**1. SYSTEM IDENTIFICATION**

**1.1. System Name/Title:** Alpha Beta Program (ABP) System

**1.1.1. System Categorization** (FIPS 199 overall System impact) **– Moderate Impact**

**1.1.2. System Unique Identifier: 111-01**

Note**:** The System UID consists of five numeric characters (xxx-xx) assigned by the Information Assurance Division. The first three characters will correspond to the System Owner OU/Division.

**1.2. Responsible Organization:**

|  |  |
| --- | --- |
| Name: | Alpha Beta Corporation |
| Address: |  |
| Phone: |  |

**1.2.1. Information Contacts:**

**1.2.1.1. Authorizing Official (Designated Approving Authority):**

|  |  |
| --- | --- |
| Name: | John Smith |
| Title: | ABC Chief Information Officer |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

**1.2.1.2. Co-Authorizing Official:**

|  |  |
| --- | --- |
| Name: | Joe Smith |
| Title: | Director, Alpha Beta Program |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

**1.2.1.3. ABC Operating Unit IT Security Officer:**

|  |  |
| --- | --- |
| Name: | Mary Waters |
| Title: | Information Technology Specialist |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

**1.2.1.4. System Owner:**

|  |  |
| --- | --- |
| Name: | Joanna Myers |
| Title: | Alpha Beta Manager |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

**1.2.1.5. Primary Information Contact:**

|  |  |
| --- | --- |
| Name: | Mary Smith |
| Title: | Information Technology Specialist |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

**1.2.1.6. Secondary Information Contact:**

|  |  |
| --- | --- |
| Name: | N/A |
| Title: |  |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

**1.2.2. Information System Security Officer (ISSO)** (assignment of security responsibility)**:**

|  |  |
| --- | --- |
| Name: | Mary Smith |
| Title: | Information Technology Specialist |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

**1.3. System Operational Status:**

Operational  Under Development  Major Modification  Retired

If the system is under development or undergoing a major modification, include a schedule for the system design, development, implementation, and operational phases.

**1.4. General Description/Purpose of System:**

a) What is the function/purpose of the system?

**The function/purpose of the system is to support the electronic needs and activities of the internal and external customers. These activities include providing structured database access by ABC staff within ABC Business environment to information relevant to the processes related to the Alpha team activities. Shared files and print services are available to staff members.**

**External customers interested in applying to become a Alpha Reviewer access the OCIO hosted web-based Alpha Reviewer Applicant (ARA). Further details are provided in Section 1.5 of this Document.**

**Contract information for the Alpha system is outsourced to EXT in Branson, MS. Further details are provided in Section 1.5 of this document and in the EXT subsystem SSP.**

**The Alpha Beta Program presents the Alpha Technology Innovation Award to businesses. These Reviewers use an online scorebook called Alpha Beta Program Solution (ABPS).**

**ABPS is utilized to evaluate and score applications online.  It makes the review and scoring process more efficient, while centralizing the storage of data and allowing for the proper monitoring and guidance of the Reviewer’s work in a secure manner.**

b) User Population served (i.e. all of ABC, all or part of a given OU, all or part of a given division within an OU, internal researchers, external researchers, administrative officers, the general public, etc.)**:**

**User Population(s) Served:**

|  |  |
| --- | --- |
| **User Population Served** | **Internal or External?** |
| Internal administrative, management, and staff personnel | Internal |
| External reviewers | External |
| Award applicants | External |

c) Number of end users and privileged users:

**Roles of Users and Number of Each Type:**

|  |  |
| --- | --- |
| **Number of Users** | **Number of Administrators/**  **Privileged Users** |
| 600 | 20 for ABPS |

**There are 3 DBAs for the SQL databases maintained within SSP 111-02.**

**There are 3 system administrators for the ABPS and ARA applications.**

**There are 3 application managers for the ABPS and ARA applications.**

**There is a Primary Alpha System Administrator that has the following responsibilities:**

* **Information System Security Officer (ISSO) for the Alpha system.**
* **System administrator for the Alpha file server.**
* **Administrator for the Alpha OU on the ABC organization Active Directory structure (SSP 111-03) who manages user accounts, group memberships, and computer accounts).**
* **System administrator for desktop support activities in coordination with the OCIO desktop support team.**

**Also refer to the System Support section (1.5 f) for more details regarding the privileged users/support staff.**

d) How does the system fulfill ABC mission requirements?

