Compliance, Risk & Resilience:

DFARS AND CMMC COMPLIANCE

On November 30, 2020, the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, 7019, 7020 and 7021 took effect. The regulation updates defense contractors' obligation to come into compliance with NIST SP 800-171, describes a new level of scrutiny of contractor compliance, and introduces tougher Department of Defense (DoD) assessment requirements. The rule has 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.

Every contract procurement from the DoD requires prime contractors and the subcontractors throughout their supply chains to:

- Maintain compliance with DFARS requirements that align their cybersecurity practices to NIST 800-171 at one of three levels, in a way that demonstrates credible maturity efforts and meets the scrutiny of defense procurement officers.
- Between now and 2025, become independently certified at one of five 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).

The DFARS addresses the national security risk from what the DoD considers inadequate security of Controlled Unclassified Information that is in place — especially at smaller companies — throughout the Defense Industrial Base (DIB) supply chain. The rule materially raises the cybersecurity bar:

- Self-attestations of cybersecurity compliance to NIST 800-171 are replaced with the scrutiny by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), supported by the official disclosure of compliance scores on the Supplier Performance Risk System (SPRS) database.
    - "Basic" contracts accept self-attestation, but contractors must submit scores to SPRS, creating risk if contract officers find that POAMs are not well executed.
    - "Medium" contracts includes a DIBCAC audit of submitted compliance artifacts that could result in a physical audit if DIBCAC cannot verify compliance.
    - "High" contracts include a mandatory physical DIBCAC audit.
- Compliance to CMMC is binary — organizations either pass 100% of the controls at the CMMC level assigned by their defense contracts or they are prohibited from participating.
- Prime contractors are responsible for the compliance of subcontractors in their supply chains.
- Falsified results expose contractors to legal jeopardy under the False Claims Act and the Federal Contract Act.

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.

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 LEADERS

Scott Corzine
scorzine@brileyfin.com
(917) 930-5300

Steve Gilmer
sgilmer@brileyfin.com
(248) 832-3808

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

ABOUT THE FIRM

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, 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 formally 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.

B. Riley's diverse suite of business capabilities goes beyond traditional financial service offerings. By leveraging cross-platform expertise and assets, our business units are uniquely positioned to provide full service, collaborative solutions at every stage of the business life cycle and in all market conditions. B. Riley is made more exciting by our willingness to invest our own capital in opportunities organically derived from the platform along with our ability to maximize return on investment by leveraging in-house operational expertise.