



PRETRIAL SERVICES AGENCY FOR THE DISTRICT OF COLUMBIA
OFFICE OF INFORMATION TECHNOLOGY

Susan W. Shaffer, Director
Effective Date: June 01, 2012

POLICY STATEMENT

5500

Table of Contents

INFORMATION SECURITY POLICY	3
Rule.....	3
Authority.....	3
Rationale.....	3
Applicability	4
Supercedure	4
SECURITY CONTROL CLASS DESCRIPTION.....	5
Management Controls.....	5
Operational Controls.....	5
Technical Controls.....	5
PART I- ENTIRE STAFF	6
MANAGEMENT	
Planning (PL 1, 4-5)	6
Program Management(PM 1-3, 9-11).....	6
Risk Assessment (RA 1-3, 5).....	8
Security Assessment and Authorization (CA 1-3, 6).....	10
System and Services Acquisition (SA 1-4, 6-7, 9)	11
OPERATIONAL	
Awareness and Training (AT 1-2, 4).....	13
Configuration Management (CM 1, 3)	13
Contingency Planning (CP 1-4).....	14
Incident Response (IR 1-4, 6-7).....	15
System Maintenance (MA 1).....	17
Media Protection (MP 1-6).....	17
Personnel Security (PS 1-8).....	19
Physical and Environmental Protection (PE 1, 5, 17).....	21
System and Information Integrity (SI 1, 8-12)	21

Table of Contents continued

TECHNICAL

Access Control (AC 1-3, 6-8, 11, 17-20, 22).....	23
Audit and Accountability (AU 1)	28
Identification and Authentication (IA 1-6)	28
System and Communications Protection (SC 1, 10, 13-15, 19)	31

PART II- INFORMATION TECHNOLOGY STAFF

MANAGEMENT

Planning (PL 2, 6)	33
Program Management (PM 4-8)	34
Security Assessment and Authorization (CA 5, 7).....	34
System Services and Acquisition (SA 3, 5, 8, 10-11).....	35

OPERATIONAL

Awareness and Training (AT 3)	37
Configuration Management (CM 2, 4-9).....	39
Contingency Planning (CP 6, 8-10).....	41
Incident Response (IR 5, 8)	42
Maintenance (MA 2-6)	44
Physical and Environmental Protection (PE 2-4, 6-16, 18).....	47
System and Information Integrity (SI 2-5, 7).....	47

TECHNICAL

Access Control (AC 4-5, 14)	50
Audit and Accountability (AU 2-9, 11-12).....	51
Identification and Authentication (IA 7-8)	54
System and Communications Protection (SC 2, 4-5, 7-9, 12, 17-18, 20, 22-23, 28, 32) .	54

CONTROL LOCATOR INDEX.....	59
----------------------------	----

Information Security Policy

Rule Security planning is a core component of an information security program and is integral to understanding the state and effectiveness of the security controls of an information system. Security planning control includes the establishment, documentation, and systematic maintenance of a system security plan.

The Office of Information Technology (OIT) at Pretrial Services Agency for the District of Columbia (PSA) develops, disseminates, and annually reviews:

- A formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and
- Provides formal documented procedures to facilitate the implementation of the policy and associated controls.

Authority The Federal Information Security Management Act (FISMA) requires federal agencies to institute procedures to facilitate the implementation of a planning policy. The procedures are derived from guidance provided by the National Institute of Standards and Technology (NIST) in its special publication 800-53 dated August, 2009 with updates from May, 2010.

Rationale For the security objectives of confidentiality, integrity, and availability, PSA's information systems (PSA Enterprise, PRISM, and DTMS) are categorized as moderate impact. This policy contains 170 controls as required by security categorization standards.

Each of the controls are divided into categories:

- Management
- Operational
- Technical

Continued on next page

Information Security Policy, Continued

Applicability This policy applies to all permanent and temporary PSA employees, including contractors and interns that use, manage, develop, maintain or support PSA business and mission critical systems. The term employee as used in this policy collectively refers to all of the aforementioned personnel types unless specifically stated.

This policy is divided into sections that apply to all PSA employees (Part I) and those that exclusively apply to PSA's Office of Information Technology (OIT) (Parts I & II).

Supercedure This policy supersedes all policy statements and management instructions issued in 2005 by PSA's OIT.

Security Control Class Description

Management Controls

The controls that address security topics than can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

Operational Controls

Broadly speaking, the security controls that are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and rely upon management activities as well as technical controls.

Technical Controls

Focus on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls however, always requires significant operational considerations and should be consistent with the management of security within the organization.

PART I- Entire Staff

MANAGEMENT- Planning

- Policy (PL-1)** PSA's OIT develops, disseminates, and reviews/updates annually:
- A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
-

- Rules of Behavior (PL-4)** PSA's OIT:
- Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and
 - Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
-

- Privacy Impact Assessment (PL-5)** PSA conducts a privacy impact assessment on the information system in accordance with OMB policy.
-

MANAGEMENT-Program Management

- Information Security Program Plan (PM-1)** PSA's OIT develops and disseminates an organization-wide information security program plan that:
- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
 - Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
-

Continued on next page

MANAGEMENT-Program Management, Continued

Information Security Program Plan
Error! Not a valid bookmark self-reference.
(continued)

- Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

The organization-wide information security program plan is reviewed annually and revisions to the plan address organizational changes and problems identified during plan implementation or security control assessments.

Senior Information Security Officer (PM-2)

PSA appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Information Security Resources (PM-3)

PSA's OIT:

- Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
 - Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
 - Ensures that information security resources are available for expenditure as planned.
-

Risk Management Strategy (PM-9)

PSA's OIT:

- Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and
 - Implements that strategy consistently across the organization.
-

Continued on next page

MANAGEMENT-Program Management, Continued

**Security
Authorization
Process
(PM-10)**

PSA's OIT:

- Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;
 - Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
 - Fully integrates the security authorization processes into an organization-wide risk management program.
-

**Mission
Business
Process
(PM-11)**

PSA's OIT

- Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
 - Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.
-

MANAGEMENT- Risk Assessment

**Policy
(RA-1)**

PSA's OIT develops, disseminates, and reviews/updates annually:

- A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
-

**Security
Categorization
(RA-2)**

PSA's OIT:

- Categorizes information and the information systems in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
 - Documents the security categorization results (including supporting rationale) in the security plan for the information systems; and
 - Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
-

Continued on next page

MANAGEMENT- Risk Assessment, Continued

**Risk
Assessment
(RA-3)**

PSA's OIT:

- Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
 - Documents risk assessment results in the risk assessment report titled "PSA Enterprise (PSAE)- Risk Assessment Report";
 - Reviews risk assessment results annually or when security posture changes; and
 - Updates the risk assessment at least every three years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
-

**Vulnerability
Scanning
(RA-5)**

PSA employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. PSA also:

- Scans for vulnerabilities in the information systems and hosted applications on ongoing basis or at least once a week and when new vulnerabilities potentially affecting the system/applications are identified and reported;
 - Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - Enumerating platforms, software flaws, and improper configurations;
 - Formatting and making transparent, checklists and test procedures; and
 - Measuring vulnerability impact;
 - Analyzes vulnerability scan reports and results from security control assessments;
 - Remediates legitimate vulnerabilities on ongoing basis or at least once a month in accordance with an organizational assessment of risk; and
 - Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
-

MANAGEMENT- Security Assessment and Authorization

**Policy
(CA-1)**

PSA's OIT develops, disseminates, and reviews/updates annually:

- Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.
-

**Security
Assessments
(CA-2)**

PSA's OIT develops a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities.

PSA's OIT is responsible for assessing security controls in the information system on an ongoing basis and at least once every year 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.

PSA's OIT produces a security assessment report that documents the results of the assessment and provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

In addition PSA employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

**Information
System
Connections
(CA-3)**

PSA's OIT:

- Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;
 - Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
 - Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.
-

Continued on next page

MANAGEMENT- Risk Assessment, Continued

**Security
Authorization
(CA-6)**

PSA:

- Assigns a senior-level executive or manager to the role of authorizing official for the information systems;
 - Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
 - Updates the security authorization every three years.
-

MANAGEMENT- System and Services Acquisition

**Policy
(SA-1)**

PSA's OIT develops, disseminates, and reviews/updates annually:

- A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
-

**Allocation of
Resources
(SA-2)**

PSA's OIT:

- Includes a determination of information security requirements for the information systems in mission/business process planning;
 - Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and
 - Establishes a discrete line item for information security in organizational programming and budgeting documentation.
-

**Acquisitions
(SA-4)**

PSA includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

- Security functional requirements/specifications;
 - Security-related documentation requirements; and
 - Developmental and evaluation-related assurance requirements.
-

Continued on next page

MANAGEMENT- System and Services Acquisition, Continued

**Acquisitions
(SA-4)
(Continued)**

PSA requires that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. PSA also ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

**Software Usage
Restrictions
(SA-6)**

PSA's OIT:

- Uses software and associated documentation in accordance with contract agreements and copyright laws;
 - Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
 - Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
-

**User-Installed
Software
(SA-7)**

PSA enforces explicit rules governing the installation of software by users.

- Users are not authorized to install any software
 - Any software must be installed by authorized IT personnel or under their guidance.
-

**External
Information
System Service
(SA-9)**

PSA's OIT:

- Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
 - Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
 - Monitors security control compliance by external service providers.
-

OPERATIONAL- Awareness and Training

Policy (AT-1)	PSA develops, disseminates, and reviews/updates annually: <ul style="list-style-type: none">• A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and• Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
--------------------------	--

Security Awareness (AT-2)	PSA provides basic security awareness, role based; security related training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and every fiscal year thereafter.
--	---

Security Training Records (AT-4)	PSA documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records as defined by the National Archives and Records Administration; General Records Schedule 1; Civilian Records item 29; Training Records.
---	--

OPERATIONAL- Configuration Management

Policy (CM-1)	PSA's OIT develops, disseminates, and reviews/updates annually: <ul style="list-style-type: none">• A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and• Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
--------------------------	---

Continued on next page

OPERATIONAL- Configuration Management, Continued

Configuration Change Control (CM-3)	<p>PSA's OIT tests, validates and documents changes to the information system before implementing changes on the operational system. In addition, PSA's OIT:</p> <ul style="list-style-type: none">• Determines the types of changes to the information system that are configuration controlled;• Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;• Documents approved configuration-controlled changes to the system;• retains and reviews records of configuration-controlled changes to the system;• Audits activities associated with configuration-controlled changes to the system; and• Coordinates and provides oversight for configuration change control activities through established Change Control Boards (CCB) which met at least once a month.
--	---

OPERATIONAL- Contingency Planning

Policy (CP-1)	<p>PSA's OIT develops, disseminates, and reviews/updates annually:</p> <ul style="list-style-type: none">• A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and• Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
Contingency Plan (CP-2)	<p>PSA's OIT develops a contingency plan for the information systems that:</p> <ul style="list-style-type: none">• Identify essential missions and business functions and associated contingency requirements;• Provide recovery objectives, restoration priorities, and metrics;• Address contingency roles, responsibilities, assigned individuals with contact information;• Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure;• Address eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and

Continued on next page

OPERATIONAL- Contingency Planning, Continued

Contingency Plan Error! Not a valid bookmark self-reference. (continued)

- Are reviewed and approved by designated officials within the organization.

Copies of the contingency plan are distributed to OIT Personnel, and Office and Program Directors.

Contingency Training (CP-3)

PSA trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.

Contingency Plan Exercises and Testing (CP-4)

PSA's OIT:

- Tests and/or exercises the contingency plan for the information systems once a year using preparations for the Eagle Horizon exercise to determine the plan's effectiveness and the organization's readiness to execute the plan; and
- Reviews the contingency plan test/exercise results and initiates corrective actions.

PSA coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

OPERATIONAL- Incident Response

Policy (IR-1)

PSA's OIT develops, disseminates, and reviews/updates annually:

- A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
-

Incident Response Training (IR-2)

PSA:

- Trains personnel in their incident response roles and responsibilities with respect to the information system; and
 - Provides refresher training annually.
-

Continued on next page

OPERATIONAL- Incident Response, Continued

Testing and Exercises (IR-3)

PSA tests and/or exercises the incident response capability for the information systems annually using the incident response plan during the Eagle Horizon exercise to determine the incident response effectiveness and documents the results.

Incident Handling (IR-4)

PSA's OIT:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises; and
- Implements the resulting changes accordingly.

In addition, PSA employs automated mechanisms to support the incident handling process.

Incident Reporting (IR-6)

PSA's OIT employs automated mechanisms to assist in the reporting of security incidents. PSA also:

- Requires personnel to report suspected security incidents to the organizational incident response capability within one hour of becoming aware of it; and
 - Reports security incident information to designated authorities.
-

Incident Response Assistance (IR-7)

PSA provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information systems for the handling and reporting of security incidents. PSA also employs automated mechanisms to increase the availability of incident response related information and support.

