B | RILEY Advisory Services

COMPLIANCE, RISK & RESILIENCE:

DFARS AND CMMC 2.0 COMPLIANCE

BACKGROUND

On November 30, 2020, the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, 7019, 7020 and 7021 took effect. The regulation updated defense contractors' obligation to come into compliance with NIST SP 800-171, described a new level of scrutiny of contractor compliance, and introduced tougher Department of Defense (DoD) assessment requirements. The rule established DFARS and Cybersecurity Maturity Model Certification (CMMC) as gating requirements for U.S. or foreign entities wishing to provide goods and services to the U.S. Defense Department, whether as a direct, prime or subcontractor.

CMMC 2.0 - UNDER RULEMAKING

From November 2021 through February 2022, after significant industry comment and an internal DoD assessment of the implementation of the CMC program, the DoD issued "CMMC 2.0", designed to simplify the program structure and improve adoption and implementation. The DoD will formalize CMMC 2.0 in new rulemaking expected in 2H22 or 1H23 that will be open to further public comment. Until then, no DoD procurements will include a CMMC requirement.

When formalized, CMMC 2.0 is expected to require that contractors and their subcontractors will maintain compliance with current DFARS requirements and become assessed at one of three CMMC levels as a condition of contract award, based on the level of contractors' interaction with Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

CMMC 2.0 Levels	Level 1 Foundational	Level 2 Advanced	Level 3 Expert
Objective	Safeguard FCI	Safeguard CUI	Safeguard CUI in Critical Programs
Security	17 Core Practices	110 Practices Aligned with NIST 800-171	110+ Practices Based on NIST 800-172
Assessment	Annual Self-Assessment	Independent C3PAO Assessment	Triennial DBCAC Assessment
Impact	All DoD Contracts	All Contracts with CUI	500-600 Mission Critical Contracts
Ongoing DFARS	Continue to Attest to DFARS 252.204—7012, 8019, 7020 & 7021 Relative to NIST 800-171		

DFARS - CURRENT REQUIREMENT

The DFARS addresses the national security risk from what the DoD considers inadequate security of CUI that is in place throughout the Defense Industrial Base (DIB) supply chain. The rules materially raise the cybersecurity bar for DoD contractors and subcontractors. Self-attestation of cybersecurity compliance with NIST 800-171 is now replaced with the scrutiny of the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), supported by the official disclosure of compliance scores on the Supplier Performance Risk System (SPRS) database, at three security levels.

HOW DOES THIS AFFECT YOUR ORGANIZATION?

The enforcement mechanism that was missing in the original release of the cyber DFARS (7012) is now resolved with the requirement for a C3PAO assessment or a DIBCAC audit of contractor cybersecurity programs. With CUI it also means that the DoD has less incentive to give organizations that have been self-attesting to the DFARS a long runway to finish up their POAM.

Organizations that are already attesting that they meet NIST 800-171 should make sure they meet all the requirements in NIST 800-171A, not just their organizational interpretation of 171. They should understand and consider the enhanced exposure to liability they could face under the False Claims Act after cyber breaches.

It would not be surprising for future contracts to require POAMs to be closed within six months of the awarding of a DoD contract. This means contractors need to meet all the requirements of NIST 800-171 as defined in NIST 800-171A in a rather brief period and must pass a C3PAO or government audit.

The time between now and the final rule making is the best time to close security gaps. The change from CMMC 1.0 to CMMC 2.0 did not change the basic intent of the program – to encourage contractors to meet the full requirements of NIST 800-171 & NIST 800-171A. Instead, CMMC 2.0 made a few control enhancements, changed the administration of CMMC, made stronger cybersecurity in the DIB even more of an imperative, and subtly but clearly added liability "teeth" to process.

SERVICES

As a CMMC-AB Registered Provider Organization (RPO), the Compliance, Risk & Resilience practice offers a unique approach to CMMC compliance for our defense clients. Our approach includes the following steps:

- **Model the Flow of CUI** – We first develop an overall model of the flow and "behavior" of CUI within the organization and how CUI flows among corporate departments, functions and processes by facilitating business process analysis.
- **Define the CMMC Boundary** – We then establish the "CMMC operational boundary" to identify that part of the client's environment that touches CUI and must meet federal cybersecurity requirements.
- **Develop the CMMC Gap Assessment and Remediation Plan** – We conduct the CMMC gap analysis within the boundary and create the gap remediation plan. This will ultimately position the client for a successful 3rd party CMMC audit, support its SP 800-171 attestation, its SSP and POAM, and prepare the client for any DoD audits.
- **Define Support Client Implementation & Validate C3PAO Assessment Readiness** – We assist and support our clients' efforts to close compliance gaps. We carefully review their remediation efforts, provide our validation of their efforts, and determine their readiness for an assessment by an independent, Certified 3rd Party Assessment Organization licensed by the CMMC Accreditation Body (CMMC-AB).

REPRESENTATIVE ENGAGEMENTS

DFARS Gap Assessment for Global Company Entering the Defense Sector
We conducted a NIST 800-171 and ISO 27001 current state assessment, gap analysis, and remediation and compliance roadmap for a multinational trading company becoming part of the defense industrial base (DIB).

CMMC L3 Review for Silicon Valley Communications Technology Provider
We identified improvements needed to get a SPRS score of 110 for NIST 800-171 and assessed the additional 20 controls required for CMMC L3, identifying the gaps necessary to close. We are validating that the updates will pass a CMMC audit.

CMMC Compliance Strategy for Biotherapeutics Company
We reviewed the research and clinical operational plans of a biotech company doing COVID work, and advised on information security program changes that will be required to become a provider to the DoD.

ABOUT B. RILEY ADVISORY SERVICES

B. Riley Advisory Services provides specialty advisory services and solutions to complex business problems and board-level agenda items. Our team applies a unique mix of skill sets to address top-level, non-typical business challenges, such as developing compliance and risk systems for organizations, planning and executing a major acquisition or divestiture, pursuing a fraud investigation or corporate litigation, or managing through a business crisis or bankruptcy. In addition, we are a leading provider of valuation and appraisal services for asset-based lending applications.

Our team works with lenders, law firms, government entities, private equity sponsors and companies of all types. Our Advisory Services are a unique mix of Compliance, Risk & Resilience Services, Valuation and Appraisal Services, Restructuring and Turnaround Management, Operations Management Services, Forensic Accounting and Litigation Support and Transaction Support Services including Due Diligence and Quality of Earnings Reviews. B. Riley Advisory Services is a combination of the firms formerly known as GlassRatner Advisory & Capital Group and Great American Group.

ABOUT B. RILEY FINANCIAL (“B. RILEY”)

B. Riley Financial, Inc. (NASDAQ: RILY) companies provide tailored financial solutions to meet the strategic, operational, financial advisory and capital needs of its clients through a diverse range of collaborative and complementary business capabilities.

THE B. RILEY DIFFERENCE

Led by the former CISO of major defense prime contractors with founding level expertise in DFARS security requirements, our team uses a unique, purpose-built tool to:

- Manage and integrate the workflow of DFARS and CMMC gap assessments
- Collect artifacts that validate findings and observations
- Design actionable remediation programs within budget
- Develop remediation options, recommendations, and project plans
- Create technical, compliance and risk management oversight reports
- Provide visibility to prime contractors into the security of their supply chains

PRACTICE LEADER

Duane Lohn
dlohn@brileyfin.com
(602) 321-9818

Corey Gooch
cgooch@brileyfin.com
(312) 925-8550