**Alpha Beta Program’s mission is to enhance the technical innovation of U.S. organizations for the benefit of all residents.**

e) Exhibit 53/300 Account Code**:**

**1.5. System Environment:**

(See ABC SP 800‑18 for more information on this classification):

**Standalone or Small Office/Home Office (SOHO)** (encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems)

**Managed/Enterprise** (systems with defined, organized suites of hardware and software configurations, usually consisting of centrally-managed workstations and servers protected from the Internet by firewalls and other network security devices)

**Custom - Specialized Security-Limited Functionality** (environment contains systems and networks at high risk of attack or data exposure, with security taking precedence over functionality)

**Custom – Legacy** (older machines or applications that may use older, less-secure communication mechanisms)

**Cloud –** Systems using access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) provided by a third party (outside ABC.)

a) Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and KEY devices within it. (Note**:** *this does not require depicting every workstation or desktop*, but you must include an instance for each operating system in use, an instance for portable components (if applicable), **all** **servers**, (file, print, web, database, application, etc.) as well as any networked workstations, (e.g., Unix, Windows, Mac, Linux Desktops) firewalls, routers, switches, copiers, printers, lab equipment, handhelds, etc.) If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote system boundaries by referencing the security plan number of other system(s) in the diagram.

**The system diagram is included within this Security Assessment and Authorization (A&A) package.**

**Alpha Beta Program system components plug into switches. The switches uplink to the Bldg. 800 Cisco Router and the router uplinks to the redundant backbone.**

**Alpha Beta Program consists of the following components. The Alpha Beta Program will be referred to as “Alpha” throughout this document.**

1. **AlphaFS (M/M/L)**

**There is a Windows 2008R2 Server within the ABC domain that serves as file server. The file server maintains shared files for the Alpha staff. Access to shared directories and files is managed through Active Directory group membership and associated file level and share level permissions. The AlphaFS server is also a print server for networked printers for all Alpha staff to use.**

1. **External Facing ABC Hosted Web Applications**

**ABPS Application (M/M/L)- A secure web application hosted on ABPSprod with the server and OS completely maintained by the OCIO staff under SSP 111-03. The server is physically located in the ABC DATA CENTER (SSP 111-03) and logically located in the Public Network behind the Admin firewall. Access from the internet is directed through a reverse proxy device (SSP 111-03). The development server, ABPSwebdev sits in the Business network.**

**The OCIO manages the Physical Environment, Hardware, Operating System and Software (SSP 111-03). Please refer to the AC section of this document as well as the SLA on file if needed. Access is provided based on the Reviewer’s assignment to a specific applicant and their specific information.**

**For ABPS Application, users access ABC resources through this secure web application and would normally be required to have an external user account, but a waiver has been granted through the OCIO Director.**

**Alpha Public Website (L/L/L) – 111-01 staff members also provide input for the Alpha public website. This is a content Management System (CMS) maintained completely by OCIO, where designated Alpha staff have the rights to post and manage.**

**Alpha Reviewer Applicant (ARA) website (M/M/L): This site allows potential Alpha external users to complete an online application. It also includes an internal portion that is used to administer the site and review the applicants. The data that is collected is similar to information that would be included in an employment résumé. ARA is hosted on ARAprod with the server and OS completely maintained by the OCIO staff under SSP 111-03. The server is physically located in the ABC DATA CENTER (SSP 111-03) and logically located behind a firewall (SSP 111-05). Access from the internet is directed through a reverse proxy device (SSP 111-03). The development server, ARAwebdev (SSP 111-03) sits on the Test/Dev network.**

**The site is hosted in the ABC Public network since some of the data collected is rated at a moderate level. A network diagram has been provided to show the exact architecture. The records are only available in the Public Network temporarily, and then they are purged and only available within the OCIO managed internal database (SSP 111-03 HW and SSP 111-02 DB).**

1. **Windows laptops with docking stations and desktop workstations (M/M/L)**

**Workstations and laptops are attached to the network and run Windows 7 and 10 as the Operating Systems. These workstations are part of the Desktop plan, and are managed by the services provided in (SSP 111-04). The Alpha Primary System Administrator has been given administrative privileges for the Alpha OU on the ABC Domain Active Directory structure (SSP 111-03). All users login at all times with their Central account with their Personal Identity Verification (PIV) card. All networked machines receive their IP addresses from OCIO DHCP implementation, DHCP.**

