

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

<System Name> (<System Acronym>)

System Security Plan (SSP)  
Document Evaluation

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Nate Lee Andrew Bennett Ernie Riviere | Initial release of MITRE ACT templates and work aids. |

Purpose

This System Security Plan (SSP) Document Evaluation Checklist is designed to help assess the completeness of the application’s SSP. The evaluation criteria were derived from industry best practices and from <Organization>’s policies and procedures.

How the Checklist Is Used:

1. The document is reviewed to verify that each of the requirements noted in the checklist is adequately addressed in the document.
2. The Status column indicates whether each requirement is:
   1. **Met** **-** The requirement has been completely satisfied, and no additional information needs to be documented.
   2. **Partial -** The requirement has been partially satisfied but there is still missing information as explained in the **Comments** column.
   3. **Not Met -** The requirement has not been satisfied and any additional information noting the reasons are provided in the **Comments** column.
   4. **N/A -** The requirement is not applicable to the system that is being evaluated and the reason that it is not applicable is provided in the **Comments** column.
3. The Comments column contains an explanation if a control is not met, partially met, or not applicable.
4. The Low, Moderate, and High columns indicate whether or not the control is part of the Low, Moderate, or High control baselines.

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Topics Quick Reference

[1. Assessment Logistics 1](#_Toc199515887)

[2. General Requirements 1](#_Toc199515888)

[3. Access Control (AC) 7](#_Toc199515889)

[4. Awareness and Training (AT) 14](#_Toc199515890)

[5. Audit and Accountability (AU) 15](#_Toc199515891)

[6. Security Assessment and Authorization (CA) 19](#_Toc199515892)

[7. Configuration Management (CM) 21](#_Toc199515893)

[8. Contingency Planning (CP) 25](#_Toc199515894)

[9. Identification and Authentication (IA) 28](#_Toc199515895)

[10. Incident Response (IR) 32](#_Toc199515896)

[11. Maintenance (MA) 35](#_Toc199515897)

[12. Media Protection (MP) 37](#_Toc199515898)

[13. Physical and Environmental Protection (PE) 39](#_Toc199515899)

[14. Planning (PL) 43](#_Toc199515900)

[15. Personnel Security (PS) 44](#_Toc199515901)

[16. Risk Assessment (RA) 46](#_Toc199515902)

[17. System and Services Acquisition (SA) 47](#_Toc199515903)

[18. System and Communications Protection (SC) 53](#_Toc199515904)

[19. System and Information Integrity (SI) 60](#_Toc199515905)

[20. Additional Comments 65](#_Toc199515906)

# 

# Evaluation Logistics

Table . Evaluation Logistics

|  |  |
| --- | --- |
| Official System Name | Official System Name |
| System Acronym | ABCD |
| Document Name |  |
| Document Version / Date |  |
| Assessment Date(s) | Jan 1 – 3, 2025 |

Table . Evaluator(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| M&O Assessor |  | Assessment Team |  |  |

# General Requirements

Table . General Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Index | Assessment Check | Status  (Met, Partial, Not Met, or N/A) | Comments |
|  | Is the SSP using the most recent version of the ACT SSP template? |  |  |
|  | If a government or military system, is the System Security Plan’s classification or sensitivity clearly marked? |  |  |
|  | Does the SSP have a Review Log and has it been maintained? |  |  |
|  | Provided the system name, acronym, and system of records (SOR) number (if applicable).  (Section 2.3/System Identification and Security Level) |  |  |
|  | Categorized the system as one of the following:   * Major Application (MA) * General Support System (GSS) * Cloud Service Provider (CSP) * Single-User Standalone System (SUSA) * Multi-User Standalone System (MUSA) * Closed Restricted Network (Local Area Network (LAN)) * Wide Area Network (WAN) * Interconnected System – Contractor-to-Contractor (C2C) * Interconnected System – Contractor-to-Government (C2G) * <Other System Type>   (Section 2.4/System Type Designation and Categorization/Classification) |  |  |
|  | Provided the name of the *internal* organization responsible for the system, to include the name of the organization, the address, the contract number and the contract name.  (Section 2.8/Responsible Parties) |  |  |
|  | Provided the name of the *external* organization responsible for the system (if applicable), to include:   * Organization Name * Address * Contract number * Contractor contact information   (Front Matter and Section 2.8/Responsible Parties) |  |  |
|  | Provided the person(s) designated to be the point(s) of contact for the system including the business owner, system developer/maintainer, SSP author, and contractor contact information (if applicable). Information to be provided for each:   * Name * Title * Organization * Address * Mail stop * City, State, Zip * E-mail * Telephone number * Contractor contact information   (Section 2.8/Responsible Parties) |  |  |
|  | Listed the person(s) designated to be responsible for the security of the system and the component ISSO. Information to be provided for each includes:   * Name * Title * Organization * Address * Mail stop * City, State, Zip * E-mail * Telephone number * Emergency contact information (daytime)   (Section 2.8/Responsible Parties) |  |  |
|  | Has the operational status been identified as New, Operational, or Undergoing a Major Modification?  (Section 2.5/System Operational Status) |  |  |
|  | Has a description of the purpose of the system been provided? It may include (but not be limited to):   * Business functions description * Supporting processes and resources * Reason system is still in use * Information flows or information processed by the system * Internal or external organizations that comprise the user community   (Section 2.1/System Background and Purpose) |  |  |
|  | Has a description of the operational/system environment and any special considerations been provided? This may include (but not be limited to):   * Communications requirements * User-interface expectations * Network connectivity requirements   (Section 2.2/System Description) |  |  |
|  | Does the system description include:   * General description of the technical aspects * Use of PDAs or wireless technology (if applicable)   (Section 2.2/System Description) |  |  |
|  | Does the system environment description include:   * Functions of the system * Deployment architecture and the technologies supporting the architecture * Other systems and technologies the system interfaces with * Deployment environment * Types of users interacting with the system * Critical processing periods * System access methods   (Section 2.2/System Description) |  |  |
|  | Is the architecture and topology information provided, or if included in another plan is the name of the other plan provided?  (Section 2.6/Authorization Boundary Diagram and System Description) |  |  |
|  | Is a detailed description of the system boundary and technical components provided?  (Section 2.6/Authorization Boundary Diagram and System Description) |  |  |
|  | Is a detailed description of the primary platforms and systems components including server names vendors and version and security software protecting the system and information provided?  (Section 2.7/Authorization Boundary Details) |  |  |
|  | Are all interconnectivity interfaces, web portals and distributed and collaborative computing environments included? Included should be:   * Connectivity between system modules * For any system that allows individual web-based access (Internet, Intranet, Extranet) include: * URLs for web-based transactions * All authentication products * Electronic logons per year * Number of registered G2G, G2B, G2C and internal users (if applicable)   (Section 2.7/Authorization Boundary Details) |  |  |
|  | Described any special security concerns related to system interconnection or information sharing (e.g. Internet connection).  (Section 2.7/Authorization Boundary Details) |  |  |
|  | Provided names, unique identifiers and the owner organization for all systems to which the system under review is connected or with which it shares information.  (Section 2.7/Authorization Boundary Details) |  |  |
|  | Described system interconnection and information sharing with other systems including a Memorandum of Understanding or Agreement (MOU/MOA) for each interface. (include the Internet/Intranet and all interfacing systems)  (Section 2.7/Authorization Boundary Details) |  |  |
|  | Is the system security level provided including all information types?  (Section 2.3/System Identification and Security Level) |  |  |
|  | Listed laws, regulations, and policies affecting the system.  (Section 2.10/Applicable Laws, Regulations, and Standards) |  |  |
|  | Have system specific rules of behavior (ROB) been documented? Include specific rules for individual user types.  (Section 2.9/Rules of Behavior) |  |  |
|  | Have any security control reviews been completed? Provide details including a description of the type of security control review (i.e., OIG audit, self-assessment, etc.) conducted for the system in the last three years.  (Section 3/Security Controls Detail and Comment) |  |  |