OPERATIONAL- System Maintenance

**Policy
(MA-1)**

PSA's OIT develops, disseminates, and reviews/updates annually:

- A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
-

OPERATIONAL- Media Protection

**Policy
(MP-1)**

PSA's OIT develops, disseminates, and reviews/updates annually:

- A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
-

**Media Access
(MP-2)**

PSA restricts access to external/removable media which is not issued by the government to authorized personnel using only approved equipment.

PSA employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

**Media Marking
(MP-3)**

PSA's OIT:

- Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
 - Exempts government issued media equipment from marking as long as the exempted items remain within confines of the agency or its security measures are in place.
-

Continued on next page

OPERATIONAL- Media Protection, Continued

**Media Storage
(MP-4)**

PSA's OIT:

- Physically controls and securely stores hard drives, digital media and tapes in the media storage cabinets in a designated area;
 - Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
-

**Media
Transport
(MP-5)**

PSA's OIT:

- Protects and controls magnetic tapes, removable hard drives, and flash/thumb drives during transport outside of controlled areas using encryption;
 - Maintains accountability for information system media during transport outside of controlled areas;
 - Restricts the activities associated with transport of such media to authorized personnel;
 - Documents activities associated with the transport of information system media; and
 - Employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
-

**Media
Sanitation
(MP-6)**

PSA's OIT:

- Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
 - Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.
-

OPERATIONAL- Personnel Security

**Policy
(PS-1)**

PSA's OIT annually reviews and/or updates:

- A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Also see Policy Statement 4060 *Personnel Security Program*.

**Position
Categorization
(PS-2)**

For all positions within the Agency:

- An assigned risk designation is given to each position;
- A screening criteria is established for individuals filling those positions; and
- Reviews and revisions of each position are made as determined by the Office of Human Capital Management (OHCM).

Also see Policy Statement 4060 *Personnel Security Program*.

**Personnel
Screening
(PS-3)**

PSA screens individuals prior to authorizing access to the information systems; and rescreens individuals according to the procedures in Policy Statement 4060 *Personnel Security Program*.

PSA's OIT provides information system access only after getting notification of approval from OHCM.

Continued on next page

OPERATIONAL- Personnel Security, Continued

**Personnel
Termination
(PS-4)**

Upon termination of employment PSA's OIT and OHCM:

- Terminate information system access;
 - Conduct exit interviews;
 - Retrieve all security-related organizational information and system-related property; and
 - Retains access to organization information and information systems formerly controlled by the terminated individual.
-

**Personnel
Transfer (PS-5)**

PSA's OIT reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the Agency.

Upon OHCM notification, PSA's OIT will make changes that pertain to the access of shared drives, or Agency information and information systems.

**Access
Agreements
(PS-6)**

PSA ensures that individuals requiring access to Agency information and information systems sign appropriate access agreements prior to being granted access. Access agreements are reviewed and updated every three (3) years or when an individual transfers from one unit to another within the Agency.

OHCM determines the nature of access for information and/or to information systems that a newly hired employee must have and submits a Request for Computer Access form for processing. OIT grants access upon receipt of proper documentation.

**Third-Party
Personnel
Agreement
(PS-7)**

PSA's OHCM and OIT:

- Establish personnel security requirement including security roles and responsibilities for third-party providers;
 - Document personnel security requirements; and
 - Monitor provider compliance.
-

**Personnel
Sanctions
(PS-8)**

PSA has a formal sanction process for employees who fail to comply with established information security policies and procedures see Policy Statement 4090.1 *Disciplinary and Adverse Actions*.

OPERATIONAL- Physical and Environmental Protection

Policy (PE-1)	PSA develops, disseminates, and reviews/updates annually: <ul style="list-style-type: none">• A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and• Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
----------------------	--

Control for Output Devices (PE-5)	PSA controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
--	--

Alternate Work Site (PE-17)	PSA's OIT: <ul style="list-style-type: none">• Employs security controls applicable for remote access as defined in the employee telecommuting agreement Policy Statement 4040.2 <i>Telework Program</i> and includes multi-factor authentication to access PSA information systems from alternate work sites;• Assesses as feasible, the effectiveness of security controls at alternate work sites; and• Provides a means for employees to communicate with information security personnel in case of security incidents or problems.
------------------------------------	---

OPERATIONAL- System and Information Integrity

Policy (SI-1)	PSA's OIT develops, disseminates, and reviews/updates annually: <ul style="list-style-type: none">• A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and• Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
----------------------	---

Continued on next page

OPERATIONAL- System and Information Integrity, Continued

**Spam
Protection
(SI-8)**

PSA's OIT:

- Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
 - Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.
-

**Information
Input
Restrictions
(SI-9)**

PSA restricts the capability to input information to the information systems to authorized personnel.

**Information
Input
Validation
(SI-10)**

PSA information systems check the validity of information inputs.

**Error Handling
(SI-11)**

PSA's OIT:

- Identifies potentially security-relevant error conditions;
 - Generates error messages that provide information necessary for corrective actions without revealing any error code, personally identifiable information (PII), operating system (OS), IP addresses, Net-Bois names or information that is related to security or any administrative messages that could be exploited by adversaries; and
 - Reveals error messages only to authorized personnel.
-

**Information
Output
Handling and
Retention
(SI-12)**

PSA handles and retains both information within and output from the information systems in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

TECHNICAL- Access Control

**Policy
(AC-1)**

PSA develops, disseminates, and reviews/updates annually a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

**Account
Management
(AC-2)**

PSA manages information system accounts by:

- Identifying account types including individual, group, system, application, guest/anonymous, and temporary accounts;
- Establishing conditions for group membership;
- Identifying authorized users of the information system and specifying access privileges;
- Requiring appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling, and removing accounts;
- Authorizing and monitoring the use of specific guest/anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
- Deactivating temporary, terminated or transferred user accounts;
- Granting access based on authorization, intended system usage, or other attributes as required; and
- Reviewing accounts every fiscal quarter.

In addition PSA:

- Employs automated mechanisms to support the management of information systems accounts whenever possible;
 - Automatically terminates temporary and emergency accounts after 45-days of inactivity;
 - Disables inactive accounts after 45-days of inactivity; and
 - Automatically audits account creation, modification, disabling, and termination actions, and notify appropriate individuals as required.
-

**Access
Enforcement
(AC-3)**

PSA information systems enforce approved authorizations for logical access to the systems.