1. **MAC OS Workstation and laptops (M/M/L)**

**These Mac OSs are attached to the network and are part of the OCIO Desktop (SSP 111-04) environment. The users of the Mac OS assets have system administrative rights for their own machines. These assets are used to host specialized applications for designing graphics, brochures, etc. Software inventories for these components are provided in the Software Inventory document. The Mac OS laptops have Checkpoint full disc encryption. Users log in with their ABC Central account.**

1. **Mobile Devices (L/L/L)**

**There are two IPhones and four IPads in use. See the Asset Inventory for details. All are managed under SSP 111-04.**

1. **Network Printers (M/M/L)**

**Network Printers are accessed by all Alpha staff members within the Alpha subnet.**

1. **SQL Database Services (M/M/L)**

**There is a SQL database hosted under (SSP 111-02) that maintains a majority of the Alpha system data. The Alpha staff use SQL client software to connect to the database and run queries.**

1. **There is one external subsystem for this system**

**EXT (M/M/L) is an outsourced, offsite subsystem and provides services ABPS. The subsystem resides in a datacenter in Branson, Missouri.**

b) Include or reference a **complete and accurate** listing of all hardware (a reference to the asset inventory system and/or Desktop asset inventory is acceptable) and software (system software and application software) components, including make/OEM, model, version, and service packs.

**The system asset inventory is included within the Security Assessment and Authorization (A&A) package.**

c) Software category for **all types** of software installed within the boundaries of this system must be documented. List all applications supported by the general support system.

**This information is provided in the system software inventory included within this Security Assessment and Authorization package.**

d) Hardware and Software Ownership - Is all hardware and software government owned? **No**

If no, explain: **Subsystem components are not government owned. See the subsystem SSP EXT.**

e) General Location of System Components (see the asset inventory for specific component buildings/rooms) –

**Location of System Components**

|  |  |  |
| --- | --- | --- |
| **ABC Facility** | **Contractor Facility** | **Other (explain)** |
| **All Parent System Components** | **See subsystem SSP EXT.** | **N/A** |

f) System Support –

|  |  |
| --- | --- |
| **Government Supported** | **Contract Staff Supported** |
| **Both** | |

g) Detail any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, externally hosted data, Software as a Service, and Cloud Computing, etc.

**Users of this system include reviewers who are selected to review award applications. They in turn have controlled access to award applicant documents.**

**1.6. System Interconnections/Information Sharing:**

NOTE**:** ABC SP 800-18 defines a system interconnection as a “**direct** connection of two or more IT systems for the purpose of sharing information resources.”

a) A detailed discussion of system connectivity -- where data goes out and who/what is authorized to come in, name(s) of interconnected system(s), type of interconnection(s), sensitivity levels of the interconnected system(s), and any security concerns and rules of behavior of the other system(s) that need to be considered in the protection of this system. Include a discussion of ALL connections to other systems not governed by this security plan, including untrusted connections or connections to the Internet that require protective devices as a barrier to unauthorized system intrusion.

**All system connectivity is via TCP/IP across the ABC Network Business (SSP 111-05). The Network Business system provides all services for physical cabling, network frame synchronization/flow control/error checking, routing, switching, and DNS.**

**OCIO’s DHCP service is used to provides IP Addresses for all the Windows and Mac OS desktop machines on this subnet. All staff networked machines are assigned an IP address through DHCP reservation. All addresses in the DHCP scope are on the Alpha subnet. DHCP lease duration is 90 days.**

**Alpha does not have any direct interconnections with the subsystem contractor EXT. All data communications are done via encrypted email, ABC ncryptfiles encrypted file sharing, or Federal Express (FedEx) protected mail.**

b) In the table below, list system connections and check the appropriate box as to whether each connection is/are government-to-government (G2G), government-to-business (G2B), or government-to-citizen (G2C). Describe the controls to allow and restrict public access.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Connection**  **(Sys ID # if ABC system or description if external)** | **G2G** | **G2B** | **G2C** | **Is the Connection Trusted?** |
| 111-02 | √ |  |  | Yes |
| 111-03 | √ |  |  | Yes |
| 111-04 | √ |  |  | Yes |
| 111-05 | √ |  |  | Yes |
| 111-06 | √ |  |  | Yes |
| 111-07 | √ |  |  | Yes |
| EXT |  | √ |  | Yes |

If the system includes trusted connections (e.g. connections that do not require barrier protection devices such as firewalls), discuss why the connection is trusted.