# Access Control (AC)

Table . Access Control (AC) Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | AC-01 Access Control Policy And Procedures |  | L | M | H |  |
|  | AC-02 Account Management |  | L | M | H |  |
|  | AC-02 (01) Automated Information System Account Management |  |  | M | H |  |
|  | AC-02 (02) Removal of Temporary / Emergency Accounts |  |  | M | H |  |
|  | AC-02 (03) Disable Inactive Accounts |  |  | M | H |  |
|  | AC-02 (04) Automated Audit Actions |  |  | M | H |  |
|  | AC-02 (05) Inactivity Logout |  |  |  | H |  |
|  | AC-02 (06) Dynamic Privilege Management |  |  |  |  |  |
|  | AC-02 (07) Role-Based Schemes |  |  |  |  |  |
|  | AC-02 (08) Dynamic Account Creation |  |  |  |  |  |
|  | AC-02 (09) Restrictions On Use Of Shared / Group Accounts |  |  |  |  |  |
|  | AC-02 (10) Shared / Group Account Credential Termination |  |  |  |  |  |
|  | AC-02 (11) Usage Conditions |  |  |  | H |  |
|  | AC-02 (12) Account Monitoring / Atypical Usage |  |  |  | H |  |
|  | AC-02 (13) Disable Accounts For High-Risk Individuals |  |  |  | H |  |
|  | AC-03 Access Enforcement |  | L | M | H |  |
|  | AC-03 (02) Dual Authorization |  |  |  |  |  |
|  | AC-03 (03) Mandatory Access Control |  |  |  |  |  |
|  | AC-03 (04) Discretionary Access Control |  |  |  |  |  |
|  | AC-03 (05) Security-Relevant Information |  |  |  |  |  |
|  | AC-03 (07) Role-Based Access Control |  |  |  |  |  |
|  | AC-03 (08) Revocation Of Access Authorizations |  |  |  |  |  |
|  | AC-03 (09) Controlled Release |  |  |  |  |  |
|  | AC-03 (10) Audited Override Of Access Control Mechanisms |  |  |  |  |  |
|  | AC-04 Information Flow Enforcement |  |  | M | H |  |
|  | AC-04 (01) Object Security Attributes |  |  |  |  |  |
|  | AC-04 (02) Processing Domains |  |  |  |  |  |
|  | AC-04 (03) Dynamic Information Flow Control |  |  |  |  |  |
|  | AC-04 (04) Content Check Encrypted Information |  |  |  |  |  |
|  | AC-04 (05) Embedded Data Types |  |  |  |  |  |
|  | AC-04 (06) Metadata |  |  |  |  |  |
|  | AC-04 (07) One-Way Flow Mechanisms |  |  |  |  |  |
|  | AC-04 (08) Security Policy Filters |  |  |  |  |  |
|  | AC-04 (09) Human Reviews |  |  |  |  |  |
|  | AC-04 (10) Enable / Disable Security Policy Filters |  |  |  |  |  |
|  | AC-04 (11) Configuration Of Security Policy Filters |  |  |  |  |  |
|  | AC-04 (12) Data Type Identifiers |  |  |  |  |  |
|  | AC-04 (13) Decomposition Into Policy-Relevant Subcomponents |  |  |  |  |  |
|  | AC-04 (14) Security Policy Filter Constraints |  |  |  |  |  |
|  | AC-04 (15) Detection Of Unsanctioned Information |  |  |  |  |  |
|  | AC-04 (17) Domain Authentication |  |  |  |  |  |
|  | AC-04 (18) Security Attribute Binding |  |  |  |  |  |
|  | AC-04 (19) Validation Of Metadata |  |  |  |  |  |
|  | AC-04 (20) Approved Solutions |  |  |  |  |  |
|  | AC-04 (21) Physical / Logical Separation Of Information Flows |  |  |  |  |  |
|  | AC-04 (22) Access Only |  |  |  |  |  |
|  | AC-05 Separation Of Duties |  |  | M | H |  |
|  | AC-06 Least Privilege |  |  | M | H |  |
|  | AC-06 (01) Authorize Access To Security Functions |  |  | M | H |  |
|  | AC-06 (02) Non-Privileged Access For Nonsecurity Functions |  |  | M | H |  |
|  | AC-06 (03) Network Access To Privileged Commands |  |  |  | H |  |
|  | AC-06 (04) Separate Processing Domains |  |  |  |  |  |
|  | AC-06 (05) Privileged Accounts |  |  | M | H |  |
|  | AC-06 (06) Privileged Access By Non-Organizational Users |  |  |  |  |  |
|  | AC-06 (07) Review Of User Privileges |  |  |  |  |  |
|  | AC-06 (08) Privilege Levels For Code Execution |  |  |  |  |  |
|  | AC-06 (09) Auditing Use Of Privileged Functions |  |  | M | H |  |
|  | AC-06 (10) Prohibit Non-Privileged Users From Executing Privileged Functions |  |  | M | H |  |
|  | AC-07 Unsuccessful Logon Attempts |  | L | M | H |  |
|  | AC-07 (02) Purge / Wipe Mobile Device |  |  |  |  |  |
|  | AC-08 System Use Notification |  | L | M | H |  |
|  | AC-09 Previous Logon (Access) Notification |  |  |  |  |  |
|  | AC-09 (01) Unsuccessful Logons |  |  |  |  |  |
|  | AC-09 (02) Successful / Unsuccessful Logons |  |  |  |  |  |
|  | AC-09 (03) Notification Of Account Changes |  |  |  |  |  |
|  | AC-09 (04) Additional Logon Information |  |  |  |  |  |
|  | AC-10 Concurrent Session Control |  |  |  | H |  |
|  | AC-11 Session Lock |  |  | M | H |  |
|  | AC-11(01) Pattern Hiding Displays |  |  | M | H |  |
|  | AC-12 Session Termination |  |  |  |  |  |
|  | AC-12 (01) User-Initiated Logouts / Message Displays |  |  |  |  |  |
|  | AC-14 Permitted Actions Without Identification Or Authentication |  | L | M | H |  |
|  | AC-16 Security Attributes |  |  |  |  |  |
|  | AC-16 (01) Dynamic Attribute Association |  |  |  |  |  |
|  | AC-16 (02) Attribute Value Changes By Authorized Individuals |  |  |  |  |  |
|  | AC-16 (03) Maintenance Of Attribute Associations By Information System |  |  |  |  |  |
|  | AC-16 (04) Association Of Attributes By Authorized Individuals |  |  |  |  |  |
|  | AC-16 (05) Attribute Displays For Output Devices |  |  |  |  |  |
|  | AC-16 (06) Maintenance Of Attribute Association By Organization |  |  |  |  |  |
|  | AC-16 (07) Consistent Attribute Interpretation |  |  |  |  |  |
|  | AC-16 (08) Association Techniques / Technologies |  |  |  |  |  |
|  | AC-16 (09) Attribute Reassignment |  |  |  |  |  |
|  | AC-16 (10) Attribute Configuration By Authorized Individuals |  |  |  |  |  |
|  | AC-17 Remote Access |  | L | M | H |  |
|  | AC-17 (01) Automated Monitoring Control |  |  | M | H |  |
|  | AC-17 (02) Protection Of Confidentiality/Integrity Using Encryption |  |  | M | H |  |
|  | AC-17 (03) Managed Access Control Points |  |  | M | H |  |
|  | AC-17 (04) Privileged Commands/Access |  |  | M | H |  |
|  | AC-17 (06) Protection Of Information |  |  |  |  |  |
|  | AC-17 (09) Disconnect / Disable Access |  |  |  |  |  |
|  | AC-18 Wireless Access Restrictions |  | L | M | H |  |
|  | AC-18 (01) Authentication And Encryption |  |  | M | H |  |
|  | AC-18 (03) Disable Wireless Networking |  |  |  |  |  |
|  | AC-18 (04) Restrict User Configuration Of Wireless Networking Capabilities |  |  |  | H |  |
|  | AC-18 (05) Antennas / Transmission Power Levels |  |  |  | H |  |
|  | AC-19 Access Control For Mobile Devices |  | L | M | H |  |
|  | AC-19 (04) Restrictions For Classified Information |  |  |  |  |  |
|  | AC-19 (05) Full Device / Container-Based Encryption |  |  | M | H |  |
|  | AC-20 Use Of External Information Systems |  | L | M | H |  |
|  | AC-20 (01) Limits On Authorized Use |  |  | M | H |  |
|  | AC-20 (02) Portable Storage Devices |  |  | M | H |  |
|  | AC-20 (03) Non-Organizationally Owned Systems / Components / Devices |  |  |  |  |  |
|  | AC-20 (04) Network Accessible Storage Devices |  |  |  |  |  |
|  | AC-21 Information Sharing |  | L | M | H |  |
|  | AC-21 (01) Automated Decision Support |  |  |  |  |  |
|  | AC-21 (02) Information Search And Retrieval |  |  |  |  |  |
|  | AC-22 Publicly Accessible Content |  | L | M | H |  |
|  | AC-23 Data Mining Protection |  |  |  |  |  |
|  | AC-24 Access Control Decisions |  |  |  |  |  |
|  | AC-24 (01) Transmit Access Authorization Information |  |  |  |  |  |
|  | AC-24 (02) No User Or Process Identity |  |  |  |  |  |
|  | AC-25 Reference Monitor |  |  |  |  |  |

# Awareness and Training (AT)

Table . Awareness and Training (AT) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | AT-01 Security Awareness And Training Policy And Procedures |  | L | M | H |  |
|  | AT-02 Security Awareness Training |  | L | M | H |  |
|  | AT-02 (01) Practical Exercises |  |  |  |  |  |
|  | AT-02 (02) Insider Threat |  |  | M | H |  |
|  | AT-03 Role-Based Security Training |  | L | M | H |  |
|  | AT-03 (01) Environmental Controls |  |  |  |  |  |
|  | AT-03 (02) Physical Security Controls |  |  |  |  |  |
|  | AT-03 (30) Practical Exercises |  |  |  |  |  |
|  | AT-03 (04) Suspicious Communications And Anomalous System Behavior |  |  |  |  |  |
|  | AT-04 Security Training Records |  | L | M | H |  |

