



#### 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



A Gap Assessment is performed on the NIST 800-171 security controls to evaluate your current level of implementation.



Develop a Plan of Actions and Milestones (POA&M); this is an actionable plan to achieve compliance with the 800-171 controls.



Develop a System
Security Plan (SSP) that
provides an overview of
security requirements of your
environment and describes
the controls in place or
planned.



Maintain a Continuous Monitoring Strategy to assist in making progress towards implementation of the 800-171 security controls.

# 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.















### BECOME 800-171 COMPLIANT WITH MANAGED SECURITY SERVICES

Audit & Accountability

User Activity Monitoring Log Monitoring & Management Intrusion Detection System

Access Control

- (HIDS/NIDS)
- Configuration & Vulnerability Scanning
- Awareness & Training **Human Security** 
  - Behavior Assessment Phishing Training Network Behavior **Analysis**
- File Integrity Monitoring Real-time Service &
- Infrastructure Monitoring User Activity Monitoring
- Log Management Intrusion Detection
- System (HIDS/NIDS) SÍFM
- Configuration & Vulnerability Scanning

Configuration Management

User Activity Monitoring Log Monitoring &

Intrusion Detection

Vulnerability Scanning

Management

(HIDS/NIDS)

Correlation

Security Event

SIEM

- User Activity Monitoring Log Monitoring &

Identification & Authentication

- Management
- Network Monitoring Intrusion Detection
- System (HIDS/NIDS)
- SÍEM
- Detection of changes to assets and applications in vour environment

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

#### **Maintenance**

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

Media Protection

- Media Access Monitoring of CDI Transmission, Access & Storage
- Monitoring & Control of Media Devices
- **Asset Scanning**
- Intrusion Detection System
- Monitoring of CUI Transmission, Access & Storage

Personnel Security

- Human Security Behavior Assessment & Monitoring
- Phishing Training

Communications & System Protection

Access Monitoring & Alerts

Physical Protection

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

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
- Security Assessment
- Real-time Service & Infrastructure Monitoring
- **Asset Monitoring** Equipment maintenance & sanitation
- Vulnerability scanning of media assets
- Behavioral Monitoring
- Continuous Monitoring
- Monitoring & Control of Media Access
- Monitoring of CDI Transmission, Access & Storage
- Monitoring & Control of Media Devices
- **Asset Scanning**
- Intrusion Detection System (HIDS)
- SIEM

3.14

Threat Intelligence Monitoring & Reporting

System & Information Integrity

- Network Analysis & Monitoring
- Vulnerability Scanning
- Prioritization of incident response and remediation efforts

# WHY MAD SECURITY

At MAD Security, our goal is to Make A Difference 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 as your Managed Security Services Provider, you can rest easy knowing that our services will:

**Exceed required compliance** 

Be resource efficient

Be cost-effective

Be maintained to keep you compliant

MAD Security is the premier provider of information and cybersecurity 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.







