Supply Chain Cybersecurity Readiness

We provide Cybersecurity assessment against Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 (NIST SP800-171) to identify supplier risk and provide solutions toward compliance.

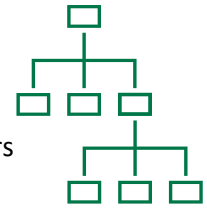
Applicable to:

Organizations that have contracts with the US Department of Defense (DoD) and access to its Controlled Unclassified Information (CUI), as well as any of their subcontractors.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 defines the regulations for compliance in government/DoD contractor organizations.

Who needs to comply?

- Government Contractors
- Government Subcontractors
- Defense Industrial Base (DIB) Suppliers
- DIB Suppliers' Subcontractors



What is CUI?

- Data or information deemed sensitive and relevant to the interests of the United States but not strictly regulated by the federal government
- Data or information whose importance does not rise to "classified" (e.g., Confidential, Secret, or Top Secret)
- Data or information acquired or generated in relation to a government contract

Benefits:

- **Reduced risk of breaches and threats**
- **Best practices for data access and policies**
- **Business continuity and compliance**
- **Enhanced system protection**
- **Security awareness**

Risks:

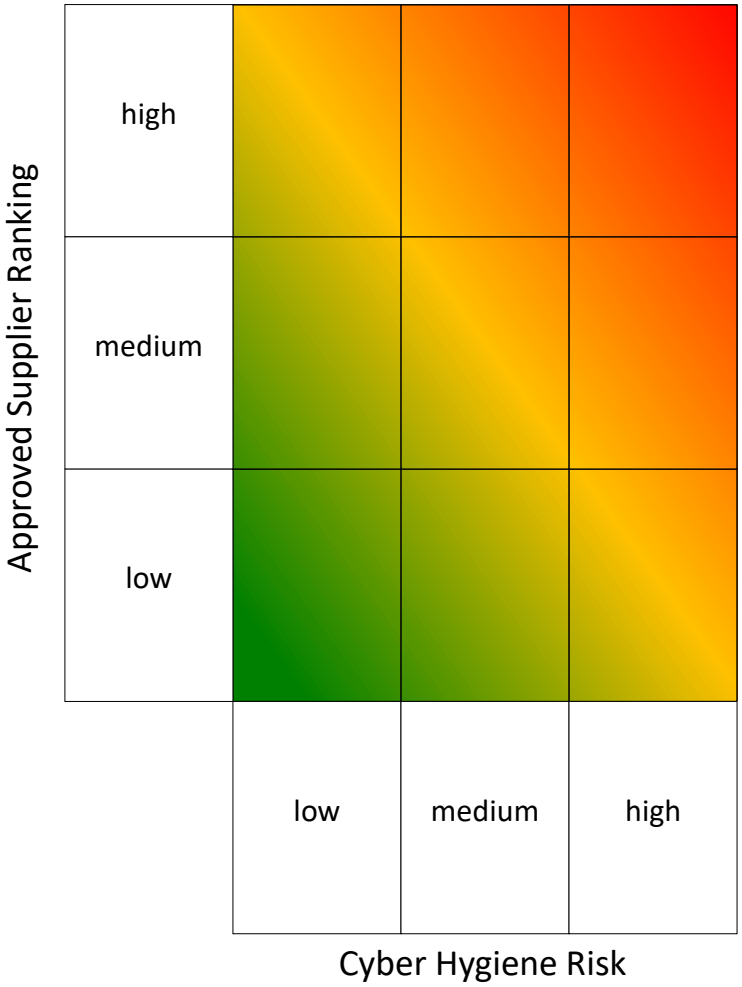
Threats are real.
You could be a target.

The **DoD** may impose fines or financial penalties, including damages for breaches of contract and false claims.

The **DoD** can terminate contracts and even bar the contractor in question from working with the **DoD** on future projects

SQA SERVICES, INC.
550 Silver Spur Rd, 3rd Floor | Rolling Hills CA 90275 | Phone (310) 544 6888; (800) 333 6180 | Fax (310) 544 5541
www.sqaservices.com | info@sqaservices.com

Supplier Assessment Risk-Based Model



SQA Managed Solutions

Supply Chain Analysis

- Supplier ranking methodology
- Cyber trend identification
- Vulnerability strategy plan

Supplier Evaluation Program

- Supplier Desktop Evaluation tool in STEPQ
- Supplier Cyber Hygiene scorecard using DoD Assessment Methodology (DAM)-based score

Full Readiness Program

- Pre-assessment planning
- On-site assessment
- Cyber-expert assessor
- Security Assessment Report (SAR)
- System Security Plan (SSP) Analysis
- Plan of Actions and Milestones (POAM) in STEPQ

Client uses Internal Strategic Supply Management Resources

Summary:

SQA's Cybersecurity readiness programs involve the inspection of digital and physical security elements that preserve intellectual property, human life, and the physical information of our clients. Cybersecurity preserves the strategic advantage of the US Armed Forces and the US government. SQA can aid the government's prime suppliers to guarantee a supply chain that has controls to identify, detect, protect from, respond to, and recover from cyber espionage and other attacks.

SQA Global Solutions: SQA Services specializes in providing Supplier Audit, Engineering, and Inspection services globally. For more than 25 years, SQA has helped clients reach their quality and business objectives, with annual capacities supporting global compliance as follows:

3,000 Audits	150,000 Inspection Hours	40,000 Engineering Hours	70 Countries	1,000 SQA Associates

SQA SERVICES, INC.
550 Silver Spur Rd, 3rd Floor | Rolling Hills CA 90275 | Phone (310) 544 6888; (800) 333 6180 | Fax (310) 544 5541
www.sqaservices.com | info@sqaservices.com