Continued on next page

TECHNICAL- Access Control, Continued

Least Privilege (AC-6) PSA employs the concepts of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions.

Unsuccessful Login Attempts (AC-7) PSA information systems apply the following regardless of whether the login occurs via a local or network connection:

- Enforces a limit of up to 10 consecutive invalid access attempts by a user during a 30 minutes period; and
 - Automatically locks the account until released by an administrator.
-

System Use Notification (AC-8) PSA information systems display an approved system use notification message before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

- Users are accessing a U.S. Government information system;
- System usage may be monitored, recorded, and subject to audit;
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
- Use of the system indicates consent to monitoring and recording.

The notification message remains on the screen until users take explicit actions to log on to or further access the information system. For publicly accessible systems:

- The system use information is displayed when appropriate before granting further access;
 - The display any references, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
 - The display includes a description of the authorized uses for the system.
-

Continued on next page

TECHNICAL- Access Control, Continued

Session Lock (AC-11)

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system as required that users log out at the end of the workday.

Additionally, PSA information systems:

- Prevent further access to the system by initiating a session lock after no more than 15 minutes of inactivity or upon receiving a request from a user; and
 - Retain the session lock until the user reestablishes access using established identification and authentication procedures.
-

Remote Access (AC-17)

PSA information systems:

- Document allowed methods of remote access to the information system;
- Establish usage restrictions and implementation guidance for each allowed remote access method;
- Monitor for unauthorized remote access to the information system;
- Authorize remote access to the information system prior to connection; and
- Enforce requirements for remote connections to the information system.

In addition, PSA employs automated mechanisms to facilitate the monitoring and control of remote access methods and uses cryptography to protect the confidentiality and integrity of remote access sessions.

Continued on next page

TECHNICAL- Access Control, Continued

Remote Access

Error! Not a valid bookmark self-reference.
(continued)

PSA's information system routes all remote accesses through a limited number of manages access control points, and;

- Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system;
- Authorizes users remote access based on the approval of user's request which has to be first approved by their respective supervisor and then users have to successfully complete on-line training upon which an RSA token is issued which authorizes the user remote access to the PSA information systems;
- Ensures that users protect information about remote access mechanisms from unauthorized use and disclosure;
- Ensures that remote sessions for accessing the network and other information systems employ two factor authentication when necessary and are audited; and
- Disables Hyper Text Transfer Protocol (http), File Transfer Protocol (ftp), peer to peer protocol, and telnet protocols except for explicitly identified components in support of specific operational requirements.

Wireless Access (AC-18)

PSA information systems protect wireless access to the system using authentication and encryption and also:

- Establishes usage restrictions and implementation guidance for wireless access;
- Monitors for unauthorized wireless access to the information system;
- Authorizes wireless access to the information system prior to connection; and
- Enforces requirements for wireless connections to the information system.

Access Control for Mobile Devices (AC-19)

PSA establishes usage restrictions and guidance for organization-controlled mobile devices.

PSA authorizes connection, monitors for unauthorized connections, and enforces requirements for the connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems.

Continued on next page

TECHNICAL- Access Control, Continued

(AC-19)
(AC-19)
(continued)

PSA also:

- Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
- Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
- Applies, inspects, and re-image mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Additionally, PSA:

- Restricts the use of writable, removable media in organizational information systems;
 - Prohibits the use of personally owned, removable media in organizational information systems; and
 - Prohibits the use of removable media in organizational information systems when the media has no identifiable owner.
-

**Use of External
Information
Systems**
(AC-20)

PSA establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- Access the information system from the external information systems; and
- Process, store, and/or transmit organization-controlled information using the external information systems.

In addition PSA:

Permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

- (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
- (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

PSA limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

Continued on next page

TECHNICAL- Access Control, Continued

Publicly
Accessible
Content
(AC-22)

PSA implements the following:

- Designates individuals authorized to post information onto an organizational information system that is publicly accessible;
 - Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
 - Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;
 - Annually reviews the content on the publicly accessible organizational information system for nonpublic information; and
 - Removes nonpublic information from the publicly accessible organizational information system, if discovered.
-

TECHNICAL- Audit and Accountability

Policy
(AU-1)

Each year PSA develops, disseminates reviews and/or updates of the audit and accountability policy.

Audit and accountability is designed to address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with FISMA regulations and NIST guidelines.

TECHNICAL- Identification and Authentication

Policy
(IA-1)

PSA develops, disseminates, and reviews/updates annually:

- A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Formal documented procedures to facilitate the implementation of the identification and authentication policy and associated controls.
-

Continued on next page

TECHNICAL- Identification and Authentication, Continued

Organizational and Users (IA-2) PSA's OIT uniquely identifies and authenticates organizational and non-organizational users (or processes acting on behalf of organizational and non-organizational users).

PSA information systems use multifactor authentication for network access to:

- Privileged accounts.
- Non-privileged accounts

PSA also uses:

- Multifactor authentication for local access to privileged accounts; and
 - One time authenticators for network access to privileged accounts.
-

Devices (IA-3) PSA information systems uniquely identify and authenticate PCs, laptops, and mobile devices before establishing a connection.

Identifier Management (IA-4) PSA manages information system identifiers for users and devices by:

- Receiving authorization from a designated organizational official to assign a user or device identifier;
- Selecting an identifier that uniquely identifies an individual or device;
- Assigning the user identifier to the intended party or the device identifier to the intended device;
- Preventing reuse of user or device identifiers for 5 years; and
- Disabling the user identifier after 45 days of inactivity.

Authenticator Management (IA-5) PSA manages information system authenticators for users and devices by:

Step	Action
1	Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.
2	Establishing initial authenticator content for authenticators defined by the Agency.
3	Ensuring authenticators have sufficient strength of mechanism for their intended use.

Continued on next page

TECHNICAL- Identification and Authentication, Continued

Authenticator Management
Error! Not a valid bookmark self-reference.
(continued)

Step	Action
4	Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
5	Changing default content of authenticators upon information system installation.
6	Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators, if appropriate.
7	Changing/refreshing authenticators every 90 days.
8	Protecting authenticator content from unauthorized disclosure and modification.
9	Requiring users to take and have devices implement specific measures to safeguard authenticators.

Additional Authenticator Procedures (IA-5)

Additional authenticator procedures include password-based authentication which:

- Enforces minimum password complexity of three types of lower-case and upper-case letters, numbers, and special characters (e.g., #, %, etc.).
- Enforces a minimum of 8 characters for newly created passwords;
- Encrypts passwords in storage and in transmission;
- Enforces password lifetime restrictions of 90 days; and
- Prohibits password reuse for 10 generations.

