Overview of the NIST 800-171 Security Framework

In October 2016, the Department of Defense (DoD) promulgated a final rule implementing Defense Federal Acquisition Regulation Supplement (DFARS) clauses that apply to all contractors who process, store or transmit "covered defense information." As a result, many businesses are now required to implement the NIST 800-171 security framework.

Adopting the defense in depth methodology requires the implementation of 14 families of controls, leveraging existing practices and infrastructure. In addition, this creates opportunities to implement advanced solutions such as privilege management and next generation firewalls. All requirements in the NIST 800-171 are traced to NIST 800-53 and FIPS where most controls require both a procedural and technical control to implement the procedure.

NIST CONTROLS

CONTROL 1: ACCESS CONTROL

The Access Control requirement is the most salient control in the NIST 800-171. In general, this control family specifies limiting system access to authorized users and making sure those users are only able to do specified actions based on job functions (also known as the principle of least functionality). Separation of duties through security groups and Access Control Lists (ACLs) can be applied to meet this control.

CONTROL 2: AWARENESS AND TRAINING

Leadership and employees should receive security and awareness training on secure usage of the information systems. This is essential to satisfying NIST 800-171 requirements. Conducting mandatory annual security training and exercises is necessary to keep employees lucid and vigilant.

CONTROL 3: AUDIT AND ACCOUNTABILITY

NIST 800-71 Audit and Accountability requirements focus specifically on ensuring that an organization's audit generation and reporting capabilities sufficiently support the security monitoring and management needed for a secure environment.

CONTROL 4: CONFIGURATION MANAGEMENT

Change is defined as the addition, modification, or removal of configuration items. Processes and standard configurations promote systematic changes to maintain integrity over time.

aemcorp.com | 13880 Dulles Corner Lane, Suite 300, Herndon, VA 20171

Overview of the NIST 800-171 Security Framework

CONTROL 5: IDENTIFICATION AND AUTHENTICATION

Identification and authentication requirements ensure systems are properly identifying users and verifying their identity prior to granting any access. Multi-Factor Authentication can be a key component to meeting this control.

CONTROL 6: INCIDENT RESPONSE

Organizations should have operational incident-handling capabilities that include adequate preparation, detection, analysis, containment, recovery, and user response activities.

CONTROL 7: MAINTENANCE

System maintenance should be performed at regular intervals to protect organizational information systems from zero-day attacks and other vulnerabilities.

CONTROL 8: MEDIA PROTECTION

On-premise media should be physically protected and monitored to adequately protect it from loss or theft.

CONTROL 9: PERSONNEL SECURITY

Verifying and validating personnel though background checks and other vetting processes are important steps to onboarding procedures.

CONTROL 10: PHYSICAL PROTECTION

Physical protection can be enforced with alarm systems, locks and cameras.

CONTROL 11: RISK ASSESSMENT

Standard assessments are needed to identify risks related to procedures, functions, information systems. Implementing standard controls and security scans can be used to stay abreast of system vulnerabilities.

CONTROL 12: SECURITY ASSESSMENT

Auditing controls, processes and procedures should be completed to validate that the security posture meets the NIST standards. An outside assessment can also be a validation of the security framework.

CONTROL 13: SYSTEM AND COMMUNICATIONS PROTECTION

Highly secure firewalls should guard the perimeter of your organization and provide intrusion prevention/detection capabilities. Segmented networks are another best practice for both security and performance.

CONTROL 14: SYSTEM AND INFORMATION INTEGRITY

Keeping antivirus signatures up to date while scanning for viruses and malware is an essential step in maintaining system and information integrity. Malicious websites should be filtered and denied access from corporate resources.

aemcorp.com | 13880 Dulles Corner Lane, Suite 300, Herndon, VA 20171