# Audit and Accountability (AU)

Table . Audit and Accountability (AU) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | AU-01 Audit And Accountability Policy And Procedures |  | L | M | H |  |
|  | AU-02 Audit Events |  | L | M | H |  |
|  | AU-02 (03) Reviews And Updates |  |  | M | H |  |
|  | AU-03 Content Of Audit Records |  | L | M | H |  |
|  | AU-03 (01) Additional Audit Information |  |  | M | H |  |
|  | AU-03 (02) Centralized Management Of Planned Audit Record Content |  |  |  | H |  |
|  | AU-04 Audit Storage Capacity |  | L | M | H |  |
|  | AU-05 Response To Audit Processing Failures |  |  |  |  |  |
|  | AU-05 (01) Audit Storage Capacity |  |  |  | H |  |
|  | AU-05 (02) Real-Time Alerts |  |  |  | H |  |
|  | AU-05 (03) Configurable Traffic Volume Thresholds |  |  |  |  |  |
|  | AU-05 (04) Shutdown On Failure |  |  |  |  |  |
|  | AU-06 Audit Review, Analysis, And Reporting |  | L | M | H |  |
|  | AU-06 (01) Process Integration |  |  | M | H |  |
|  | AU-06 (03) Correlate Audit Repositories |  |  | M | H |  |
|  | AU-06 (04) Central Review And Analysis |  |  |  |  |  |
|  | AU-06 (05) Integration/Scanning And Monitoring Capabilities |  |  |  | H |  |
|  | AU-06 (06) Correlation With Physical Monitoring |  |  |  | H |  |
|  | AU-06 (07) Permitted Actions |  |  |  |  |  |
|  | AU-06 (08) Full Text Analysis Of Privileged Commands |  |  |  |  |  |
|  | AU-06 (09) Correlation With Information From Nontechnical Sources |  |  |  |  |  |
|  | AU-06 (10) Audit Level Adjustment |  |  |  |  |  |
|  | AU-07 Audit Reduction And Report Generation |  |  | M | H |  |
|  | AU-07 (01) Automatic Processing |  |  | M | H |  |
|  | AU-07 (02) Automatic Sort And Search |  |  |  |  |  |
|  | AU-08 Time Stamps |  | L | M | H |  |
|  | AU-08 (01) Synchronization With Authoritative Time Source |  |  | M | H |  |
|  | AU-08 (02) Secondary Authoritative Time Source |  |  |  |  |  |
|  | AU-09 Protection Of Audit Information |  | L | M | H |  |
|  | AU-09 (01) Hardware Write-Once Media |  |  |  |  |  |
|  | AU-09 (02) Audit Backup On Separate Physical Systems / Components |  |  |  | H |  |
|  | AU-09 (03) Cryptographic Protection |  |  |  | H |  |
|  | AU-09 (04) Access By Subset Of Privileged Users |  |  | M | H |  |
|  | AU-09 (05) Dual Authorization |  |  |  |  |  |
|  | AU-09 (06) Read Only Access |  |  |  |  |  |
|  | AU-10 Non-Repudiation |  |  |  | H |  |
|  | AU-10 (01) Association Of Identities |  |  |  |  |  |
|  | AU-10 (02) Validate Binding Of Information Producer Identity |  |  |  |  |  |
|  | AU-10 (03) Chain Of Custody |  |  |  |  |  |
|  | AU-10 (04) Validate Binding Of Information Reviewer Identity |  |  |  |  |  |
|  | AU-11 Audit Record Retention |  | L | M | H |  |
|  | AU-11 (01) Long-Term Retrieval Capability |  |  |  |  |  |
|  | AU-12 Audit Generation |  | L | M | H |  |
|  | AU-12 (01) System-Wide / Time-Correlated Audit Trail |  |  |  | H |  |
|  | AU-12 (02) Standardized Formats |  |  |  |  |  |
|  | AU-12 (03) Changes By Authorized Individuals |  |  |  | H |  |
|  | AU-13 Monitoring For Information Disclosure |  |  |  |  |  |
|  | AU-13 (01) Use Of Automated Tools |  |  |  |  |  |
|  | AU-13 (02) Review Of Monitored Sites |  |  |  |  |  |
|  | AU-14 Session Audit |  |  |  |  |  |
|  | AU-14 (01) System Start-Up |  |  |  |  |  |
|  | AU-14 (02) Capture/Record And Log Content |  |  |  |  |  |
|  | AU-14 (03) Remote Viewing / Listening |  |  |  |  |  |
|  | AU-15 Alternate Audit Capability |  |  |  |  |  |
|  | AU-16 Cross-Organizational Auditing |  |  |  |  |  |
|  | AU-16 (01) Identity Preservation |  |  |  |  |  |
|  | AU-16 (02) Sharing Of Audit Information |  |  |  |  |  |

# Security Assessment and Authorization (CA)

Table . Security Assessment and Authorization (CA) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | CA-01 Security Assessment And Authorization Policies And Procedures |  | L | M | H |  |
|  | CA-02 Security Assessments |  | L | M | H |  |
|  | CA-02 (01) Independent Assessor |  |  | M | H |  |
|  | CA-02 (02) Specialized Assessments |  |  |  | H |  |
|  | CA-02 (03) External Organizations |  |  |  |  |  |
|  | CA-03 System Interconnections |  | L | M | H |  |
|  | CA-03 (01) Unclassified National Security System Connections |  |  |  |  |  |
|  | CA-03 (02) Classified National Security System Connections |  |  |  |  |  |
|  | CA-03 (03) Unclassified Non-National Security System Connections |  |  |  |  |  |
|  | CA-03 (04) Connections To Public Networks |  |  |  |  |  |
|  | CA-03 (05) Restriction On External System Connections |  |  | M | H |  |
|  | CA-05 Plan Of Action And Milestones |  | L | M | H |  |
|  | CA-05 (01) Automation Support For Accuracy/Currency |  |  |  |  |  |
|  | CA-06 Security Authorization |  | L | M | H |  |
|  | CA-07 Continuous Monitoring |  | L | M | H |  |
|  | CA-07 (01) Independent Assessment |  |  | M | H |  |
|  | CA-07 (03) Trend Analyses |  |  |  |  |  |
|  | CA-08 Penetration Testing |  |  |  | H |  |
|  | CA-08 (01) Independent Penetration Agent Or Team |  |  |  |  |  |
|  | CA-08 (02) Red Team Exercises |  |  |  |  |  |
|  | CA-09 Internal System Connections |  | L | M | H |  |
|  | CA-09 (01) Security Compliance Checks |  |  |  |  |  |
|  | CA Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Configuration Management (CM)

Table . Configuration Management (CM) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | CM-01 Configuration Management Policy And Procedures |  | L | M | H |  |
|  | CM-02 Baseline Configuration |  | L | M | H |  |
|  | CM-02 (01) Reviews And Updates |  |  | M | H |  |
|  | CM-02 (02) Automation Support For Accuracy / Currency |  |  |  | H |  |
|  | CM-02 (03) Retention Of Previous Configuration |  |  | M | H |  |
|  | CM-02 (06) Development And Test Environments |  |  |  |  |  |
|  | CM-02 (07) Configure Systems, Components, Or Devices For High-Risk Areas |  |  | M | H |  |
|  | CM-03 Configuration Change Control |  |  | M | H |  |
|  | CM-03 (01) Automated Document / Notification / Prohibition Of Changes |  |  |  | H |  |
|  | CM-03 (02) Test / Validate / Document Changes |  |  | M | H |  |
|  | CM-03 (03) Automated Change Implementation |  |  |  |  |  |
|  | CM-03 (04) Security Representative |  |  |  |  |  |
|  | CM-03 (05) Automated Security Response |  |  |  |  |  |
|  | CM-03 (06) Cryptography Management |  |  |  |  |  |
|  | CM-04 Security Impact Analysis |  | L | M | H |  |
|  | CM-04 (01) Separate Test Environment |  |  |  | H |  |
|  | CM-04 (02) Verification Of Security Functions |  |  | M | H |  |
|  | CM-05 Access Restrictions For Change |  |  | M | H |  |
|  | CM-05 (01) Automated Access Enforcement / Auditing |  |  |  | H |  |
|  | CM-05 (02) Review System Changes |  |  |  | H |  |
|  | CM-05 (03) Signed Components |  |  |  | H |  |
|  | CM-05 (04) Dual Authorization |  |  |  |  |  |
|  | CM-05 (05) Limit Production/Operational Privileges |  |  |  |  |  |
|  | CM-05 (06) Limit Library Privileges |  |  |  |  |  |
|  | CM-06 Configuration Settings |  | L | M | H |  |
|  | CM-06 (01) Automated Central Management / Application / Verification |  |  |  | H |  |
|  | CM-06 (02) Respond To Unauthorized Changes |  |  |  | H |  |
|  | CM-07 Least Functionality |  | L | M | H |  |
|  | CM-07 (01) Periodic Review |  |  | M | H |  |
|  | CM-07 (02) Prevent Program Execution |  |  | M | H |  |
|  | CM-07 (03) Registration Compliance |  |  |  |  |  |
|  | CM-07 (04) Unauthorized Software/Backlisting |  |  | M |  |  |
|  | CM-07 (05) Authorized Software / Whitelisting |  |  |  | H |  |
|  | CM-08 Information System Component Inventory |  | L | M | H |  |
|  | CM-08 (01) Updates During Installations/Removals |  |  | M | H |  |
|  | CM-08 (02) Automated Maintenance |  |  |  | H |  |
|  | CM-08 (03) Automated Unauthorized Component Detection |  |  | M | H |  |
|  | CM-08 (04) Accountability Information |  |  |  | H |  |
|  | CM-08 (05) No Duplicate Accounting Of Components |  |  | M | H |  |
|  | CM-08 (06) Assessed Configurations / Approved Deviations |  |  |  |  |  |
|  | CM-08 (07) Centralized Repository |  |  |  |  |  |
|  | CM-08 (08) Automated Location Tracking |  |  |  |  |  |
|  | CM-08 (09) Assignment Of Components To Systems |  |  |  |  |  |
|  | CM-09 Configuration Management Plan |  |  | M | H |  |
|  | CM-09 (01) Assignment Of Responsibility |  |  |  |  |  |
|  | CM-10 Software Usage Restrictions |  | L | M | H |  |
|  | CM-10 (01) Open-Source Software |  |  |  |  |  |
|  | CM-11 User-Installed Software |  | L | M | H |  |
|  | CM-11 (01) Alerts For Unauthorized Installations |  |  |  |  |  |
|  | CM-11 (02) Prohibit Installation Without Privileged Status |  |  |  |  |  |
|  | CM Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Contingency Planning (CP)