The information system, for PKI-based authentication:

- Validates certificates by constructing a certification path with status information to an accepted trust anchor;
- Enforces authorized access to the corresponding private key; and
- Maps the authenticated identity to the user account.

PSA's OIT requires that the registration process to receive user ID or network tokens to be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

Continued on next page

TECHNICAL- Identification and Authentication, Continued

Authenticator Feedback (IA-6) PSA's OIT obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

TECHNICAL- System and Communications Protection

Policy (SC-1) PSA develops, disseminates, and reviews/updates annually:

- A formal, documented system and communications protection for addressing the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- A formal, documented procedure to facilitate the implementation of the system and communications protection and associated system and communications protection controls.

Network Disconnect (SC-10) PSA information systems terminate the network connection associated with a communications session at the end of the session or after 15 minutes of inactivity.

Use of Cryptography (SC-13) PSA information systems implement required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Public Access Protections (SC-14) PSA information systems protect the integrity and availability of publicly available information and applications.

Collaborative Computing Devices (SC-15) PSA information systems:

- Prohibit remote activation of collaborative computing devices with the following exceptions: MS Office Live, WebEx, and Citrix; and
- Provide an explicit indication of use to users physically present at the devices.

Continued on next page

TECHNICAL- System and Communications Protection, Continued

**Voice over
Internet
Protocol
(SC-19)**

PSA's OIT:

- 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
 - Authorizes, monitors, and controls the use of VoIP within the information system.
-

PART II- Information Technology Staff

Applicability This section only applies to the Office of Information Technology.

MANAGEMENT- Planning

System Security Plan (PL-2) PSA's OIT develops, reviews and updates a security plan for the information system that:

- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

The security plan for the information system is reviewed annually, and updates to the plan are made to address changes to the information system/environment of operation or identify problems during plan implementation or security control assessments.

Security-Related Activity Planning (PL-6)

PSA plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

MANAGEMENT- Program Management

Plan of Action and Milestones (PM-4)	PSA implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.
Information System Inventory (PM-5)	PSA develops and maintains an inventory of its information systems.
Measures of Performance (PM-6)	PSA develops, monitors, and reports on the results of information security measures of performance.
Enterprise Architecture (PM-7)	PSA develops enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.
Critical Infrastructure Plan (PM-8)	PSA addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

MANAGEMENT- Security Assessment and Authorization

Plan of Action and Milestones (CA-5)	PSA's OIT: <ul style="list-style-type: none">• Develops a plan of action and milestones for the information systems to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and• Updates existing plan of action and milestones twice a year based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
---	--

Continued on next page

MANAGEMENT- Security Assessment and Authorization,

Continued

Continuous Monitoring (CA-7)

PSA's OIT establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

- A configuration management process for the information systems and its constituent components;
- A determination of the security impact of changes to the information system and environment of operation;
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
- Reporting the security state of the information system to appropriate organizational officials on an ongoing basis when feasible and least once a year.

MANAGEMENT- System Services and Acquisition

Life Cycle Support (SA-3)

PSA's OIT:

- Manages the information systems using a system development life cycle methodology that includes information security considerations;
- Defines and documents information systems security roles and responsibilities throughout the system development life cycle; and
- Identifies individuals having information systems security roles and responsibilities.

Information System Documentation (SA-5)

PSA's OIT obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:

- Secure configuration, installation, and operation of the information system;
- Effective use and maintenance of security features/functions; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

Continued on next page

MANAGEMENT- System Services and Acquisition, Continued

(SA-5)
(continued)

PSA's OIT obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:

- User-accessible security features/functions and how to effectively use those security features/functions;
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
- User responsibilities in maintaining the security of the information and information system.

PSA's OIT documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Security
Engineering
Principles
(SA-8)

PSA applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Developer
Configuration
Management
(SA-10)

PSA requires that information system developers/integrators:

- Perform configuration management during information system design, development, implementation, and operation;
 - Manage and control changes to the information system;
 - Implement only organization-approved changes;
 - Document approved changes to the information system; and
 - Track security flaws and flaw resolution.
-

Developer
Security
Testing
(SA-11)

PSA requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):

- Create and implement a security test and evaluation plan;
 - Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
 - Document the results of the security testing/evaluation and flaw remediation processes.
-

OPERATIONAL- Awareness and Training

Security Training (AT-3)	PSA provides role-based security-related training: <ul style="list-style-type: none">• Before authorizing access to the system or performing assigned duties;• When required by system changes; and• Every fiscal year thereafter.
---------------------------------	--

OPERATIONAL- Configuration Management

Baseline Configuration (CM-2)	<p>PSA's OIT develops, documents, and maintains under configuration control, a current baseline configuration of the information system.</p> <p>Additionally PSA: Reviews and updates the baseline configuration of the information system:</p> <ul style="list-style-type: none">• At least once every fiscal year;• When required due to incidents, upgrades and changes in security posture; and• As an integral part of information system component installations and upgrades. <p>Older versions of baseline configurations are retained as deemed necessary to support rollback. PSAs OIT develops and maintains a list of software programs that are authorized and those which are not authorized to be installed on the information systems (See: PSA approved list of Software Programs), and the installation of software is done through implementation of an allow-all, deny-by-exception authorization policy to identify PSA allowed software to execute on the information systems.</p>
Security Impact Analysis (CM-4)	PSA's OIT analyzes changes to the information system to determine potential security impacts prior to change implementation.
Access Restrictions for Change (CM-5)	PSA's OIT defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Continued on next page

OPERATIONAL- Configuration Management, Continued

Configuration Settings (CM-6) PSA's OIT incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. Additionally PSA:

- Establishes and documents mandatory configuration settings for information technology products employed within the information systems using DOD's Secure Technical Implementation Guides (STIG) that reflect the most restrictive mode consistent with operational requirements;
 - Implements the configuration settings;
 - Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
 - Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
-

Least Functionality (CM-7) PSA configures the information systems to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: http, ftp, telnet, peer-to-peer protocol, non-compliance passwords, IM, VOIP. Some of these functions may be turned on when necessary to provide such services to the enterprise.

