

Cybersecurity Maturity Model Certification (CMMC)

Cotton & Company LLP

- Veteran-owned
- Alexandria, VA
- Certified Public Accounting firm
- 16 partners
- Founded in 1981
- 180 employees

Cotton & Company LLP is a veteran-owned Certified Public Accounting (CPA) firm based in Alexandria, Virginia. We have 16 partners and more than 180

employees providing a full range of audit, cybersecurity, financial management and accounting, internal control and risk management, information system, and litigation support services, primarily to governmental agencies and programs.

In particular, Cotton & Company has the necessary expertise to assist the U.S. Defense Industrial Base (DIB) sector in enhancing its cybersecurity posture within the multi-tier supply chain to ensure compliance with Cybersecurity Maturity Model Certification (CMMC) requirements. Our services include:

CMMC MISSION STATEMENT

The intent is to incorporate CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a requirement for contract award.

The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.

Source: <https://www.acq.osd.mil/cmmc>



CMMC ADVISORY SUPPORT

Cotton & Company is ready to provide DIB-sector partners and contractors with expertise to navigate the new and evolving requirements to help protect and defend the Department of Defense (DoD) supply chain from cyber risks.

DIB PARTNER AND CONTRACTOR EDUCATION

- Our experience performing financial statement audits, attestation engagements, and consulting support projects places Cotton & Company among the best in the industry in assisting DIB partners and contractors in understanding National Institute of Standards and Technology (NIST) guidance and the CMMC framework, model, certification requirements, and best practices.
- We are able to provide our clients with tailored CMMC educational courses and stand ready to assist our clients in staying ahead of the progressive timeline for full implementation of the CMMC framework.

IMPLEMENTATION AND COMPLIANCE SUPPORT SERVICES

- Cotton & Company has a track record of implementing and executing effective risk-based management control programs.
- Our services include assisting with the design, documentation, and implementation of required cybersecurity controls; assisting in establishing proper governance structures; and developing, implementing, and monitoring corrective action plans.

CMMC READINESS ASSESSMENTS

- To achieve CMMC certification, DIB partners and contractors must assess the as-is and to-be states of their cybersecurity environment to gauge their current level of information security, identify and track risks more effectively, and prioritize information security and system procurement needs.
- Cotton & Company performs pre-assessments to assist our clients in identifying corrective actions and implementing the required cybersecurity controls.

CMMC AUDIT SUPPORT SERVICES

- Cotton & Company has significant experience in assisting agencies in implementing new requirements, including acting as a liaison between management and their selected certified third-party assessor organization (C3PAO).
- We will support the full life cycle of the CMMC audit on behalf of our clients, working with the parties to ensure efficient, seamless, and streamlined processes to mitigate audit budget and timeline overruns while achieving the desired certification level.



CMMC ASSURANCE/ OVERSIGHT SUPPORT

Cotton & Company stands ready to assist DIB-sector partners and contractors with all aspects of their oversight responsibilities.

PERFORMANCE AUDITS

- Performance audit objectives are tailored to the needs of the organization and include assessing program effectiveness, economy, and efficiency; internal controls; compliance; and prospective analyses.
- Cotton & Company has significant and varied performance audit experience, including audits of compliance with rules and regulations and NIST SP 800-171 audits, as well as cybersecurity and Federal Information Security Modernization Act (FISMA) audits.

IT AND CYBERSECURITY AUDITS

- Our IT and cybersecurity audit testing includes evaluating access controls; configuration and change management; systems development life cycles, including audits of Agile and Waterfall implementations, disaster recovery, and contingency planning; and overall governance and security frameworks.
- We have also performed in-depth cybersecurity audits of firewall design and implementation, including analyzing firewall rule sets and the implementation, management, and monitoring of security information event management (SIEM) tools used as part of security operations centers.

Although there are currently no CMMC Accreditation Board C3PAOs, Cotton & Company is following the CMMC Accreditation Body processes to become a C3PAO that can provide participating DIB partners and contractors with consistent and informative assessments against the defined set of controls/best practices within the CMMC program. We are currently ready and able to assist DIB partners and contractors with their CMMC readiness efforts.

CONTACT

Gary Barton, Practice Lead
gbarton@cottoncpa.com

CONTACT

Loren Schwartz, Practice Lead
lschwartz@cottoncpa.com