DIB.

**Conclusion**

The CMMC certification is a critical component of the DoD's efforts to protect CUI and ensure the security of the defense industrial base. Government must identify, mark, safeguard and communicate CUI requirements to the DIB. In turn, DIB contractors must safeguard CUI by prioritizing CMMC compliance and achieving the required CMMC Levels to be eligible for contract awards. Successful CMMC implementation ensures protection of sensitive DoD information, enhances the security posture of USACE and the DIB, provides compliant companies with a competitive advantage, and ensures the DoD ecosystem at large mitigates cyber risk by maintaining necessary cyber hygiene and protections.