



atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: 512-615-7300
Fax: 512-615-7301
www.atsec.com

Comparison of CC Functionality & FISMA 800-53 Controls



Table of contents

1	Introduction	4
2	Assumptions:	4
3	Summary of Linux TOE support for the SP 800-53 Families of Controls	4



1 Introduction

The purpose of this document is to provide the mapping of Linux (What Type Red Hat or SLES) Common Criteria (Which EAL) Target of Evaluation (TOE) requirements to NIST SP 800-53 Security Controls This paper tries to highlights the identification of the Linux Operating System (TOE) CC certified requirements for the NIST recommended security controls of SP-800.

2 Assumptions:

It is assumed that any activity that requires a human action and does not directly impact the functions or development of the TOE, is beyond the scope of this comparison. Such activities can be evaluated for a particular agency or a customer.

The information under the column titled ‘Comments’ is general mapping to the CC 2.3 standard. It does not represent any specific implementation. This document represents coverage in general for most of the Linux operating systems evaluations done by atsec till 2Q/2006). For a specific evaluated product, the security owner of implementation will have to map their specifics to this FISMA requirement using the security target .This should be used as a guidance document.

3 Summary of Linux TOE support for the SP 800-53 Families of Controls

CONTROL NO.	CONTROL NAME	CC Certified TOE SUPPORT	Comment (all SFRs must be met to meet control compliance unless otherwise specified – in case of hierarchical SFRs, one of the listed hierarchical SFRs is sufficient unless otherwise specified)
FAMILY: ACCESS Control			
AC-1	Access Control Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.		
	Control without Enhancements	N/A	
AC-2	Account Management: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency].		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization employs automated mechanisms to support the management of	N/A	

	information system accounts.		
	Control Enhancement (2) The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
	Control Enhancement (3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
	Control Enhancement (4) The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.	N/A	
AC-3	Access Enforcement: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.		
	Control without Enhancements	Yes	FIA_UAU.1/2, FIA_UID1/2, FDP_ACC.1/2, FDP_ACF.1
	Control Enhancement (1) The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).	Yes	FMT_MSA.1 and FMT_MTD.1 (restriction to authorized administrators)
AC-4	Information Flow Enforcement: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		

	Control without Enhancements	Yes	FDP_IFC.1/2, FDP_IFF.1/2
AC-5	Separation of Duties: The information system enforces separation of duties through assigned access authorizations.		
	Control without Enhancements	Yes	FMT_SMR.1/2
AC-6	Least Privilege: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.		
	Control without Enhancements	Yes	depending on rules set forth in SFRs outlined for AC-3 and/or AC-4
AC-7	Unsuccessful Login Attempts: The information system enforces a limit of [<i>Assignment: organization-defined number</i>] consecutive invalid access attempts by a user during a [<i>Assignment: organization-defined time period</i>] time period. The information system automatically [<i>Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]</i>] when the maximum number of unsuccessful attempts is exceeded.		
	Control without Enhancements	Yes	FIA_AFL.1 (account locking required)
	Control Enhancement (1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	Yes	FIA_AFL.1 (restoration allowed by authorized administrator only)
AC-8	System Use Notification: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.		
	Control without Enhancements	Yes	FTA_TAB.1
AC-9	Previous Logon Notification: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.		
	Control without Enhancements	Yes	FTA_TAH.1
AC-10	Concurrent Session Control: The information system limits the number of concurrent sessions for any user to [<i>Assignment: organization-defined number of sessions</i>].		
	Control without Enhancements	Yes	FTA_MCS.1/2

AC-11	Session Lock: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.		
	Control without Enhancements	Yes	FTA_SSL.1/2
AC-12	Session Termination: The information system automatically terminates a session after [Assignment: organization-defined time period] of inactivity.		
	Control without Enhancements	Yes	FTA_SSL.3
AC-13	Supervision and Review – Access Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.		
	Control without Enhancements	Yes	FAU_SAR.1, FAU_SAR.3 (Controls need to be provided, actual supervision is outside the scope of the CC standard)
	Control Enhancement (1) The organization employs automated mechanisms to facilitate the review of user activities.	Yes	FAU_SAR.1, FAU_SAR.3 (Controls are provided, actual supervision is outside the scope of the CC standard)
AC-14	Permitted Actions Without Identification or Authentication: The organization identifies specific user actions that can be performed on the information system without identification or authentication.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.	N/A	
AC-15	Automated Marking: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.		
	Control without Enhancements	Yes	FDP_ETC.1/2 (Example found in LSPP)
AC-16	Automated Labeling: The information system appropriately labels information in storage, in process, and in transmission.		
	Control without Enhancements	Yes	FDP_ITC.1/2, FDP_IFC.1, FDP_IFF.1/2, FDP_ETC.1/2
AC-17	Remote Access: The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access		

