Achieve CMMC/DFARS Capabilities with SCA

SECURITY COMPLIANCE ASSOCIATES

The US Council of Economic Advisors estimates that malicious cyber activity could cost the national economy upwards of $1 trillion by the year 2026.

As a supplier or contractor for the United States Department of Defense (DOD), you're required to maintain CMMC (Cybersecurity Maturity Model Certification) compliance in conjunction with DFARS (Defense Federal Acquisition Regulation Supplement) requirements. These lengthy program names serve a succinct purpose: to fortify our national cybersecurity posture in an effort to protect our data and reduce the economic impact of cyberattacks.

Any contractor or subcontractor who handles Controlled Unclassified Information (CUI) is required to follow these federal regulations regarding cybersecurity practices. The team at Security Compliance Associates understands that navigating these standards can be challenging, especially if you—or your suppliers—are a small firm with limited resources.

DOD contractors and subcontractors must do the following to be in good standing:

- Complete a NIST SP 800-171 DoD Basic Assessment
- Upload Assessment scoring and required documentation into the Supplier Performance Risk System (SPRS)
- Achieve the appropriate CMMC level certification as required by the contracting documents/solicitation

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

Let the team of experts at SCA guide you through the tedious process of achieving CMMC compliance as part of DFARS regulations! SCA has been trusted as a leading cybersecurity expert since 2005 and continues to diligently protect assets, resources, and reputation across a wide array of industries.

SCA is a CMMC-AB Registered Provider Organization (RPO) and offers a variety of services to help you and your suppliers maintain a strong cybersecurity posture:

- **NIST 800-171 DoD Assessment:** Following DFARS 252.204.7020 requirements, SCA will evaluate your organization against the 110 controls found in NIST 800-171; this also includes gap analysis, scoring per NIST methodology, and creating a Plan of Action and Milestones (POAM)
- **System Security Plan:** This service includes a thorough review of your existing SSP, revising your current security plan, and annual maintenance of this vital document
- **CMMC Gap Analysis:** Depending on your specific CMMC requirements, SCA will evaluate your organization in relation to one of three CMMC levels in CMMC 2.0

> Their staff was friendly, non-disruptive to our practice, and provided a comprehensive and helpful report. **I recommend them to any practice.**

For DoD contractors or suppliers who only handle Federal Contract Information (FCI), your requirements are less stringent. These basic cybersecurity hygiene practices remain a part of CMMC 2.0. SCA can help ensure your organization adopts them appropriately, thereby securing your place in the supply chain.