**The ABC Network Business system and the ABC Network Security system are trusted connections because they are operated by ABC and are fully authorized to operate by the ABC CIO.**

c) Reference here and attach a full copy of all Interconnection Security Agreements (ISA) and Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA) for provision of IT security for this connectivity. Other relevant ABC security plans may also be referenced. Note: ABC SP 800-18 does NOT require an ISA/MOU/A with owners of internal agency systems (i.e. internal to ABC).

**1.7. Applicable Laws and Regulations Affecting the System:**

1. The system is subject to the DOC IT Security Program Policy and Minimum Implementation Standards along with the IT security laws and federal regulations including:

[**Public Law 107-347 E-Government Act of 2002**](http://www.nist.gov/director/ocla/Public_Laws/PL107-347.pdf) **(FISMA included)**

**Public Law 200-253 Computer Security Action of 1987**

[**OMB Circular No. A-130, Appendix III, Security of Automated Information Resources**](http://www.whitehouse.gov/omb/rewrite/circulars/a130/a130.html)

[**Department of Commerce Administrative Orders**](http://dms.osec.doc.gov/cgi-bin/doit.cgi?218:112:1:2)

**ABC SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE**

**ABC Administrative Manual Chapter 11.02 and the ABC IT Security Management Handbook**

Do any additional laws or regulations apply specifically to this system? **No**

If yes, list them here:

1. Privacy Act – **See ABC Privacy Controls; Privacy Impact and Risk Assessment (AR-2).**

**1.8 General Description of Information and System Sensitivity/Impact:**

FIPS 199 and ABC SP 800-60 Rev 1 were used to determine all system impact levels.

a) All 800-60 information/data types processed on the system (such as D.20.1 - Research and Development Information, or C.2.8.9 - Personal Identity and Authentication Information) must be determined and documented.

The impact designation of the system or the application is a reflection of the data types that are resident on the system or managed by the application.

**C.2.3.1 - Budget Formulation Information (L/L/L)**

**C.2.8.9 - Personal Identity and Authentication Information (M/M/L)**

**C.3.1.4 - Travel Information (L/L/L)**

**C.3.2.3 - Budget and Finance Information (M/M/L)**

**C.3.5.1 – System Development Information (L/M/L)**

**C.3.5.4 - IT Business Maintenance Information (M/L/L)**

**D.9.1 - Business and Industry Development Information (L/L/L)**

**D.9.2 - Intellectual Property Protection Information (M/L/L)**

**Confidentiality, Integrity, and Availability Value Guideline** (based on FIPS 199)

|  |  |
| --- | --- |
| **Impact Level** | **Level Definition** |
| High | Severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals such as  loss of life, e.g. due to faulty research or faulty calibrations. |
| Moderate | Serious adverse effect on organizational operations, organizational assets, or individuals such as  loss of reputation or customer trust, loss of external funding, loss of confidence in data, loss of critical equipment. |
| Low | Limited adverse effect on organizational operations, organizational assets, or individuals such as  inconvenience or loss of equipment. |

b) What would the risk of harm be (how would the ABC mission be affected) if the Confidentiality, Integrity, or Availability of the information processed was compromised?

**Proprietary business and personal information and conflict of interest data on Alpha applicants and Reviewers are collected and entered into the databases and stored in files on the network. Unauthorized disclosure could result in loss of public confidence and impact program integrity perceptions. Incorrect (loss of integrity) data could result in the same consequence.**

c)

|  |  |  |
| --- | --- | --- |
| **Security Objective** | **Impact Rating** | **Short Description of Basis for Rating** |
| Confidentiality | **Moderate** | Proprietary business and personal information and conflict of interest data on Alpha applicants and Reviewers are collected and entered into the databases and stored in files on the network. Unauthorized disclosure could result in loss of public confidence and impact program integrity perceptions. |
| Integrity | **Moderate** | Unauthorized or unexpected changes to applicant-specific proprietary information (e.g., information contained in feedback reports) could result in loss of public confidence and impact program integrity perceptions. |
| Availability | **Low** | Users’ reliance on calendars, email, network storage, and web access to information and communications. There would be a limited adverse effect if the system were unavailable. The Program’s mission would not be impacted significantly by short-term outages (10 working days). Contingency planning would include disaster recovery procedures and/or system outage emergency planning. |