	method.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	N/A
	Control Enhancement (2) The organization uses encryption to protect the confidentiality of remote access sessions.	N/A
	Control Enhancement (3) The organization controls all remote accesses through a managed access control point.	N/A
AC-18	Wireless Access Restrictions: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization uses authentication and encryption to protect wireless access to the information system.	N/A
AC-19	Access Control For Portable and Mobile Devices: The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.	N/A
AC-20	Personally Owned Information Systems: The organization restricts the use of personally owned information	



	systems for official U.S. Government business involving the processing, storage, or transmission of federal information.		
	Control without Enhancements	N/A	
Awareness and Training			
AT-1	Security Awareness and Training Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.		
	Control without Enhancements	N/A	
AT-2	Security Awareness: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.		
	Control without Enhancements	N/A	
AT-3	Security Training: The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and [<i>Assignment: organization-defined frequency</i>] thereafter.		
	Control without Enhancements	N/A	
AT-4	Security Training Records: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.		
	Control without Enhancements	N/A	
AT-5	Contacts with Security Groups and Associations: The organization establishes and maintains contacts with special interest groups, specialized forums, or professional associations to stay up to date with the latest recommended security practices, techniques, and technologies.		
	Control without Enhancements	N/A	
FAMILY: Audit and Accountability			
AU-1	Audit and Accountability Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.		
	Control without Enhancements	N/A	
AU-2	Auditable Events: The information system generates audit records for the following events: [<i>Assignment:</i>		

	<i>organization-defined auditable events</i>].		
	Control without Enhancements	Yes	FAU_GEN.1
	Control Enhancement (1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
	Control Enhancement (2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.	Yes	FAU_SAR.1
AU-3	Content of Audit Records: The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.		
	Control without Enhancements	Yes	FAU_GEN.1
	Control with Enhancements (1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	Yes	FAU_SEL.1
	Control with Enhancements(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
AU-4	Audit Storage Capacity: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.		
	Control without Enhancements	N/A	

AU-5	Audit Processing: In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].		
	Control without Enhancements	Yes	FAU_STG.4
	Control with Enhancements (1) The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage of maximum audit record storage capacity].	Yes	FAU_STG.3/4
AU_6	Audit Monitoring, Analysis, and Reporting: The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.		
	Control without Enhancements	N/A	
	Control Enhancements (1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.	N/A	
	Control Enhancement (2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.	N/A	
AU-7	Audit Reduction and Report Generation: The information system provides an audit reduction and report generation capability.		
	Control without Enhancements	Yes	FAU_SEL.1
	Control Enhancement (1) The information system provides the capability to automatically process audit	Yes	one from the family FAU_SAA

	records for events of interest based upon selectable, event criteria.		
AU-8	Time Stamps: The information system provides time stamps for use in audit record generation.		
	Control without Enhancement	Yes	FPT_STM.1
AU-9	Protection of Audit Information: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.		
	Control without Enhancements	Yes	FAU_STG.1.
AU-10	Non-Repudiation: The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).		
	Control without Enhancements	Yes	FAU_GEN.2
AU-11	Audit Retention: The organization retains audit logs for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		
	Control without Enhancements	N/A	
<u>FAMILY: Certification, Accreditation, and Security Assessments</u>			
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.		
	Control without Enhancements	N/A	
CA-2	Security Assessments: The organization conducts an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.		
	Control without Enhancements	N/A	
CA-3	Information System Connections: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.		
	Control without Enhancements	N/A	
CA-4	Security Certification: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.		

