MAD Security
Making A Difference

Defense Federal Acquisition Regulation Supplement (DFARS) Compliance

Understanding the DFARS Regulation

The Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-Clause 7012 is the latest U.S. mandate requiring all Department of Defense (DoD) prime contractors and subcontractors to protect Controlled Unclassified Information from unauthorized disclosure or processing as well as requirements for reporting on incidents.

DFARS mandates NIST SP 800-171 control compliance, which protects Covered Defense Information (CDI) on non-federal information systems for systems on premises or DFARS 252.239-7010, which specifies requirements for Cloud Computing Services.

Steps to Becoming Compliant

1. A Gap Assessment is performed on the NIST 800-171 security controls to evaluate your current level of implementation.
2. Develop a Plan of Actions and Milestones (POA&M); this is an actionable plan to achieve compliance with the 800-171 controls.
3. Develop a System Security Plan (SSP) that provides an overview of security requirements of your environment and describes the controls in place or planned.
4. Maintain a Continuous Monitoring Strategy to assist in making progress towards implementation of the 800-171 security controls.

IN ORDER TO MAINTAIN CURRENT DoD CONTRACTS AND BID ON FUTURE CONTRACTS, A COMPLETED POA&M AND SSP SHOULD BE IN EFFECT.

About Us

MAD Security is the premier provider of information and cyber security solutions that combine technology, services, support, and training. MAD Security has enabled clients in a wide range of verticals to manage risk, meet compliance requirements and reduce costs while maximizing security effectiveness and operational efficiency. MAD Security is committed to cyber security excellence and has a track record of delivering quality solutions.

MAD Security, LLC. (888) MAD-SEC4 info@MADSecurity.com MADSecurity.com

MAD Security
Making A Difference

Become DFARS Compliant with Managed Security Services

3.1 Access Control

- User Activity Monitoring
- Log Monitoring & Management Intrusion Detection System (HIDS/NIDS)
- SIEM
- Configuration & Vulnerability Scanning

3.2 Awareness & Training

- Human Security Behavior Assessment
- Phishing Training
- Network Behavior Analysis

3.3 Audit & Accountability

- File Integrity Monitoring
- Real-time Service & Infrastructure Monitoring
- User Activity Monitoring
- Log Management
- Intrusion Detection System (HIDS/NIDS)
- SIEM
- Configuration & Vulnerability Scanning

3.4 Configuration Management

- User Activity Monitoring
- Log Monitoring & Management
- Intrusion Detection (HIDS/NIDS)
- SIEM
- Security Event Correlation
- Vulnerability Scanning

3.5 Identification & Authentication

- User Activity Monitoring
- Log Monitoring & Management
- Network Monitoring
- Intrusion Detection System (HIDS/NIDS)
- SIEM
- Detection of changes to assets and applications in your environment

3.6 Incident Response

- Incident Response & Analysis
- Prioritization of incident response & remediation efforts
- Discovery & tracking of hosts, services, installed software present in the environment for improved correlation and context

3.7 Maintenance

- Real-time Service & Infrastructure Monitoring
- Asset Monitoring
- Equipment maintenance & sanitation
- Vulnerability scanning of media assets
- Behavioral Monitoring
- Continuous Monitoring

3.8 Media Protection

- Monitoring & Control of Media Access
- Monitoring of CDI Transmission, Access & Storage
- Monitoring & Control of Media Devices
- Asset Scanning
- Intrusion Detection System (HIDS)

3.9 Personnel Security

- Monitoring of CUI Transmission, Access & Storage
- Human Security Behavior Assessment & Monitoring
- Phishing Training

3.10 Physical Protection

- Access Monitoring & Alerts
- Log Management & Incident Response
- Behavior Monitoring
- Asset Inventory & Availability Monitoring

3.11 Risk Assessment

- Incident Response & Analysis
- Prioritization of incident response & remediation efforts
- Discovery & tracking of hosts, services, installed software present in the environment for improved correlation and context

3.12 Security Assessment

- Real-time Service & Infrastructure Monitoring
- Asset Monitoring
- Equipment maintenance & sanitation
- Vulnerability scanning of media assets
- Behavioral Monitoring
- Continuous Monitoring

3.13 Communications & System Protection

- Monitoring & Control of Media Access
- Monitoring of CDI Transmission, Access & Storage
- Monitoring & Control of Media Devices
- Asset Scanning
- Intrusion Detection System (HIDS)

3.14 System & Information Integrity

- SIEM
- Threat Intelligence Monitoring & Reporting
- Network Analysis & Monitoring
- Vulnerability Scanning
- Prioritization of incident response and remediation efforts

Why MAD Security

At MAD Security, our goal is to **M**ake **A D**ifference in everything we do for our customers. While defending and improving the security of your information is our top priority, we also know that understanding your business goals is of equal importance to ensure compliance and efficiency. When partnering with MAD Security, you can rest easy knowing that our services will:

- Exceed required compliance
- Be cost-effective
- Be maintained to keep you compliant
- Be resource efficient

MAD Security, LLC. (888) MAD-SEC4 info@MADSecurity.com MADSecurity.com