Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G501 Cybersecurity Framework Guidance

CONTENTS:

I. DEFINITIONS

Security Framework: A security framework consists of a series of functions promoting layered security defenses which include a series of different defenses each used to cover the gaps in the others' protective capabilities.

II. RATIONALE

A security framework relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk.

III. GUIDELINE

The framework can be used to help identify and prioritize actions for reducing cybersecurity risk and can be used as a tool for aligning policy, business, and technological approaches to managing that risk.

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are: Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.
- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities

Establishing the Framework

Organizations can use the framework to develop and improve their security program by:

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps.

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step.

Critical Security Controls

Agencies can accelerate implementation of the CSF through the early adoption of the Center for Internet Security (CIS) Critical Security Controls (CSC). The CSCs are effective because they represent the combined knowledge of actual attacks and how to prevent them.

The five tenets reflected in the CSC are:

- Offense informs defense: Leverage attack forensics to design effective defensive controls.
- Prioritization: Implement CSCs that provide the greatest risk reduction.
- Metrics: Develop metrics that security, IT personnel, management, and auditors understand.
- Continuous Monitoring: Test and validate security measures effectiveness.
- Automation: To achieve reliable, scalable, and continuous measurements.

CSC Critical Security Controls

The following CSCs are prioritized to provide the greatest risk reduction. Agencies may implement CSC in series or parallel subject to resource availability. A detailed description of the CSCs is contained within the CIS Measurement Companion to the CIS Critical Security Controls *(Version 6)* .

The CSCs listed below are mapped to the NIST SP 800-53 (Revision 4): Controls for ease of reference.

CSC 1: Inventory of Authorized and Unauthorized Devices
[NIST 800-53 Rev 4: CA-7, IA-3, SI-4, CM-8, SA-4, PM-5, CM-8, SA-4, PM-5, SC-17]
CSC 2: Inventory of Authorized and Unauthorized Software
[NIST 800-53 Rev 4: CA-7, CM-8, SA-4. SI-4, CM-2, CM-10, SC-18, PM-5, CM-11, SC-34]
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers [NIST 800-53 Rev 4: CA-7, CM-6, CM-11, SC-15, CM-2, CM-7, MA-4, SC-34, CM-3, CM-8, RA-5, SI-2, CM-5, CM-9, and SA-4. SI-4]
CSC 4: Continuous Vulnerability Assessment and Remediation
[NIST 800-53 Rev 4: AC-2, AC-19, IA-5, AC-6, CA-7, SI-4, AC-17, IA-4]
CSC 5: Controlled Use of Administrative Privileges
[NIST 800-53 Rev 4: AC-2, AC-19, IA-5, AC-6, CA-7, SI-4, AC-17, 1A-4]
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
[NIST 800-53 Rev 4: AC-23, AU-6, AU-11, IA-10, AU-2, AU-7, AU-12, SI-4, AU-3, AU-7, AU-12, SI-4, AU-3, AU-8, AU-13, AU-4, AU-9, AU-14, AU-5, AU-10, CA-7]
CSC 7: Email and Web Browser Protections
[NIST 800-53 Rev 4: CA-7, CM-6, CM-11, SC-15, CM-2, CM-7, MA-4, SC-35, CM-3, C,-8, RA-5, SI-2, CM-5, CM-9, SA-4, SI-4]
CSC 8: Malware Defenses
[NIST 800-53 Rev 4: CA-7, SC-44, SI-4, SC-39, SI-3, SI-8]
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
[NIST 800-53 Rev 4: AT-1, AT-4, PM-13, AT-2, ASA-11, PM-14, AT-2, SA-11, PM-14, AT-3, SA-16, PM-16]
CSC 10: Data Recovery Capability
[NIST 800-53 Rev 4: CP-9, AP-10, PR-4, IP-4, MP-4]
CSC 11: Secure Configurations for Network Devices; Firewalls, Routers, and Switches
[NIST 800-53 Rev 4: AC-4, CA-9, CAM-5, MA-4, CA-3, CM-2, CM-6, SC-24, CA-7, CM-3, CM-8, SI-4]
CSC 12: Boundary Defense
[NIST 800-53 Rev 4: AC-4, CA-7, SC-7, AC-17, CA-9, SC-8, AC-20, CM-2, CI-4, CA-3, SA-9]
CSC 13: Data Protection
[NIST 800-53 Rev 4: AC-3, CA-9, SC-8, SI-4, AC-4, IR-9, SC-28, AC-23, MP-5, SC-31, CA-7, SA-18, SC-41]
CSC 14: Controlled Access Based on the Need to Know
[NIST 800-53 Rev 4: SA-1, AC-6, RA-2, AC-2, AC-24, SC-16, AC-3, CA-7, SI-4, MP-3]

CSC 15: Wireless Access Control
[NIST 800-53 Rev 4: AC-18, CM-2, SC-40, AC-19, IA-3, SI-4, CA-3, SC-8, CA-7, SC-17]
CSC 16: Account Monitoring and Control
[NIST 800-53 Rev 4: AC-2, CA-7, AC-3, IA-5, AC-7, SI-4, IA-10, AC-11, SC-17, AC-12, SC-23]
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
[NIST 800-53 Rev 4: AT-1, AT-4, PM-13, AT-2, SA-11, PM-14, AT-3, SA-16, PM-16]
CSC 18: Application Software Security
[NIST 800-53 Rev 4: SA-13, SA-20, SI-11, SA-15, SA-21, SI-15, SA-16, SC-39, SI-16, SA-17, SI-10]
CSC 19: Incident Response and Management
[NIST 800-53 Rev 4: IR-1, IR-4, IR-7, IR-2, IR-5, IR-8, IR-3, IR-6, IR-10]
CSC 20: Penetration Tests and Red Team Exercises
[NIST 800-53 Rev 4: CA-2, CA-8, PM-6, CA-5, RA-6, PM-14, CA-6, SI-6]

CSC Measurements

Agencies can measure their CSC progress utilizing the methodology outlined in the CIS Measurement Companion to the CIS Critical Security Controls (Version 6). In addition, in partnership with SANS, AuditScripts offers a free CSC implementation assessment tool to measure the maturity levels within the agency.

IV. PROCEDURE REFERENCE

NIST SP 800-53 (Revision 4)
NIST Cybersecurity Framework
NIST Cybersecurity Core
CIS Measurement Companion to the CIS Critical Security Controls *(Version 6)*
Enterprise ITA Policy P4140 (Cybersecurity Framework)

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.
To report an incident, send email to: security@cio.idaho.gov or call (208) 332-1510.

REVISION HISTORY

Effective date: December 15, 2015