	Control without Enhancements	N/A	
CA-5	Plan of Action and Milestones: The organization develops and updates [<i>Assignment: organization-defined frequency</i>], a plan of action and milestones for the information system that documents the organization’s planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.		
	Control without Enhancements	N/A	
CA-6	Security Accreditation: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [<i>Assignment: organization-defined frequency, at least every three years</i>]. A senior organizational official signs and approves the security accreditation.		
	Control without Enhancements	N/A	
CA-7	Continuous Monitoring: The organization monitors the security controls in the information system on an ongoing basis.		
	Control without Enhancements	N/A	
CA-7	Continuous Monitoring: The organization monitors the security controls in the information system on an ongoing basis.		
	Control without Enhancements	N/A	
<u>FAMILY: Configuration Management</u>			
CM-1	Configuration Management Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.		
	Control without Enhancements	N/A	
CM-2	Baseline Configuration and System Inventory: The organization develops, documents, and maintains a current, baseline configuration of the information system, an inventory of the system’s constituent components, and relevant ownership information.		
	Control without Enhancements	N/A	
	Control Enhancements (1) The organization updates the baseline configuration as an integral part of information system component installations	N/A	
	Control Enhancements (2) The organization employs automated mechanisms to	N/A	

	maintain an up-to-date, complete, accurate, and readily available baseline configuration.		
CM-3	Configuration Change Control: The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.		
	Control without Enhancements	N/A	
	Control Enhancements (1) The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.	N/A	
CM-4	Monitoring Configuration Changes: The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.		
	Control without Enhancements	N/A	
CM-5	Access Restrictions for Change: The organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such change		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	N/A	
CM-6	Configuration Settings: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the		

	configuration settings; and (iv) enforces the configuration settings in all components of the information system	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.	N/A
CM-7	Least Functionality: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: <i>[Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services]</i> .	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization reviews the information system [Assignment: organization-defined frequency], to identify and eliminate unnecessary functions, ports, protocols, and/or services.	N/A
FAMILY: Contingency Planning		
CP-1	Contingency Planning Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	
	Control without Enhancements	N/A
CP-2	Contingency Plan: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan,	

	Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).		
CP-3	Contingency Training: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [<i>Assignment: organization-defined frequency, at least annually</i>].		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	N/A	
	Control Enhancement (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	N/A	
CP-4	Contingency Plan Testing: The organization tests the contingency plan for the information system [<i>Assignment: organization-defined frequency, at least annually</i>] using [<i>Assignment: organization-defined tests and exercises</i>] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).	N/A	
	Control Enhancement (2) The organization tests the contingency plan at the alternate processing site to	N/A	

	familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.		
	Control Enhancement (3) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.	N/A	
CP-5	Contingency Plan Update: The organization reviews the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing		
	Control without Enhancements	N/A	
CP-6	Alternate Storage Sites: The organization identifies storage sites and initiates necessary agreements to permit the storage of information system backup information.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.	N/A	
	Control Enhancement (2) The alternate storage site is configured to facilitate timely and effective recovery operations.	N/A	
	Control Enhancement (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	N/A	
CP-7	Alternate Processing Sites: The organization identifies an alternate processing site and initiates necessary		

	agreements to permit the resumption of information system operations for critical mission business functions within [Assignment: organization-defined time period] when primary processing capabilities are unavailable	
	Control without Enhancements	N/A
	Control Enhancement (1) The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.	N/A
	Control Enhancement (2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	N/A
	Control Enhancement (3) Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.	N/A
	Control Enhancement (4) The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.	N/A
CP-8	Telecommunication Services: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.	
	Control without Enhancements	N/A
	Control Enhancement (1) Primary and alternate telecommunications service	N/A

	agreements contain priority-of-service provisions in accordance with the organization's availability requirements.		
	Control Enhancement (2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services.	N/A	
	Control Enhancement (3) Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.	N/A	
	Control Enhancement (4) Primary and alternate telecommunications service providers have adequate contingency plans.	N/A	
CP-9	Information System backup: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [<i>Assignment: organization-defined frequency</i>] and stores backup information at an appropriately secured location.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization tests backup information [<i>Assignment: organization-defined frequency</i>] to ensure media reliability and information integrity.	N/A	
	Control Enhancement (2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.	N/A	