In addition, PSA reviews the information systems annually or as needed to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Component Inventory (CM-8) PSA's OIT develops, documents, and maintains an inventory of information system components that:

- Accurately reflect the current information system;
 - Is consistent with the authorization boundary of the information system;
 - Is at the level of granularity deemed necessary for tracking and reporting;
 - Includes date of purchase, serial number, amount paid and warranty information of the product for property accountability; and
 - Is available for review and audit by designated organizational officials.
-

Continued on next page

OPERATIONAL- Configuration Management, Continued

**Component
Inventory
(CM-8)
(Continued)**

In addition PSA updates the inventory of information system components as an integral part of component installations, removals, and information system updates; and verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

**Configuration
Management
Plan
(CM-9)**

PSA's OIT develops, documents, and implements a configuration management plan for the information system that:

- Addresses roles, responsibilities, and configuration management processes and procedures;
 - Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
 - Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
-

OPERATIONAL- Contingency Planning

**Alternate
Storage Site
(CP-6)**

PSA's OIT:

- Establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.
 - Identifies an alternate storage site that is separate from the primary storage site so as not to be susceptible to the same hazards.
 - Identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
-

Continued on next page

OPERATIONAL- Contingency Planning, Continued

Alternate Processing Site (CP-7)

PSA's OIT:

- Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within 48 hours when the primary processing capabilities are unavailable; and
- Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the 48 to 72 hour time period for resumption.

In addition PSA:

- Identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.
 - Identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
 - Develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.
 - Ensures that the alternate processing site provides information security measures equivalent to that of the primary site.
-

Telecommunications Services (CP-8)

PSA establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within 48 to 72 hours when the primary telecommunications capabilities are unavailable.

PSA's OIT also:

- Develops primary and alternate telecommunications service agreements that contain priority of-service provisions in accordance with the organization's availability requirements; and
 - Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
 - PSA obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.
-

Continued on next page

OPERATIONAL- Contingency Planning, Continued

System Backup (CP-9) PSA's OIT conducts backups of :

- User-level;
- System-level;
- Information systems documentation; and
- Security-related

Information contained in the information systems at a minimum on a daily basis or real-time based on the agency's need. PSA's OIT also protects the confidentiality and integrity of backup information at the storage location. In addition PSA tests backup information every quarter to verify media reliability and information integrity.

Recovery and Reconstitution (CP-10) PSA provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

In addition PSA implements transaction recovery for systems that are transaction-based. Also provides compensating security controls for the systems that are victims of catastrophic failure or physical destruction.

OPERATIONAL- Incident Response

Incident Monitoring (IR-5) PSA tracks and documents information system security incidents.

Incident Response Plan (IR-8) PSA's OIT develops an incident response plan that:

- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall organization;
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;

Continued on next page

OPERATIONAL- Incident Response, Continued

Incident Response Plan (IR-8) (continued)

- Provides metrics for measuring the incident response capability within the organization.
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by designated officials within the organization.

In addition, copies of the incident response plan are distributed to the IT Security Incident Response Team which in turn;

- Reviews the incident response plan every two years;
- Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and

Communicates incident response plan changes to the IT Security Incident Response Team and Senior Management.

OPERATIONAL- Maintenance

Controlled Maintenance (MA-2)

PSA's OIT:

- Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
 - Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
 - Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
 - Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and
 - Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
-

Continued on next page

OPERATIONAL- Maintenance, Continued

**Controlled
Maintenance
(MA-2)
(continued)**

In addition, PSA keeps maintenance records for the information system that include:

- Date and time of maintenance;
- Name of the individual performing the maintenance;
- Name of escort, if necessary;
- A description of the maintenance performed; and

A list of equipment removed or replaced (including identification numbers, if applicable).

**Maintenance
Tools
(MA-3)**

PSA approves, controls, monitors, and maintains on an ongoing basis, information system maintenance tools. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. PSA also checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

**Non-local
Maintenance
(MA-4)**

PSA's OIT:

- Authorizes, monitors, and controls non-local maintenance and diagnostic activities;
- Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
- Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
- Maintains records for non-local maintenance and diagnostic activities; and
- Terminates all sessions and network connections when non-local maintenance is completed.

PSA audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. Also the organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.

Continued on next page

OPERATIONAL- Maintenance, Continued

**Maintenance
Personnel
(MA-5)**

PSA's OIT:

- Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and
 - Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
-

**Timely
Maintenance
(MA-6)**

PSA obtains maintenance support and/or spare parts for production level information systems within 24 hours of failure.

OPERATIONAL- Physical and Environmental Protection

**Physical Access
Authorization
(PE-2)**

PSA's OIT:

- Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
 - Issues authorization credentials;
 - Reviews and approves the access list and authorization credentials annually, removing from the access list personnel no longer requiring access.
-

Continued on next page

OPERATIONAL- Physical and Environmental Protection,

Continued

Physical Access Control (PE-3)	<p>PSA's OIT:</p> <ul style="list-style-type: none">• Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);• Verifies individual access authorizations before granting access to the facility;• Controls entry to the facility containing the information system using physical access devices and/or guards;• Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;• Secures keys, combinations, and other physical access devices;• Inventories physical access devices every two years; and• Changes combinations and keys annually and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
Control for Transmission Medium (PE-4)	<p>PSA controls physical access to information system distribution and transmission lines within organizational facilities.</p>
Monitoring Physical Access (PE-6)	<p>PSA's OIT:</p> <ul style="list-style-type: none">• Monitors physical access to the information system to detect and respond to physical security incidents;• Reviews physical access logs annually;• Coordinates results of reviews and investigations with the organization's incident response capability; and• Monitors real-time physical intrusion alarms and surveillance equipment.
Visitor Control (PE-7)	<p>PSA controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. The organization escorts visitors and monitors visitor activity, when required.</p>

Continued on next page

OPERATIONAL- Physical and Environmental Protection,

Continued

Access Records (PE-8)	PSA's OIT: <ul style="list-style-type: none">• Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and• Reviews visitor access records annually.
Power Equipment and Cabling (PE-9)	PSA protects power equipment and power cabling for the information system from damage and destruction.
Emergency Shutoff (PE-10)	PSA's OIT: <ul style="list-style-type: none">• Provides the capability of shutting off power to the information system or individual system components in emergency situations;• Places emergency shutoff switches or devices in data centers and computer rooms to facilitate safe and easy access for personnel; and• Protects emergency power shutoff capability from unauthorized activation.
Emergency Power (PE-11)	PSA 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.
Emergency Lighting (PE-12)	PSA employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
Fire Protection (PE-13)	PSA employs and maintains fire suppression and detection devices/systems for the information systems that: <ul style="list-style-type: none">• Are supported by an independent energy source;• Activate automatically and notify the organization and emergency responders in the event of a fire;• Provide automatic notification of any activation to the organization and emergency responders; and• Are in a facility which may not be staffed on a continuous basis.