Table . Contingency Planning (CP) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | CP-01 Contingency Planning Policy And Procedures |  | L | M | H |  |
|  | CP-02 Contingency Plan |  | L | M | H |  |
|  | CP-02 (01) Coordinate With Related Plans |  |  | M | H |  |
|  | CP-02 (02) Capacity Planning |  |  |  | H |  |
|  | CP-02 (03) Resume Essential Missions/Business Functions |  |  | M | H |  |
|  | CP-02(04) Resume All Missions/Business Functions |  |  |  | H |  |
|  | CP-02 (05) Continue Essential Mission/Business Functions |  |  |  | H |  |
|  | CP-02 (06) Alternate Processing / Storage Site |  |  |  |  |  |
|  | CP-02 (07) Coordinate With External Service Providers |  |  |  |  |  |
|  | CP-02 (08) Identify Critical Assets |  |  | M | H |  |
|  | CP-03 Contingency Training |  | L | M | H |  |
|  | CP-03 (01) Simulated Events |  |  |  | H |  |
|  | CP-03 (02) Automated Training Environments |  |  |  |  |  |
|  | CP-04 Contingency Plan Testing |  | L | M | H |  |
|  | CP-04 (01) Coordinate With Related Plans |  |  | M | H |  |
|  | CP-04 (02) Alternate Processing Site |  |  |  | H |  |
|  | CP-04 (03) Automated Testing |  |  |  |  |  |
|  | CP-04 (04) Full Recovery & Reconstitution |  |  |  |  |  |
|  | CP-06 Alternate Storage Site |  |  | M | H |  |
|  | CP-06 (01) Separation From Primary Site |  |  | M | H |  |
|  | CP-06 (02) Recovery Time/Point Objectives |  |  |  | H |  |
|  | CP-06 (03) Accessibility |  |  | M | H |  |
|  | CP-07 Alternate Processing Site |  |  | M | H |  |
|  | CP-07 (01) Separation From Primary Site |  |  | M | H |  |
|  | CP-07 (02) Accessibility |  |  | M | J |  |
|  | CP-07 (03) Priority Of Service |  |  | M | H |  |
|  | CP-07 (04) Preparation For Use |  |  |  | H |  |
|  | CP-07 (06) Inability To Return To Primary Site |  |  |  |  |  |
|  | CP-08 Telecommunications Services |  |  | M | H |  |
|  | CP-08 (01) Priority Of Service Provisions |  |  | M | H |  |
|  | CP-08 (02) Single Points Of Failure |  |  | M | H |  |
|  | CP-08 (03) Separation Of Primary / Alternative Providers |  |  |  | H |  |
|  | CP-08 (04) Provider Contingency Plan |  |  |  | H |  |
|  | CP-08 (05) Alternate Telecommunication Service Testing |  |  |  |  |  |
|  | CP-09 Information System Backup |  | L | M | H |  |
|  | CP-09 (01) Testing For Reliability/Integrity |  |  | M | H |  |
|  | CP-09 (02) Test Restoration Using Sampling |  |  |  | H |  |
|  | CP-09 (03) Separate Storage For Critical Information |  |  |  | H |  |
|  | CP-09 (05) Transfer To Alternate Site |  |  |  | H |  |
|  | CP-09 (06) Redundant Secondary System |  |  |  |  |  |
|  | CP-09 (07) Dual Authorization |  |  |  |  |  |
|  | CP-10 Information System Recovery And Reconstitution |  | L | M | H |  |
|  | CP-10 (02) Transaction Recovery |  |  | M | H |  |
|  | CP-10 (04) Restore Within Time Period |  |  |  | H |  |
|  | CP-10 (06) Component Protection |  |  |  |  |  |
|  | CP-11 Alternate Communications Protocols |  |  |  |  |  |
|  | CP-13 Alternative Security Mechanisms |  |  |  |  |  |
|  | CP Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Identification and Authentication (IA)

Table . Identification and Authentication (IA) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | IA-01 Identification And Authentication Policy And Procedures |  | L | M | H |  |
|  | IA-02 Identification And Authentication (Organizational Users) |  | L | M | H |  |
|  | IA-02 (01) Network Access To Privileged Accounts |  | L | M | H |  |
|  | IA-02 (02) Network Access To Non-Privileged Accounts |  |  | M | H |  |
|  | IA-02 (03) Local Access To Privileged Accounts |  |  | M | H |  |
|  | IA-02 (04) Local Access To Non-Privileged Accounts |  |  |  | H |  |
|  | IA-02 (05) Group Authentication |  |  |  |  |  |
|  | IA-02 (06) Network Access To Privileged Accounts - Separate Device |  |  |  |  |  |
|  | IA-02 (07) Network Access To Non-Privileged Accounts - Separate Device |  |  |  |  |  |
|  | IA-02 (08) Network Access To Privileged Accounts – Replay Resistant |  |  | M | H |  |
|  | IA-02 (09) Network Access To Non-Privileged Accounts |  |  |  | H |  |
|  | IA-02 (10) Single Sign-On |  |  |  |  |  |
|  | IA-02 (11) Remote Access – Separate Device |  |  | M | H |  |
|  | IA-02 (12) Acceptance Of PIV Credentials |  | L | M | H |  |
|  | IA-02 (13) Out-Of-Band Authentication |  |  |  |  |  |
|  | IA-03 Device Identification And Authentication |  |  | M | H |  |
|  | IA-03 (01) Cryptographic Bidirectional Authentication |  |  |  |  |  |
|  | IA-03 (03) Dynamic Address Allocation |  |  |  |  |  |
|  | IA-03 (04) Device Attestation |  |  |  |  |  |
|  | IA-04 Identifier Management |  | L | M | H |  |
|  | IA-04 (01) Prohibit Account Identifiers As Public Identifiers |  |  |  |  |  |
|  | IA-04 (02) Supervisor Authorization |  |  |  |  |  |
|  | IA-04 (03) Multiple Forms Of Certification |  |  |  |  |  |
|  | IA-04 (04) Identify User Status |  |  |  |  |  |
|  | IA-04 (05) Dynamic Management |  |  |  |  |  |
|  | IA-04 (06) Cross-Organization Management |  |  |  |  |  |
|  | IA-04 (07) In-Person Registration |  |  |  |  |  |
|  | IA-05 Authenticator Management |  | L | M | H |  |
|  | IA-05 (01) Password-Based Authentication |  | L | M | H |  |
|  | IA-05 (02) PKI-Based Authentication |  |  | M | H |  |
|  | IA-05 (03) In-Person Or Trusted Third-Party Registration |  |  | M | H |  |
|  | IA-05 (04) Automated Support For Password Strength Determination |  |  |  |  |  |
|  | IA-05 (05) Change Authenticators Prior To Delivery |  |  |  |  |  |
|  | IA-05 (06) Protection Of Authenticators |  |  |  |  |  |
|  | IA-05 (07) No Embedded Unencrypted Static Authenticators |  |  |  |  |  |
|  | IA-05 (08) Multiple Information System Accounts |  |  |  |  |  |
|  | IA-05 (09) Cross-Organization Credential Management |  |  |  |  |  |
|  | IA-05 (10) Dynamic Credential Association |  |  |  |  |  |
|  | IA-05(11) Hardware Token-Based Authentication |  | L | M | H |  |
|  | IA-05 (12) Biometric-Based Authentication |  |  |  |  |  |
|  | IA-05 (13) Expiration Of Cached Authenticators |  |  |  |  |  |
|  | IA-05 (14) Managing Content Of PKI Trust Stores |  |  |  |  |  |
|  | IA-05 (15) FICAM-Approved Products And Services |  |  |  |  |  |
|  | IA-06 Authenticator Feedback |  | L | M | H |  |
|  | IA-07 Cryptographic Module Authentication |  | L | M | H |  |
|  | IA-08 Identification And Authentication (Non-Organizational Users) |  | L | M | H |  |
|  | IA-08 (01) Acceptance Of PIV Credentials From Other Agencies |  | L | M | H |  |
|  | IA-08 (02) Acceptance Of Third-Party Credentials |  | L | M | H |  |
|  | IA-08 (03) Use Of FICAM-Approved Products |  | L | M | H |  |
|  | IA-08 (04) Use Of FICAM-Issued Profiles |  | L | M | H |  |
|  | IA-08 (05) Acceptance Of PIV-I Credentials |  |  |  |  |  |
|  | IA-09 Service Identification And Authentication |  |  |  |  |  |
|  | IA-09 (01) Information Exchange |  |  |  |  |  |
|  | IA-09 (02) Transmission Of Decisions |  |  |  |  |  |
|  | IA-10 Adaptive Identification And Authentication |  |  |  |  |  |
|  | IA-11 Re-Authentication |  |  |  |  |  |
|  | IA Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Incident Response (IR)