	Control Enhancement (3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.	N/A	
CP-10	Information System Recovery and Reconstitution: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.	N/A	
FAMILY: Identification and Authentication			
IA-1	Identification and Authentication Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.		
	Control without Enhancements	N/A	
IA-2	User Identification and Authentication: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).		
	Control without Enhancements	Yes	FIA_UID.1/2, FIA_UAU.1/2
	Control Enhancements (1) The information system employs multifactor authentication.	Yes	FIA_UAU.5
IA-3	Device Identification and Authentication: The information system identifies and authenticates specific devices before establishing a connection.		
	Control without Enhancements	Yes	implementation specific
IA-4	Identifier Management: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier		

	after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.	
	Control without Enhancements	N/A
IA-5	Authenticator Management: The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.	
	Control without Enhancements	Yes
IA-6	Authenticator Feedback: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals	
	Control without Enhancements	Yes FIA_UAU.7
IA-7	Cryptographic Module Authentication: For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.	
	Control without Enhancements	N/A depending on the rationale about the claimed cryptographic mechanism in the ST
FAMILY: Incident Response		
IR-1	Incident Response Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	
	Control without Enhancements	N/A
IR-2	Incident Response Training: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.	N/A
	Control Enhancement (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	N/A
IR-3	Incident Response Testing: The organization tests the incident response capability for the information system	

	[Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and exercises] to determine the incident response effectiveness and documents the results.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.	N/A
IR-4	Incident Handling: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs automated mechanisms to support the incident handling process.	N/A
IR-5	Incident Monitoring: The organization tracks and documents information system security incidents on an ongoing basis.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	N/A
IR-6	Incident Reporting: The organization promptly reports incident information to appropriate authorities.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs automated mechanisms to assist in the reporting of security incidents.	N/A
IR-7	Incident Response Assistance: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The	

	support resource is an integral part of the organization's incident response capability.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	N/A
FAMILY: Maintenance		
MA-1	Maintenance Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	
	Control without Enhancements	N/A
MA-2	Periodic Maintenance: The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).	N/A
	Control Enhancement (2) The organization employs automated mechanisms to ensure that periodic	N/A

	<p>maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.</p>		
MA-3	<p>Maintenance Tools: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.</p>		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.	N/A	
	Control Enhancement (2) The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.	N/A	
Control Enhancement (3) The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate	N/A		

	organization official explicitly authorizes an exception.		
	Control Enhancement (4) The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools.	N/A	
MA-4	Remote Maintenance: The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.	N/A	
	Control Enhancement (2) The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.	N/A	
	Control Enhancement (3) Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.	N/A	
MA-5	Maintenance Personnel: The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.		
	Control without Enhancements	N/A	
MA-6	Timely Maintenance: The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.		



	Control without Enhancements	N/A	
FAMILY: Media Protection			
MP-1	Media Protection Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.		
	Control without Enhancements	N/A	
MP-2	Media Access: The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.		
	Control without Enhancements	N/A	
	Control Enhancement (1) Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.	N/A	
MP-3	Media Labeling: The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: [<i>Assignment: organization-defined list of media types and hardware components</i>].		
	Control without Enhancements	N/A	
MP-4	Media Storage: The organization physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.		
	Control without Enhancements	N/A	
MP-5	Media Transport: The organization controls information system media (paper and digital) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.		
	Control without Enhancements	N/A	
MP-6	Media Sanitization and Disposal: The organization: (i) sanitizes information system media, both paper and digital, prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii) periodically tests sanitization equipment and procedures to ensure correct performance.		
	Control without Enhancements	N/A	
FAMILY: Physical and Environmental Protection			

PE-1	Physical and Environmental Protection Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.		
	Control without Enhancements	N/A	
PE-2	Physical Access Authorization: The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].		
	Control without Enhancements	N/A	
PE-3	Physical Access Control: The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization’s assessment of risk.		
	Control without Enhancements	N/A	
PE-4	Access Control For Transmission Medium: The organization controls physical access to information system distribution and transmission lines within organizational facilities to prevent accidental damage, eavesdropping, in-transit modification, disruption, or physical tampering.		
	Control without Enhancements	N/A	
PE-5	Access Control For Display Medium: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.		
	Control without Enhancements	N/A	
PE-6	Monitoring Physical Access: The organization monitors physical access to information systems to detect and respond to incidents.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization monitors real-time intrusion alarms and surveillance equipment.	N/A	
	Control Enhancement (2) The organization employs automated mechanisms to	N/A	

	ensure potential intrusions are recognized and appropriate response actions initiated.		
PE-7	Visitor Control: The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.		
	Control without Enhancements	N/A	
	Control Enhancement (1)	N/A	
PE-7	Visitor Control: The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization escorts visitors and monitors visitor activity, when required.	N/A	
PE-8	Access Logs: The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the access logs [Assignment: <i>organization-defined frequency</i>].		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization employs automated mechanisms to facilitate the maintenance and review of access logs.	N/A	
PE-9	Power Equipment and Cabling: The organization protects power equipment and power cabling for the information system from damage and destruction.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization employs redundant and parallel power cabling paths.	N/A	
PE-10	Emergency Shutoff: For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or		

	threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.	
	Control without Enhancements	N/A
PE-11	Emergency Power: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
	Control without Enhancements	N/A
	Control Enhancement (1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	N/A
	Control Enhancement (2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.	N/A
PE-12	Emergency Lighting: The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.	
	Control without Enhancements	N/A
PE-13	Fire Protection: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire	
	Control without Enhancements	N/A
	Control Enhancement (1) Fire suppression and detection devices/systems activate automatically in the event of a fire.	N/A
	Control Enhancement (2) Fire suppression and detection devices/systems provide automatic notification of any activation to the organization	N/A

	and emergency responders.		
PE-14	Temperature and Humidity Controls: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within facilities containing information systems.		
	Control without Enhancements	N/A	
PE-15	Water Damage Protection: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.		
	Control without Enhancements	N/A	
	Control Enhancement (1) The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.	N/A	
PE-16	Delivery and Removal: The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.		
	Control without Enhancements	Yes	This should be covered with the evaluation of delivery & operation starting with EAL2
PE-17	Alternative Work Site: Individuals within the organization employ appropriate information system security controls at alternate work sites.		
	Control without Enhancements	N/A	
PE-18	Location of Information System Components: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.		
	Control without Enhancements	N/A	
PE-19	Information leakage: The organization protects the information system from information leakage due to electromagnetic signals emanations.		
	Control without Enhancements	N/A	
FAMILY: Planning			
PL-1	Security Planning Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls		
	Control without Enhancements	N/A	

PL-2	System Security Plan: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.
	Control without Enhancements N/A
PL-3	System Security Plan Update: The organization reviews the security plan for the information system [Assignment: organization-defined frequency] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
	Control without Enhancements N/A
PL-4	Rules of Behavior: The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.
	Control without Enhancements N/A
PL-5	Privacy Impact Assessment: The organization conducts a privacy impact assessment on the information system.
	Control without Enhancements N/A
FAMILY: Personnel Security	
PS-1	Personnel Security Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
	Control without Enhancements N/A
PS-2	Position Categorization: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [Assignment: organization-defined frequency].
	Control without Enhancements N/A
PS-3	Personnel Screening: The organization screens individuals requiring access to organizational information and information systems before authorizing access.
	Control without Enhancements N/A
PS-4	Personnel Termination: When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.
	Control without Enhancements N/A

	Control without Enhancements	N/A	
PS-5	Personnel Transfer: The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).		
	Control without Enhancements	N/A	
PS-6	Access Agreements: The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements <i>[Assignment: organization-defined frequency]</i>		
	Control without Enhancements	N/A	
PS-7	Third-Party Personnel Security: The organization establishes personnel security requirements including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.		
	Control without Enhancements	N/A	
PS-8	Personnel Sanctions: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		
	Control without Enhancements	N/A	
FAMILY: Risk Assessment			
RA-1	Risk Assessment Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.		
	Control without Enhancements	N/A	
RA-2	Security Categorization: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.		
	Control without Enhancements	N/A	
RA-3	Risk Assessment: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).		
	Control without Enhancements	N/A	

RA-4	Risk Assessment Update: The organization updates the risk assessment [<i>Assignment: organization-defined frequency</i>] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.
	Control without Enhancements N/A
RA-5	Vulnerability Scanning: The organization scans for vulnerabilities in the information system [<i>Assignment: organization-defined frequency</i>] or when significant new vulnerabilities affecting the system are identified and reported.
	Control without Enhancements N/A
	Control Enhancements (1) Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned.
	Control Enhancements (2) The organization updates the list of information system vulnerabilities [<i>Assignment: organization-defined frequency</i>] or when significant new vulnerabilities are identified and reported.
	Control Enhancements (3) Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.
FAMILY: System and Services Acquisition	
SA-1	System and Services Acquisition Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
	Control without Enhancements N/A
SA-2	Allocation of Resources: The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.
	Control without Enhancements N/A