Continued on next page

OPERATIONAL- Physical and Environmental Protection,

Continued

Temperature and Humidity Controls (PE-14)	PSA's OIT maintains and monitors temperature and humidity levels within the facility where the information systems reside at the recommended level of 72 degrees Fahrenheit and 40% humidity.
--	---

Water Damage Protection (PE-15)	PSA protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
--	--

Delivery and Removal (PE-16)	PSA authorizes, monitors, and controls all hardware entering and exiting the facility and maintains records of those items via inventory databases and all software is kept in secure file cabinets.
-------------------------------------	--

Location of Components (PE-18)	PSA positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
---------------------------------------	---

OPERATIONAL- System and Information Integrity

Flaw Remediation (SI-2)	<p>PSA's OIT:</p> <ul style="list-style-type: none">• Identifies, reports, and corrects information system flaws;• Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and• Incorporates flaw remediation into the organizational configuration management process.
--------------------------------	--

PSA employs automated mechanisms on a continuous or weekly basis to determine the state of information system components with regard to flaw remediation.

Continued on next page

OPERATIONAL- System and Information Integrity, Continued

Malicious Code Protection (SI-3)

PSA's OIT employs, updates, and configures malicious code protection mechanisms. Code protection mechanisms are used at entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code that is:

- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities.

Malicious code protection mechanisms are updated (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.

Malicious code protection mechanisms are configured to:

- Perform periodic scans of the information system on a weekly basis and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- Block, clean, or quarantine malicious code based on its severity. Once an alert is received, the system tries to clean the infected host; or the host is taken down to remediate the threat.

Malicious code detection addresses the receipt of false positives and implements eradication resulting in minimizing the potential impact on the availability of the information system.

PSA centrally manages malicious code protection mechanisms and prevents non-privileged users from circumventing malicious code protection capabilities.

Information System Monitoring (SI-4)

PSA's OIT:

- Monitors, detects and eradicates events on the information system in real-time against intrusion and unauthorized access. The information system provides real-time alerts when the system is compromised with malware, malicious code, viruses, or intrusion attacks;
 - Identifies unauthorized use of the information system;
 - Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
-

Continued on next page

OPERATIONAL- System and Information Integrity, Continued

**Information
System
Monitoring
(SI-4)
(Continued)**

- Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and
- Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

PSA employs automated tools to support near real-time analysis of events, and monitors inbound and outbound communications for unusual or unauthorized activities or conditions. The information system provides near real-time alerts when it detects malware, malicious code, viruses, or intrusion attacks and PSA prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

**Security Alerts,
Advisories, and
Directives
(SI-5)**

PSA's OIT:

- Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
 - Generates internal security alerts, advisories, and directives as deemed necessary;
 - Disseminates security alerts, advisories, and directives to IT Security and Network infrastructure teams; and
 - Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
-

**Software and
Information
Integrity
(SI-7)**

PSA information systems detect unauthorized changes to software and information. PSA reassesses the integrity of software and information by performing daily integrity scans of the information system.

TECHNICAL- Access Control

**Information
Flow
Enforcement
(AC-4)**

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization and not passing any web requests to the Internet that are not from the internal web proxy.

Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems.

Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls.

**Separation of
Duties
(AC-5)**

PSA separates duties as follows:

- Duties of individuals as necessary, to prevent malevolent activity without collusion;
- Documents separation of duties; and
- Implements separation of duties through assigned information system access authorizations.

Examples of separation of duties:

1. Mission functions and distinct information system support functions are divided among different individuals/roles;
 2. Different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security);
 3. Security personnel who administer access control functions do not administer audit functions; and
 4. Different administrator accounts for different roles.
-

Continued on next page

OPERATIONAL- System and Information Integrity, Continued

**Permitted
Actions without
Identification
or
Authentication
(AC-14)**

PSA identifies specific user actions that can be performed on the information system without identification or authentication in order to recover data from non-functional systems or in an isolated situation. PSA documents and provides supporting rationale in the security plan for the information system user of actions not requiring identification and authentication.

In addition, PSA permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives, (i.e., recovery of lost information).

TECHNICAL- Audit and Accountability

**Auditable
Events
(AU-2)**

Based on risk assessment and mission/business needs, PSA determines that the information system must be capable of auditing the following events:

- Successful and unsuccessful network log in/log out,
- File/data creation, update, and deletes

PSA's OIT coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events.

PSA's OIT provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents, and also determines, based on current threat information and ongoing assessment of risk, that the following events: successful and unsuccessful network/systems login/logout are to be audited within the information system semi-annually.

Continued on next page

TECHNICAL- Audit and Accountability, Continued

**Auditable
Events (AU-2)
(continued)**

In addition PSA:

- Reviews and updates the list of auditable events annually or as needed to balance auditing requirements with other information system needs. This control also requires identifying that subset of auditable events that are to be audited at a given point in time in systems such as 'Database Management System' where roles such as "Delegation" is assigned. Auditable events in the case of a database management system are the individual operations initiated by an untrusted user (e.g., updates, retrievals, inserts) and not just the invocation of the database management system; and
 - Includes execution of privileged functions such as a user with the auditor role is required to enable and configure the security auditing subsystem wherein the auditor role is separate from the authority of the administrator by requiring them to have separate privileges.
-

**Content of
Audit Records
(AU-3)**

PSA information systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

In addition, the information systems include whenever possible a copy of the record in its previous state. PSA keeps copies of the record since its inception in the audit records for audit events identified by type, location, or subject.

**Audit Storage
Capacity
(AU-4)**

PSA allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

**Response to
Audit
Processing
Failures
(AU-5)**

PSA information systems alert designated organizational officials in the event of an audit processing failure and take the following additional actions: Shut down information system; export and review existing logs; or over-write the oldest audit records.

Continued on next page

TECHNICAL- Audit and Accountability, Continued

Audit Review, Analysis and Reporting (AU-6) PSA reviews and analyzes information system audit records on an as needed basis, and at least twice a year for indications of inappropriate or unusual activity, and reports the findings to designated organizational officials.

PSA also adjusts when necessary, the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Audit Reduction and Report Generation (AU-7)

PSA information systems provide an audit reduction and report generation capability. In addition, PSA information systems provide the capability to automatically process audit records for events of interest based on selectable event criteria.

Time Stamps (AU-8)

PSA information systems use internal system clocks to generate time stamps for audit records. In addition, the information system synchronizes internal information system clocks on a real-time basis with the main Domain Controller server.