Table . Incident Response (IR) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | IR-01 Incident Response Policy And Procedures |  | L | M | H |  |
|  | IR-02 Incident Response Training |  | L | M | H |  |
|  | IR-02 (01) Simulated Events |  |  |  | H |  |
|  | IR-02 (02) Automated Training Environment |  |  |  | H |  |
|  | IR-03 Incident Response Testing |  |  | M | H |  |
|  | IR-03 (01) Automated Testing |  |  |  |  |  |
|  | IR-03 (02) Coordination With Related Plans |  |  | M | H |  |
|  | IR-04 Incident Handling |  | L | M | H |  |
|  | IR-04 (01) Automated Incident Handling Process |  |  | M | H |  |
|  | IR-04 (02) Dynamic Reconfiguration |  |  |  |  |  |
|  | IR-04 (03) Continuity Of Operations |  |  |  |  |  |
|  | IR-04 (04) Information Correlation |  |  |  | H |  |
|  | IR-04 (05) Automatic Disabling Of Information System |  |  |  |  |  |
|  | IR-04 (06) Insider Threats - Specific Capabilities |  |  |  |  |  |
|  | IR-04 (07) Insider Threats - Intra-Organization Coordination |  |  |  |  |  |
|  | IR-04 (08) Correlation With External Organizations |  |  |  |  |  |
|  | IR-04 (09) Dynamic Response Capability |  |  |  |  |  |
|  | IR-04 (10) Supply Chain Coordination |  |  |  |  |  |
|  | IR-05 Incident Monitoring |  | L | M | H |  |
|  | IR-05 (01) Automated Tracking/Data Collection / Analysis |  |  |  | H |  |
|  | IR-06 Incident Reporting |  | L | M | H |  |
|  | IR-06 (01) Automated Reporting |  |  | M | H |  |
|  | IR-06 (02) Vulnerabilities Related To Incidents |  |  |  |  |  |
|  | IR-06 (03) Coordination With Supply Chain |  |  |  |  |  |
|  | IR-07 Incident Response Assistance |  | L | M | H |  |
|  | IR-07 (01) Automation Support For Availability Of Information Support |  |  | M | H |  |
|  | IR-07 (02) Coordination With External Providers |  |  |  |  |  |
|  | IR-08 Incident Response Plan |  | L | M | H |  |
|  | IR-09 Information Spillage Response |  |  |  |  |  |
|  | IR-09 (01) Responsible Personnel |  |  |  |  |  |
|  | IR-09 (02) Training |  |  |  |  |  |
|  | IR-09 (03) Post-Spill Operations |  |  |  |  |  |
|  | IR-09 (04) Exposure To Unauthorized Personnel |  |  |  |  |  |
|  | IR-10 Integrated Information Security Analysis Team |  |  |  |  |  |
|  | IR Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Maintenance (MA)

Table . Family Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | MA-01 System Maintenance Policy And Procedures |  | L | M | H |  |
|  | MA-02 Controlled Maintenance |  | L | M | H |  |
|  | MA-02 (02) Automated Maintenance Activities |  |  |  | H |  |
|  | MA-03 Maintenance Tools |  |  | M | H |  |
|  | MA-03 (01) Inspect Tools |  |  | M | H |  |
|  | MA-03 (02) Inspect Media |  |  | M | H |  |
|  | MA-03 (03) Prevent Unauthorized Removal |  |  |  | H |  |
|  | MA-03 (04) Restricted Tool Use |  |  |  |  |  |
|  | MA-04 Nonlocal Maintenance |  | L | M | H |  |
|  | MA-04 (01) Auditing And Review |  |  |  |  |  |
|  | MA-04 (02) Document Nonlocal Maintenance |  |  | M | H |  |
|  | MA-04 (03) Comparable Security/Sanitization |  |  |  | H |  |
|  | MA-04 (04) Authentication / Separation Of Maintenance Sessions |  |  |  |  |  |
|  | MA-04 (05) Approvals And Notifications |  |  |  |  |  |
|  | MA-04 (06) Cryptographic Protection |  |  |  |  |  |
|  | MA-04 (07) Remote Disconnect Verification |  |  |  |  |  |
|  | MA-05 Maintenance Personnel |  | L | M | H |  |
|  | MA-05(01) Individuals Without Appropriate Access |  |  |  | H |  |
|  | MA-05 (02) Security Clearances For Classified Systems |  |  |  |  |  |
|  | MA-05 (03) Citizenship Requirements For Classified Systems |  |  |  |  |  |
|  | MA-05 (04) Foreign Nationals |  |  |  |  |  |
|  | MA-05 (05) Nonsystem-Related Maintenance |  |  |  |  |  |
|  | MA-06 Timely Maintenance |  |  | M | H |  |
|  | MA-06 (01) Preventive Maintenance |  |  |  |  |  |
|  | MA-06 (02) Predictive Maintenance |  |  |  |  |  |
|  | MA-06 (03) Automated Support For Predictive Maintenance |  |  |  |  |  |
|  | MA Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Media Protection (MP)

Table . Media Protection (MP) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | MP-01 Media Protection Policy And Procedures |  | L | M | H |  |
|  | MP-02 Media Access |  | L | M | H |  |
|  | MP-03 Media Marking |  |  | M | H |  |
|  | MP-04 Media Storage |  |  | M | H |  |
|  | MP-04 (02) Automated Restricted Access |  |  |  |  |  |
|  | MP-05 Media Transport |  |  | M | H |  |
|  | MP-05 (03) Custodians |  |  |  |  |  |
|  | MP-05 (04) Cryptographic Protection |  |  | M | H |  |
|  | MP-06 Media Sanitization |  | L | M | H |  |
|  | MP-06 (01) Review / Approve / Track / Document / Verify |  |  |  | H |  |
|  | MP-06 (02) Equipment Testing |  |  |  | H |  |
|  | MP-06 (03) Nondestructive Techniques |  |  |  | H |  |
|  | MP-06 (07) Dual Authorization |  |  |  |  |  |
|  | MP-06 (08) Remote Purging / Wiping Of Information |  |  |  |  |  |
|  | MP-07 Media Use |  | L | M | H |  |
|  | MP-07 (01) Prohibit Use Without Owner |  |  | M | H |  |
|  | MP-07 (02) Prohibit Use Of Sanitization-Resistant Media |  |  |  |  |  |
|  | MP-08 Media Downgrading |  |  |  |  |  |
|  | MP-08 (01) Documentation Of Process |  |  |  |  |  |
|  | MP-08 (02) Equipment Testing |  |  |  |  |  |
|  | MP-08 (03) Controlled Unclassified Information |  |  |  |  |  |
|  | MP-08 (04) Classified Information |  |  |  |  |  |
|  | MP Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Physical and Environmental Protection (PE)

Table . Physical and Environmental Protection (PE) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | PE-01 Physical And Environmental Protection Policy And Procedures |  | L | M | H |  |
|  | PE-02 Physical Access Authorizations |  | L | M | H |  |
|  | PE-02 (01) Access By Position / Role |  |  |  |  |  |
|  | PE-02 (02) Two Forms Of Identification |  |  |  |  |  |
|  | PE-02 (03) Restrict Unescorted Access |  |  |  |  |  |
|  | PE-03 Physical Access Control |  | L | M | H |  |
|  | PE-03 (01) Information System Access |  |  |  | H |  |
|  | PE-03 (02) Facility / Information System Boundaries |  |  |  |  |  |
|  | PE-03 (03) Continuous Guards / Alarms / Monitoring |  |  |  |  |  |
|  | PE-03 (04) Lockable Casings |  |  |  |  |  |
|  | PE-03 (05) Tamper Protection |  |  |  |  |  |
|  | PE-03 (06) Facility Penetration Testing |  |  |  |  |  |
|  | PE-04 Access Control For Transmission Medium |  |  | M | H |  |
|  | PE-05 Access Control For Output Devices |  |  | M | H |  |
|  | PE-05 (01) Access To Output By Authorized Individuals |  |  |  |  |  |
|  | PE-05 (02) Access To Output By Individual Identity |  |  |  |  |  |
|  | PE-05 (03) Marking Output Devices |  |  |  |  |  |
|  | PE-06 Monitoring Physical Access |  | L | M | H |  |
|  | PE-06 (01) Intrusion Alarms/Surveillance Equipment |  |  | M | H |  |
|  | PE-06 (02) Automated Intrusion Recognition / Responses |  |  |  |  |  |
|  | PE-06 (03) Video Surveillance |  |  |  |  |  |
|  | PE-06 (04) Monitoring Physical Access To Information Systems |  |  |  | H |  |
|  | PE-08 Visitor Access Records |  | L | M | H |  |
|  | PE-08 (01) Automated Record Maintenance/Review |  |  |  | H |  |
|  | PE-09 Power Equipment And Cabling |  |  | M | H |  |
|  | PE-09 (01) Redundant Cabling |  |  |  |  |  |
|  | PE-09 (02) Automatic Voltage Controls |  |  |  |  |  |
|  | PE-10 Emergency Shutoff |  |  | M | H |  |
|  | PE-11 Emergency Power |  |  | M | H |  |
|  | PE-11 (01) Long-Term Alternate Power Supply-Minimal Operational Capability |  |  |  | H |  |
|  | PE-11 (02) Long-Term Alternate Power Supply - Self-Contained |  |  |  |  |  |
|  | PE-12 Emergency Lighting |  | L | M | H |  |
|  | PE-12 (01) Essential Missions / Business Functions |  |  |  |  |  |
|  | PE-13 Fire Protection |  | L | M | H |  |
|  | PE-13 (01) Detection Devices / Systems |  |  |  | H |  |
|  | PE-13 (02) Suppression Devices / Systems |  |  |  | H |  |
|  | PE-13 (03) Automatic Fire Suppression |  |  | M | H |  |
|  | PE-13 (04) Inspections |  |  |  |  |  |
|  | PE-14 Temperature And Humidity Controls |  | L | M | H |  |
|  | PE-14 (01) Automatic Controls |  |  |  |  |  |
|  | PE-14 (02) Monitoring With Alarms / Notifications |  |  |  |  |  |
|  | PE-15 Water Damage Protection |  | L | M | H |  |
|  | PE-15 (01) Automation Support |  |  |  | H |  |
|  | PE-16 Delivery And Removal |  | L | M | H |  |
|  | PE-17 Alternate Work Site |  |  | M | H |  |
|  | PE-18 Location Of Information System Components |  |  |  | H |  |
|  | PE-18 (01) Facility Site |  |  |  |  |  |
|  | PE-19 Information Leakage |  |  |  |  |  |
|  | PE-19 (01) National Emissions / Tempest Policies And Procedures |  |  |  |  |  |
|  | PE-20 Asset Monitoring And Tracking |  |  |  |  |  |
|  | PE Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Planning (PL)