SA-3	Life Cycle Support: The organization manages the information system using a system development life cycle methodology that includes information security considerations.	
	Control without Enhancements	N/A ALC_DVS.1 and ALC_DVS.2 development security controls require that proper documentation is place, but enforcement is beyond the scope of CC
SA-4	Acquisitions: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk	
	Control without Enhancements	N/A
SA-5	Information System Documentation: The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel	
	Control without Enhancements	N/A
	Control Enhancements (1) The organization includes documentation describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.	N/A
	Control Enhancements (2) The organization includes documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).	N/A
SA-6	Software Usage Restrictions: The organization complies with software usage restrictions.	
	Control without Enhancements	N/A
SA-7	User Installed Software: The organization enforces explicit rules governing the downloading and installation of software by users.	
	Control without Enhancements	N/A
SA-8	Security Design Principles: The organization designs and implements the information system using security engineering principles	
	Control without Enhancements	N/A

SA-9	Outsourced Information System Services: The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance		
	Control without Enhancements	N/A	
SA-10	Developer Configuration Management: The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation		
	Control without Enhancements	N/A	
SA-11	Developer Security Testing: The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system		
	Control without Enhancements		
	Control Enhancements		
FAMILY: System and Communications Protection			
SC-1	System and Communications Protection Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.		
	Control without Enhancements	N/A	
SC-2	Application Partitioning: The information system separates user functionality (including user interface services) from information system management functionality.		
	Control without Enhancements	Yes	FPT_SEP.1/2/3, FPT_RVM.1
SC-3	Security Function Isolation: The information system isolates security functions from non-security functions.		
	Control without Enhancements	Yes	FPT_SEP.1/2/3 (also possible: FDP_ACC.1, FDP_ACF.1 for protecting application files)
	Control Enhancement (1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.	Yes	for NIAP evaluations: this is covered by the design of an operating system For BSI evaluations: SFRs for the environment must be specified which define the processor separation capability
	Control Enhancement (2) The information system further divides the security functions with the functions enforcing	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement. (examples: usage of different

	access and information flow control isolated and protected from both nonsecurity functions and from other security functions.		rings of Intel processors for TSF/non-TSF functions)
	Control Enhancement (3) The information system minimizes the amount of nonsecurity functions included within the isolation boundary containing security functions.	No/Yes	This requirement most likely is covered by assurance requirements (and therefore design constraints) of EAL5 and above, but may be implemented in TOEs with EAL4 and lower.
	Control Enhancement (4) The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.	No/Yes	This requirement is covered by assurance requirements (and therefore design constraints) of EAL5 and above, but may be implemented in TOEs with EAL4 and lower.
	Control Enhancement (5) The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.	No/Yes	This requirement is covered by assurance requirements (and therefore design constraints) of EAL5 and above, but may be implemented in TOEs with EAL4 and lower.
SC-4	Information Remnants: The information system prevents unauthorized and unintended information transfer via shared system resources.		
	Control without Enhancements	Yes	FDP_RIP.1/2
SC-5	Denial of Service Protection: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].		
	Control without Enhancements	Yes	all SFRs out of class FRU are Applicable
	Control Enhancements (1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.	Yes	all SFRs out of class FRU are Applicable
	Control Enhancements (2)	Yes	FRU_RSA.1/2

	The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.		
SC-6	Resource Priority: The information system limits the use of resources by priority.		
	Control without Enhancements	Yes	FRU_PRS.1/2
SC-7	Boundary Protection: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.		
	Control without Enhancements	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
	Control Enhancements (1) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks. The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.	N/A	
SC-8	Transmission Integrity: The information system protects the integrity of transmitted information.		
	Control without Enhancements	Yes	FPT_ITI.1
	Control Enhancements (1) The organization employs	N/A	

	cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).		
SC-9	Transmission Confidentiality: The information system protects the confidentiality of transmitted information		
	Control without Enhancements	Yes	FPT_ITC.1 or FTP_ITC.1
	Control Enhancements (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).	N/A	
SC-10	Network Disconnect: The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity		
	Control without Enhancements	Yes	FRU_RSA.1 or FTA_LSA.1
SC-11	Trusted Path: The information system establishes a trusted communications path between the user and the security functionality of the system.		
	Control without Enhancements	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement (for example: FCS class or FTP_TRP.1).
SC-12	Cryptographic Key Establishment and Management: The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management		
	Control without Enhancements	Yes	FCS_CKM.1, FCS_CKM.2, and FCS_COP.1
SC-13	Use of Validated Cryptography: When cryptography is employed within the information system, the cryptography complies with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation		
	Control without Enhancements	N/A	Please check with the FIPS-140-2 conformance claim within the ST.
SC-14	Public Access Protections: For publicly available systems, the information system protects the integrity of the		

