MADSecurity

NIST SPECIAL PUBLICATION 800-171 FOR HIGHER EDUCATION

UNDERSTANDING THE NIST 800-171 REGULATION

Colleges and Universities are faced with safeguarding **Controlled Unclassified Information (CUI)**. Whether they have large government research contracts, or just one small contract, it will need to comply with the NIST SP 800-171 security controls. In addition, the US Department of Education intends to make student financial data subject to the NIST 800- 171 controls in the very near future.

CUI can be any data received from the federal government that is not designated as classified. Some examples can be:

- **Controlled Technical Information**
- **Student Records**
- **Student Financial Information**
- **Health Records**
- **Export Control Data**
- **Research Data**
- **Engineering Data and Drawings**
- **Patent Information**
- **Agricultural Data**

The NIST SP 800-171 is the minimum security standard for protecting CUI for Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012, Federal Acquisition Regulation (FAR) clause, and the US Department of Education. This includes institutions receiving defense contracts, defense grants, civilian contracts, and student financial data.

STEPS TO BECOMING COMPLIANT

1

Perform a Gap Assessment 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.

CONTACT US

☎ 888-623-7324

madsecurity.com

MADSecurity

BECOME 800-171 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 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.

CONTACT US

☎ 888-623-7324 madsecurity.com