Table . Planning (PL) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | PL-01 Security Planning Policy And Procedures |  | L | M | H |  |
|  | PL-02 System Security Plan |  | L | M | H |  |
|  | PL-02 (03) Plan/Coordinate With Other Organizational Entities |  |  | M | H |  |
|  | PL-04 Rules Of Behavior |  | L | M | H |  |
|  | PL-04 (01) Social Media And Networking Restrictions |  |  | M | H |  |
|  | PL-07 Security Concept Of Operations |  |  |  |  |  |
|  | PL-08 Information Security Architecture |  |  | M | H |  |
|  | PL-08 (01) Defense-In-Depth |  |  |  |  |  |
|  | PL-08 (02) Supplier Diversity |  |  |  |  |  |
|  | PL-09 Central Management |  |  |  |  |  |
|  | PL Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Personnel Security (PS)

Table . Personnel Security (PS) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | PS-01 Personnel Security Policy And Procedures |  | L | M | H |  |
|  | PS-02 Position Risk Designation |  | L | M | H |  |
|  | PS-03 Personnel Screening |  | L | M | H |  |
|  | PS-03 (01) Classified Information |  |  |  |  |  |
|  | PS-03 (02) Formal Indoctrination |  |  |  |  |  |
|  | PS-03 (03) Information With Special Protection Measures |  |  |  |  |  |
|  | PS-04 Personnel Termination |  | L | M | H |  |
|  | PS-04 (01) Post-Employment Requirements |  |  |  |  |  |
|  | PS-04 (02) Automated Notification |  |  |  | H |  |
|  | PS-05 Personnel Transfer |  | L | M | H |  |
|  | PS-06 Access Agreements |  | L | M | H |  |
|  | PS-06 (02) Classified Information Requiring Special Protection |  |  |  |  |  |
|  | PS-06 (03) Post-Employment Requirements |  |  |  |  |  |
|  | PS-07 Third-Party Personnel Security |  | L | M | H |  |
|  | PS-08 Personnel Sanctions |  | L | M | H |  |
|  | PS Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Risk Assessment (RA)

Table . Risk Assessment (RA) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | RA-01 Risk Assessment Policy And Procedures |  | L | M | H |  |
|  | RA-02 Security Categorization |  | L | M | H |  |
|  | RA-03 Risk Assessment |  | L | M | H |  |
|  | RA-05 Vulnerability Scanning |  | L | M | H |  |
|  | RA-05 (01) Update Tool Capability |  |  | M | H |  |
|  | RA-05 (02) Update By Frequency/Prior To New Scan / When Identified |  |  | M | H |  |
|  | RA-05 (03) Breadth/Depth Of Coverage |  |  |  |  |  |
|  | RA-05 (04) Discoverable Information |  |  |  | H |  |
|  | RA-05 (05) Privileged Access |  |  | M | H |  |
|  | RA-05 (06) – Automated Trend Analyses |  |  |  |  |  |
|  | RA-05 (08) Review Historic Audit Logs |  |  |  |  |  |
|  | RA-05 (10) Correlate Scanning Information |  |  |  |  |  |
|  | RA-06 Technical Surveillance Countermeasures Survey |  |  |  |  |  |
|  | RA Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# System and Services Acquisition (SA)

Table . System and Services Acquisition (SA) Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | SA-01 System And Services Acquisition Policy And Procedures |  | L | M | H |  |
|  | SA-02 Allocation Of Resources |  | L | M | H |  |
|  | SA-03 System Development Life Cycle |  | L | M | H |  |
|  | SA-04 Acquisitions Process |  | L | M | H |  |
|  | SA-04 (01) Functional Properties Of Security Controls |  |  | M | H |  |
|  | SA-04 (02) Design/Implementation Information For Security Controls |  |  | M | H |  |
|  | SA-04 (03) Development Methods / Techniques / Practices |  |  |  |  |  |
|  | SA-04 (05) System / Component / Service Configurations |  |  |  |  |  |
|  | SA-04 (06) Use Of Information Assurance Products |  |  |  |  |  |
|  | SA-04 (07) – NIAP-Approved Protection Profiles |  |  |  |  |  |
|  | SA-04 (08) Continuous Monitoring Plan |  |  |  |  |  |
|  | SA-04 (09) Functions/Ports/Protocols/Services In Use |  |  | M | H |  |
|  | SA-04 (10) Use Of Approved PIV Products |  | L | M | H |  |
|  | SA-05 Information System Documentation |  | L | M | H |  |
|  | SA-08 Security Engineering Principles |  |  | M | H |  |
|  | SA-09 External Information System Services |  | L | M | H |  |
|  | SA-09 (01) – Risk Assessment/Organizational Approvals |  |  |  |  |  |
|  | SA-09 (02) Identification Of Functions / Ports / Protocols / Services |  |  | M | H |  |
|  | SA-09 (03) Establish / Maintain Trust Relationship With Providers |  |  |  |  |  |
|  | SA-09 (04) Consistent Interests Of Consumers And Providers |  |  |  |  |  |
|  | SA-09 (05) Processing, Storage, And Service Location |  |  |  |  |  |
|  | SA-10 Developer Configuration Management |  |  | M | H |  |
|  | SA-10 (01) Software / Firmware Integrity Verification |  |  |  |  |  |
|  | SA-10 (02) Alternative Configuration Management Processes |  |  |  |  |  |
|  | SA-10 (03) Hardware Integrity Verification |  |  |  |  |  |
|  | SA-10 (04) Trusted Generation |  |  |  |  |  |
|  | SA-10 (05) Mapping Integrity For Version Control |  |  |  |  |  |
|  | SA-10 (06) Trusted Distribution |  |  |  |  |  |
|  | SA-11 Developer Security Testing And Evaluation |  |  | M | H |  |
|  | SA-11 (01) Static Code Analysis |  |  |  |  |  |
|  | SA-11 (02) Threat And Vulnerability Analyses |  |  |  |  |  |
|  | SA-11 (03) Independent Verification Of Assessment Plans / Evidence |  |  |  |  |  |
|  | SA-11 (04) Manual Code Reviews |  |  |  |  |  |
|  | SA-11 (05) Penetration Testing |  |  |  |  |  |
|  | SA-11 (06) Attack Surface Reviews |  |  |  |  |  |
|  | SA-11 (07) Verify Scope Of Testing / Evaluation |  |  |  |  |  |
|  | SA-11 (08) Dynamic Code Analysis |  |  |  |  |  |
|  | SA-12 Supply Chain Protection |  |  |  | H |  |
|  | SA-12 (01) Acquisition Strategies / Tools / Methods |  |  |  |  |  |
|  | SA-12 (02) Supplier Reviews |  |  |  |  |  |
|  | SA-12 (05) Limitation Of Harm |  |  |  |  |  |
|  | SA-12 (07) Assessments Prior To Selection / Acceptance / Update |  |  |  |  |  |
|  | SA-12 (08) Use Of All-Source Intelligence |  |  |  |  |  |
|  | SA-12 (09) Operations Security |  |  |  |  |  |
|  | SA-12 (10) Validate As Genuine And Not Altered |  |  |  |  |  |
|  | SA-12 (11) Penetration Testing / Analysis Of Elements, Processes, And Actors |  |  |  |  |  |
|  | SA-12 (12) Inter-Organizational Agreements |  |  |  |  |  |
|  | SA-12 (13) Critical Information System Components |  |  |  |  |  |
|  | SA-12 (14) Identity And Traceability |  |  |  |  |  |
|  | SA-12 (15) Processes To Address Weaknesses Or Deficiencies |  |  |  |  |  |
|  | SA-13 Trustworthiness |  |  |  |  |  |
|  | SA-14 Criticality Analysis |  |  |  |  |  |
|  | SA-15 Development Process, Standards, And Tools |  |  |  | H |  |
|  | SA-15 (01) Quality Metrics |  |  |  |  |  |
|  | SA-15 (02) Security Tracking Tools |  |  |  |  |  |
|  | SA-15 (03) Criticality Analysis |  |  |  |  |  |
|  | SA-15 (04) Threat Modeling / Vulnerability Analysis |  |  |  |  |  |
|  | SA-15 (05) Attack Surface Reduction |  |  |  |  |  |
|  | SA-15 (06) Continuous Improvement |  |  |  |  |  |
|  | SA-15 (07) Automated Vulnerability Analysis |  |  |  |  |  |
|  | SA-15 (08) Reuse Of Threat / Vulnerability Information |  |  |  |  |  |
|  | SA-15 (09) Use Of Live Data |  |  |  |  |  |
|  | SA-15 (10) Incident Response Plan |  |  |  |  |  |
|  | SA-15 (11) Archive Information System / Component |  |  |  |  |  |
|  | SA-16 Developer-Provided Training |  |  |  | H |  |
|  | SA-17 Developer Security Architecture And Design |  |  |  | H |  |
|  | SA-17 (01) Formal Policy Model |  |  |  |  |  |
|  | SA-17 (02) Security-Relevant Components |  |  |  |  |  |
|  | SA-17 (03) Formal Correspondence |  |  |  |  |  |
|  | SA-17 (04) Informal Correspondence |  |  |  |  |  |
|  | SA-17 (05) Conceptually Simple Design |  |  |  |  |  |
|  | SA-17 (06) Structure For Testing |  |  |  |  |  |
|  | SA-17 (07) Structure For Least Privilege |  |  |  |  |  |
|  | SA-18 Tamper Resistance And Detection |  |  |  |  |  |
|  | SA-18 (01) Multiple Phases Of SDLC |  |  |  |  |  |
|  | SA-18 (02) Inspection Of Information Systems, Components, Or Devices |  |  |  |  |  |
|  | SA-19 Component Authenticity |  |  |  |  |  |
|  | SA-19 (01) Anti-Counterfeit Training |  |  |  |  |  |
|  | SA-19 (02) Configuration Control For Component Service / Repair |  |  |  |  |  |
|  | SA-19 (03) Component Disposal |  |  |  |  |  |
|  | SA-19 (04) Anti-Counterfeit Scanning |  |  |  |  |  |
|  | SA-20 Customized Development Of Critical Components |  |  |  |  |  |
|  | SA-21 Developer Screening |  |  |  |  |  |
|  | SA-21 (01) Validation Of Screening |  |  |  |  |  |
|  | SA-22 Unsupported System Components |  |  |  |  |  |
|  | SA-22 (01) Alternative Sources For Continued Support |  |  |  |  |  |
|  | SA Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# System and Communications Protection (SC)