	information and applications		
	Control without Enhancements	Yes	FPT_TST.1
SC-15	Collaborative Computing: The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone)		
	Control without Enhancements	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
	Control Enhancements (1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.	N/A	
SC-16	Transmission of Security Parameters: The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.		
	Control without Enhancements	Yes	FDP_ETC.1, FDP_ETC.2, FDP_ITC.1, FDP_ITC.2
SC-17	Public Key Infrastructure Certificates: The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system		
	Control without Enhancements	N/A	
SC-18	Mobile Code: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.		
	Control without Enhancements	N/A	
SC-19	Voice Over Internet Protocol: The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.		
	Control without Enhancements	N/A	
SC-20	Secure Name Lookup Service (Authoritative Source): The information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing organizational information resources to entities across the Internet provides artifacts for data origin authentication and data integrity to enable users to obtain message authentication and message integrity assurances for the information received during network-based transactions.		
	Control without Enhancements	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.

SC-21	Secure Name Lookup Service (Resolution): The information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing information resources to entities within the organization provides mechanisms for data origin authentication and data integrity verification and performs these services when requested by client systems		
	Control without Enhancements	N/A	
FAMILY: System and Information Integrity			
SI-1	System and Information Integrity Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.		
SI-2	Flaw Remediation: The organization identifies, reports, and corrects information system flaws		
	Control without Enhancements	N/A	Supported by ALC_FLR.1/2/3
	Control Enhancements (1) The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.	N/A	
	Control Enhancements (2) The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation.	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
SI-3	Malicious Code Protection: The information system implements malicious code protection that includes a capability for automatic updates.		
	Control without Enhancements	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
	Control Enhancements (1) The organization centrally manages virus protection mechanisms.	N/A	
	Control Enhancements (2)	No	

	The information system automatically updates virus protection mechanisms.		
SI-4	Intrusion Detection Tools and Techniques: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system		
	Control without Enhancements	N/A	
	Control Enhancements (1) The organization networks individual intrusion detection tools into a systemwide intrusion detection system using common protocols.	N/A	
	Control Enhancements (2) The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	N/A	
	Control Enhancements (3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.	N/A	
Control Enhancements (4) The information system monitors outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).	Yes	FDP_IFC.1, FDP_IFF.1, and FDP_IFF.2	
SI-5	Security Alerts and Advisories: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response		
	Control without Enhancements	N/A	Supported by ALC_FLR.3

	Control Enhancements (1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	N/A	
SI-6	Security Functionality Verification: The information system verifies, to the extent feasible, the correct operation of security functions [<i>Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]</i>] and [<i>Selection (one or more): notifies system administrator, shuts the system down, restarts the system</i>] when anomalies are discovered.		
	Control without Enhancements	Yes	FPT_TST.1
	Control Enhancements (1) The organization employs automated mechanisms to provide notification of failed security tests.	N/A	
	Control Enhancements (2) The organization employs automated mechanisms to support management of distributed security testing.	N/A	
SI-7	Software and Information Integrity: The information system detects and protects against unauthorized changes to software and information.		
	Control without Enhancements	Yes	FPT_TST.1
SI-8	SPAM & SPAMWARE Protection: The information system implements spam and spyware protection.		
	Control without Enhancements	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.
	Control Enhancements (1) The organization centrally manages spam and spyware protection mechanisms.	N/A	
	Control Enhancements (2) The information system automatically updates spam and spyware protection mechanisms.	Yes	There are many ways to accomplish this. There is not a group of SFRs that can be described here. Each implementation will have to map their specifics to this FISMA requirement.



SI-9	Information Input Restrictions: The organization restricts the information input to the information system to authorized personnel only.	
	Control without Enhancements	N/A
SI-10	Information Input Accuracy, Completeness, and Validity: The information system checks information for accuracy, completeness, validity, and authenticity	
	Control without Enhancements	No There is not a specific SFR for this. But the vulnerability analysis and testing part of the assurance fulfills this requirement.
SI-11	Error Handling: The information system identifies and handles error conditions in an expeditious manner.	
	Control without Enhancements	No There is not a specific SFR for this. But the vulnerability analysis and testing part of the assurance fulfills this requirement.
SI-12	Information Output Handling and Retention: The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.	
	Control without Enhancements	N/A