Protection of Audit Information (AU-9)

PSA information systems protect audit information and audit tools from unauthorized access, modification, and deletion.

Audit Record Retention (AU-11)

PSA retains audit records for at least one year after generation to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Continued on next page

TECHNICAL- Audit and Accountability, Continued

**Audit
Generation
(AU-12)**

PSA information systems:

- Provide audit record generation capability for the list of auditable events defined previously at the server level and/or transaction level in the case of database systems;
 - Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
 - Generate audit records for the list of audited events with the content of audit records.
-

TECHNICAL- Identification and Authentication

**Cryptographic
Module
Authentication
(IA-7)**

PSA's OIT uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

**Identification
and
Authentication
(Non-
Organizational
users) (IA-8)**

PSA information systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

TECHNICAL- System and Communications Protection

**Application
Partitioning
(SC-2)**

PSA's OIT separates user functionality (including user interface services) from information system management functionality.

**Information in
Shared
Resources
(SC-4)**

PSA's OIT prevents unauthorized and unintended information transfer via shared system resources.

Continued on next page

TECHNICAL- System and Communications Protection,

Continued

**Denial of
Service
Protection
(SC-5)**

PSA's OIT protects the internal network from recognized or suspected denial of service attacks based on firewall that recognizes signatures which are updated regularly.

**Boundary
Protection
(SC-7)**

PSA information systems:

- Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; and
- Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

In addition PSA's OIT:

- Physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces;
 - Prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices; and
 - Limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.
-

Continued on next page

TECHNICAL- System and Communications Protection,

Continued

**Boundary
Protection
(SC-7)
(Continued)**

There is also:

- Implementation of a managed interface for each external telecommunication service;
- Establishment of a traffic flow policy for each managed interface;
- Employment of security controls as needed to protect the confidentiality and integrity of the information being transmitted;
- Documentation of each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- A review of exceptions to the traffic flow policy annually; and
- Removal of traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

**Transmission
Integrity
(SC-8)**

PSA's OIT protects the integrity of transmitted information. In addition, PSA employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

**Transmission
Confidentiality
(SC-9)**

PSA information systems protect the confidentiality of transmitted information. In addition, PSA employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by lockbox mechanism.

**Cryptographic
Key
Establishment
& Management
(SC-12)**

PSA establishes and manages cryptographic keys for required cryptography employed within the information system.

Continued on next page

TECHNICAL- System and Communications Protection,

Continued

**Public Key
Infrastructure
Certificates
(SC-17)**

PSA obtains public key certificates under an appropriate certificate policy from an approved service provider.

**Mobile Code
(SC-18)**

PSA's OIT:

- Defines acceptable and unacceptable mobile code and mobile code technologies;
- Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- Authorizes, monitors, and controls the use of mobile code within the information system.

**Secure
Name/Address
Resolution
Service
(SC-20)**

PSA's OIT provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

In addition, PSA information systems, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

PSA's OIT collectively provide name/address resolution services that are fault-tolerant and implement internal/external role separation.

Continued on next page

TECHNICAL- System and Communications Protection,

Continued

**Architecture
and
Provisioning
for
Name/Address
Resolution
Service
(SC-22)**

PSA information systems that collectively provide name/address resolution services are fault-tolerant and implement internal/external role separation.

**Session
Authenticity
(SC-23)**

PSA information systems provide mechanisms to protect the authenticity of communications sessions.

**Protection of
Information at
Rest
(SC-28)**

PSA information systems protect the confidentiality and integrity of information at rest.

**Information
System
Partitioning
(SC-32)**

PSA partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

Control Locator Index

PART I- ENTIRE PSA STAFF

Management Controls (PL-1); (PL-4); (PL-5);
(PM-1); (PM-2); (PM-3); (PM-9); (PM-10); (PM-11);
(RA-1); (RA-2); (RA-3); (RA-5);
(CA-1); (CA-2); (CA-3); (CA-6);
(SA-1); (SA-2); (SA-4); (SA-6); (SA-7); (SA-9)

Operational Controls (AT-1); (AT-2); (AT-4);
(CM-1); (CM-3);
(CP-1); (CP-2); (CP-3); (CP-4);
(IR-1); (IR-2); (IR-3); (IR-4); (IR-6); (IR-7);
(MA-1);
(MP-1); (MP-2); (MP-3); (MP-4); (MP-5); (MP-6);
(PS-1); (PS-2); (PS-3); (PS-4); (PS-5); (PS-6); (PS-7); (PS-8);
(PE-1); (PE-5); (PE-17);
(SI-1); (SI-8); (SI-9); (SI-10); (SI-11); (SI-12)

Technical Controls (AC-1); (AC-2); (AC-3); (AC-6); (AC-7); (AC-8); (AC-11); (AC-17);
(AC-18); (AC-19); (AC-20); (AC-22);
(AU-1);
(IA-1); (IA-2); (IA-3); (IA-4); (IA-5); (IA-6);
(SC-1); (SC-10); (SC-13); (SC-14); (SC-15); (SC-19)

PART II- IT STAFF ONLY

Management Controls (PL-2); (PL-6);
(PM-4); (PM-5); (PM-6); (PM-7); (PM-8);
(CA-5); (CA-7);
(SA-3); (SA-5); (SA-8); (SA-10); (SA-11)

Continued on next page

Control Locator Index, Continued

PART II- IT STAFF ONLY

Operational Controls	(AT-3); (CM-2); (CM-4); (CM-5); (CM-6); (CM-7); (CM-8); (CM-9); (CP-6); (CP-7); (CP-8); (CP-9); (CP-10); (IR-5); (IR-8); (MA-2); (MA-3); (MA-4); (MA-5); (MA-6); (PE-2); (PE-3); (PE-4); (PE-6); (PE-7); (PE-8); (PE-9); (PE-10); (PE-11); (PE-12); (PE-13); (PE-14); (PE-15); (PE-16); (PE-18); (SI-2); (SI-3); (SI-4); (SI-5); (SI-7)
Technical Controls	(AC-4); (AC-5); (AC-14); (AU-2); (AU-3); (AU-4); (AU-5); (AU-6); (AU-7); (AU-8); (AU-9); (AU-11); (AU-12); (IA-7); (IA-8); (SC-2); (SC-4); (SC-5); (SC-7); (SC-8); (SC-9); (SC-12); (SC-17); (SC-18); (SC-20); (SC-22); (SC-23); (SC-28); (SC-32)