Table . Family Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | SC-01 System And Communications Protection Policy And Procedures |  | L | M | H |  |
|  | SC-02 Application Partitioning |  |  | M | H |  |
|  | SC-02 (01) Interfaces For Non-Privileged Users |  |  |  |  |  |
|  | SC-03 Security Function Isolation |  |  |  | H |  |
|  | SC-03 (01) Hardware Separation |  |  |  |  |  |
|  | SC-03 (02) Access / Flow Control Functions |  |  |  |  |  |
|  | SC-03 (03) Minimize Nonsecurity Functionality |  |  |  |  |  |
|  | SC-03 (04) Module Coupling And Cohesiveness |  |  |  |  |  |
|  | SC-03 (05) Layered Structures |  |  |  |  |  |
|  | SC-04 Information In Shared Resources |  |  | M | H |  |
|  | SC-04 (02) Periods Processing |  |  |  |  |  |
|  | SC-05 Denial Of Service Protection |  | L | M | H |  |
|  | SC-05 (01) Restrict Internal Users |  |  |  |  |  |
|  | SC-05 (02) Excess Capacity / Bandwidth / Redundancy |  |  |  |  |  |
|  | SC-05 (03) Detection / Monitoring |  |  |  |  |  |
|  | SC-06 Resource Availability |  |  |  |  |  |
|  | SC-07 Boundary Protection |  | L | M | H |  |
|  | SC-07 (03) Access Points |  |  | M | H |  |
|  | SC-07 (04) External Telecommunications Services |  |  | M | H |  |
|  | SC-07 (05) Deny By Default/Allow By Exception |  |  | M | H |  |
|  | SC-07 (07) Prevent Split Tunneling For Remote Devices |  |  | M | H |  |
|  | SC-07 (08) Route Traffic To Authenticated Proxy Servers |  |  |  | H |  |
|  | SC-07 (09) Restrict Threatening Outgoing Communications Traffic |  |  |  |  |  |
|  | SC-07 (10) Prevent Unauthorized Exfiltration |  |  |  |  |  |
|  | SC-07 (11) Restrict Incoming Communications Traffic |  |  |  |  |  |
|  | SC-07 (12) Host Based Protection |  |  |  |  |  |
|  | SC-07 (13) – Isolation Of Security Tools/Mechanisms/Support Components |  |  |  |  |  |
|  | SC-07 (14) Protects Against Unauthorized Physical Connections |  |  |  |  |  |
|  | SC-07 (15) Route Privileged Network Accesses |  |  |  |  |  |
|  | SC-07 (16) Prevent Discovery Of Components / Devices |  |  |  |  |  |
|  | SC-07 (17) Automated Enforcement Of Protocol Formats |  |  |  |  |  |
|  | SC-07 (18) –Fail Secure |  |  |  | H |  |
|  | SC-07 (19) Blocks Communication From Non-Organizationally Configured Hosts |  |  |  |  |  |
|  | SC-07 (20) Dynamic Isolation / Segregation |  |  |  |  |  |
|  | SC-07 (21) Isolation Of Information System Components |  |  |  | H |  |
|  | SC-07 (22) Separate Subnets For Connecting To Different Security Domains |  |  |  |  |  |
|  | SC-07 (23) Disable Sender Feedback On Protocol Validation Failure |  |  |  |  |  |
|  | SC-08 Transmission Confidentiality And Integrity |  |  | M | H |  |
|  | SC-08 (01) Cryptographic Or Alternate Physical Protection |  |  | M | H |  |
|  | SC-08 (02) Pre / Post Transmission Handling |  |  |  |  |  |
|  | SC-08 (03) Cryptographic Protection For Message Externals |  |  |  |  |  |
|  | SC-08 (04) Conceal / Randomize Communications |  |  |  |  |  |
|  | SC-10 Network Disconnect |  |  | M | H |  |
|  | SC-11 Trusted Path |  |  |  |  |  |
|  | SC-11 (01) Logical Isolation |  |  |  |  |  |
|  | SC-12 Cryptographic Key Establishment And Management |  | L | M | H |  |
|  | SC-12 (01) Availability |  |  |  | H |  |
|  | SC-12 (02) –Symmetric Keys |  |  |  |  |  |
|  | SC-12 (03) Asymmetric Keys |  |  |  |  |  |
|  | SC-15 Collaborative Computing Devices |  | L | M | H |  |
|  | SC-15 (01) Physical Disconnect |  |  |  |  |  |
|  | SC-15 (03) Disabling / Removal In Secure Work Areas |  |  |  |  |  |
|  | SC-15 (04) Explicitly Indicate Current Participants |  |  |  |  |  |
|  | SC-16 Transmission Of Security Attributes |  |  |  |  |  |
|  | SC-16 (01) Integrity Validation |  |  |  |  |  |
|  | SC-17 Public Key Infrastructure Certificates |  |  | M | H |  |
|  | SC-18 Mobile Code |  |  | M | H |  |
|  | SC-18 (01) Identify Unacceptable Code / Take Corrective Actions |  |  |  |  |  |
|  | SC-18 (02) Acquisition / Development / Use |  |  |  |  |  |
|  | SC-18 (03) Prevent Downloading / Execution |  |  |  |  |  |
|  | SC-18 (04) Prevent Automatic Execution |  |  |  |  |  |
|  | SC-18 (05) Allow Execution Only In Confined Environments |  |  |  |  |  |
|  | SC-19 Voice Over Internet Protocol |  |  | M | H |  |
|  | SC-20 Secure Name /Address Resolution Service (Authoritative Source) |  | L | M | H |  |
|  | SC-20 (02) Data Origin / Integrity |  |  |  |  |  |
|  | SC-21 Secure Name/Address Resolution Service (Recursive Or Caching Resolver) |  | L | M | H |  |
|  | SC-22 Architecture And Provisioning For Name /Address Resolution Service |  | L | M | H |  |
|  | SC-23 Session Authenticity |  |  | M | H |  |
|  | SC-23 (01) Invalidate Session Identifiers At Logout |  |  |  |  |  |
|  | SC-23 (03) Unique Session Identifiers With Randomization |  |  |  |  |  |
|  | SC-23 (05) Allowed Certificate Authorities |  |  |  |  |  |
|  | SC-24 Fail In Known State |  |  |  | H |  |
|  | SC-24 Fail In Known State |  |  |  |  |  |
|  | SC-25 Thin Nodes |  |  |  |  |  |
|  | SC-26 Honeypots |  |  |  |  |  |
|  | SC-27 Platform-Independent Applications |  |  |  |  |  |
|  | SC-28 Protection Of Information At Rest |  |  | M | H |  |
|  | SC-28 (01) Cryptographic Protection |  |  |  |  |  |
|  | SC-28 (02) Off-Line Storage |  |  |  |  |  |
|  | SC-29 Heterogeneity |  |  |  |  |  |
|  | SC-29 (01) Virtualization Techniques |  |  |  |  |  |
|  | SC-30 – Concealment And Misdirection |  |  |  |  |  |
|  | SC-30 (02) Randomness |  |  |  |  |  |
|  | SC-30 (03) Change Processing / Storage Locations |  |  |  |  |  |
|  | SC-30 (04) Misleading Information |  |  |  |  |  |
|  | SC-30 (05) Concealment Of System Components |  |  |  |  |  |
|  | SC-31 Covert Channel Analysis |  |  |  |  |  |
|  | SC-31 (01) Test Covert Channels For Exploitability |  |  |  |  |  |
|  | SC-31 (02) Maximum Bandwidth |  |  |  |  |  |
|  | SC-31 (03) Measure Bandwidth In Operational Environments |  |  |  |  |  |
|  | SC-32 Information System Partitioning |  |  |  |  |  |
|  | SC-34 Non-Modifiable Executable Programs |  |  |  |  |  |
|  | SC-34 (01) No Writable Storage |  |  |  |  |  |
|  | SC-34 (02) Integrity Protection / Read-Only Media |  |  |  |  |  |
|  | SC-34 (03) Hardware-Based Protection |  |  |  |  |  |
|  | SC-35 Honeyclients |  |  |  |  |  |
|  | SC-36 Distributed Processing And Storage |  |  |  |  |  |
|  | SC-36 (01) Polling Techniques |  |  |  |  |  |
|  | SC-37 Out-Of-Band Channels |  |  |  |  |  |
|  | SC-37 (01) Ensure Delivery / Transmission |  |  |  |  |  |
|  | SC-38 Operations Security |  |  |  |  |  |
|  | SC-39 Process Isolation |  | L | M | H |  |
|  | SC-39 (01) Hardware Separation |  |  |  |  |  |
|  | SC-39 (02) Thread Isolation |  |  |  |  |  |
|  | SC-40 Wireless Link Protection |  |  |  |  |  |
|  | SC-40 (01) Electromagnetic Interference |  |  |  |  |  |
|  | SC-40 (02) Reduce Detection Potential |  |  |  |  |  |
|  | SC-40 (03) Imitative Or Manipulative Communications Deception |  |  |  |  |  |
|  | SC-40 (04) Signal Parameter Identification |  |  |  |  |  |
|  | SC-41 Port And I/O Device Access |  |  |  |  |  |
|  | SC-42 Sensor Capability And Data |  |  |  |  |  |
|  | SC-42 (01) Reporting To Authorized Individuals Or Roles |  |  |  |  |  |
|  | SC-42 (02) Authorized Use |  |  |  |  |  |
|  | SC-42 (03) Prohibit Use Of Devices |  |  |  |  |  |
|  | SC-43 Usage Restrictions |  |  |  |  |  |
|  | SC-44 Detonation Chambers |  |  |  |  |  |
|  | SC Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# System and Information Integrity (SI)

Table . Family Control Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Index | Control | Status  (Met, Partial, Not Met, or N/A) | Low | Mod | High | Comments |
|  | SI-1 System And Information Integrity Policy And Procedures |  | L | M | H |  |
|  | SI-02 Flaw Remediation |  | L | M | H |  |
|  | SI-02 (01) Central Management |  |  |  | H |  |
|  | SI-02 (02) Automated Flaw Remediation Status |  |  | M | H |  |
|  | SI-02 (03) Time To Remediate Flaws / Benchmarks For Corrective Actions |  |  |  |  |  |
|  | SI-02 (05) Automatic Software / Firmware Updates |  |  |  |  |  |
|  | SI-02 (06) Removal Of Previous Versions Of Software / Firmware |  |  |  |  |  |
|  | SI-03 Malicious Code Protection |  | L | M | H |  |
|  | SI-03 (01) Central Management |  |  | M | H |  |
|  | SI-03 (02) Automatic Updates |  |  | M | H |  |
|  | SI-03 (04) Updates Only By Privileged Users |  |  |  |  |  |
|  | SI-03 (06) Testing / Verification |  |  |  |  |  |
|  | SI-03 (07) Nonsignature-Based Detection |  |  |  |  |  |
|  | SI-03 (08) Detect Unauthorized Commands |  |  |  |  |  |
|  | SI-03 (09) Authenticate Remote Commands |  |  |  |  |  |
|  | SI-03 (10) Malicious Code Analysis |  |  |  |  |  |
|  | SI-04 Information System Monitoring |  | L | M | H |  |
|  | SI-04 (01) System-Wide Intrusion Detection System |  |  |  |  |  |
|  | SI-04 (02) Automated Tools For Real-Time Analysis |  |  | M | H |  |
|  | SI-04 (03) Automated Tool Integration |  |  |  |  |  |
|  | SI-04 (04) Inbound And Outbound Communications Traffic |  |  | M | H |  |
|  | SI-04 (05) System-Generated Alerts |  |  | M | H |  |
|  | SI-04 (07) Automated Response To Suspicious Events |  |  |  |  |  |
|  | SI-04 (09) Testing Of Monitoring Tools |  |  |  |  |  |
|  | SI-04 (10) Visibility Of Encrypted Communications |  |  |  |  |  |
|  | SI-04 (11) Analyze Communications Traffic Anomalies |  |  |  |  |  |
|  | SI-04 (12) Automated Alerts |  |  |  |  |  |
|  | SI-04 (13) Analyze Traffic / Event Patterns |  |  |  |  |  |
|  | SI-04 (14) Wireless Intrusion Detection |  |  |  |  |  |
|  | SI-04 (15) Wireless To Wireline Communications |  |  |  |  |  |
|  | SI-04 (16) Correlate Monitoring Information |  |  |  |  |  |
|  | SI-04 (17) Integrated Situational Awareness |  |  |  |  |  |
|  | SI-04 (18) Analyze Traffic / Covert Exfiltration |  |  |  |  |  |
|  | SI-04 (19) Individuals Posing Greater Risk |  |  |  |  |  |
|  | SI-04 (20) Privileged Users |  |  |  |  |  |
|  | SI-04 (21) Probationary Periods |  |  |  |  |  |
|  | SI-04 (22) Unauthorized Network Services |  |  |  |  |  |
|  | SI-04 (23) Host-Based Devices |  |  |  |  |  |
|  | SI-04 (24) Indicators Of Compromise |  |  |  |  |  |
|  | SI-05 Security Alerts, Advisories, And Directives |  | L | M | H |  |
|  | SI-05 (01) Automated Alerts And Advisories |  |  |  | H |  |
|  | SI-06 Security Function Verification |  |  |  | H |  |
|  | SI-06 (02) Automated Support For The Distributed Testing |  |  |  |  |  |
|  | SI-06 (03) Report Verification Results |  |  |  |  |  |
|  | SI-07 Software, Firmware, And Information Integrity |  |  | M | H |  |
|  | SI-07 (01) Integrity Checks |  |  | M | H |  |
|  | SI-07 (02) Automated Notification Of Integrity Violations |  |  |  |  |  |
|  | SI-07 (03) Centrally-Managed Integrity Tools |  |  |  |  |  |
|  | SI-07 (05) Automated Response To Integrity Violations |  |  |  | H |  |
|  | SI-07 (06) Cryptographic Protection |  |  |  |  |  |
|  | SI-07 (07) Integration Of Detection And Response |  |  | M | H |  |
|  | SI-07 (08) Auditing Capability For Significant Events |  |  |  |  |  |
|  | SI-07 (09) Verify Boot Process |  |  |  |  |  |
|  | SI-07 (10) Protection Of Boot Firmware |  |  |  |  |  |
|  | SI-07 (11) Confined Environments With Limited Privileges |  |  |  |  |  |
|  | SI-07 (12) Integrity Verification |  |  |  |  |  |
|  | SI-07 (13) Code Execution In Protected Environments |  |  |  |  |  |
|  | SI-07 (14) Binary Of Machine Executable Code |  |  |  | H |  |
|  | SI-07 (15) Code Authentication |  |  |  |  |  |
|  | SI-07 (16) Time Limit On Process Execution W/O Supervision |  |  |  |  |  |
|  | SI-08 Spam Protection |  |  | M | H |  |
|  | SI-08 (01) Central Management |  |  | M | H |  |
|  | SI-08 (02) Automatic Updates |  |  | M | H |  |
|  | SI-08 (03) Continuous Learning Capability |  |  |  |  |  |
|  | SI-10 Information Input Validation |  |  | M | H |  |
|  | SI-10 (01) Manual Override Capability |  |  |  |  |  |
|  | SI-10 (02) Review / Resolution Of Errors |  |  |  |  |  |
|  | SI-10 (03) Predictable Behavior |  |  |  |  |  |
|  | SI-10 (04) Review / Timing Interactions |  |  |  |  |  |
|  | SI-10 (05) Restrict Inputs To Trusted Sources And Approved Formats |  |  |  |  |  |
|  | SI-11 Error Handling |  |  | M | H |  |
|  | SI-12 Information Handling And Retention |  | L | M | H |  |
|  | SI-13 Predictable Failure Prevention |  |  |  |  |  |
|  | SI-13 (01) Transferring Component Responsibilities |  |  |  |  |  |
|  | SI-13 (03) Manual Transfer Between Components |  |  |  |  |  |
|  | SI-13 (04) Standby Component Installation / Notification |  |  |  |  |  |
|  | SI-13 (05) Failover Capability |  |  |  |  |  |
|  | SI-14 Non-Persistence |  |  |  |  |  |
|  | SI-14 (01) Refresh From Trusted Sources |  |  |  |  |  |
|  | SI-15 Information Output Filtering |  |  |  |  |  |
|  | SI-16 Memory Protection |  |  | M | H |  |
|  | SI-17 Fail-Safe Procedures |  |  |  |  |  |
|  | SI Family Security Controls Detail, Comment And Summary |  |  |  |  |  |

# Additional Comments