(Editorial Legend for Baseline of controls based on ABC SP 800‑53 rev. 4, April 2013)

**Control Family Quick Links**

[2. REQUIRED SECURITY CONTROLS 13](#_Toc366067568)

[2.1 Access Control (AC) 13](#_Toc366067569)

[2.2 Awareness and Training (AT) 23](#_Toc366067570)

[2.3 Audit and Accountability (AU) 24](#_Toc366067571)

[2.4 Security Assessment and Authorization (CA) 30](#_Toc366067572)

[2.5 Configuration Management (CM) 34](#_Toc366067573)

[2.6 Contingency Planning (CP) 41](#_Toc366067574)

[2.7 Identification and Authentication (IA) 47](#_Toc366067575)

[2.8 Incident Response Capability (IR) 52](#_Toc366067576)

[2.9 Maintenance (MA) 56](#_Toc366067577)

[2.10 Media Protection (MP) 59](#_Toc366067578)

[2.11 Physical and Environmental Protection (PE) 63](#_Toc366067579)

[2.12 Planning (PL) 69](#_Toc366067580)

[2.13 Personnel Security (PS) 72](#_Toc366067581)

[2.14 Risk Assessment (RA) 76](#_Toc366067582)

[2.15 System and Services Acquisition (SA) 79](#_Toc366067583)

[2.16 System and Communication Protection (SC) 84](#_Toc366067584)

[2.17System and Information Integrity (SI) 90](#_Toc366067585)

2. REQUIRED SECURITY CONTROLS

[2.1 Access Control (AC)](#TOC)

[AC-1](#TOC), **Access Control Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to: **Assignment:** System Owner, Information System Security Officer(s), privileged users] an Access Control Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Access Control Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[AC-1](#TOC), **Access Control Procedures:** (Hybrid)

The organization:

1. Develops, documents, and disseminates to **Assignment:** System Owner, Information System Security Officer(s), privileged users the Procedures to facilitate the implementation of the Access Control Policy and associated access controls; and
2. Reviews and updates the current Access Control Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific** – **All provided in this SSP**

**\*\*Note for the Account Management Controls: ABC Central accounts (SSP 111-03) are used for the following components. Any time the response includes ABC Central accounts include the following components:**

* **Windows Server**
* **Windows Workstations**
* **Mac OS Workstations and Laptops**
* **Mobile Devices managed under SSP 111-04**
* **SQL Database access**

**System Specific procedures are found in AC-2 through AC- 22.**

**Account Management Waiver for Alpha Reviewers (In the “Waivers” folder under 111-01)**

[AC-2](#TOC), **Account Management:** (Hybrid)

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: *[****Assignment:*** *organization-defined information system account types];*

**ABC Central Accounts: Administrator for the Alpha OU on the ABC organization Active Directory structure manages user accounts, group memberships, and computer accounts. This includes group memberships and all authorizations**.

**ABPS Application: Role-based access is used where each user is assigned to a specific role that has predetermined level of access to the website. Role-assignments are granted by the ITSO and ABPS project lead.**

**ARA External User Application: The external website allows new users to create their own account in order to enter their application information.**

**ARA & ABPS Internal Management Applications: The internal website accounts use the OCIO approved LDAP and allow the Alpha Applicant administrators to grant the proper roles to the user. There are 15 available roles and account and role management all use the same procedures as the previously authorized ABPS website.**

1. Assigns account managers for information system accounts;

**All associated authorizations are overseen by the ITSO as authorized by the System Owner.**

1. Establishes conditions for group and role membership;

**described in a).**

1. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

**Well defined as listed in a)**

1. Requires approvals by [***Assignment:*** *organization-defined personnel or roles*] for requests to create information system accounts;

* **ABC Central Accounts: Administrator for the Alpha OU on the ABC organization Active Directory structure (manages User Accounts, Group memberships, and computer accounts). This management includes establishing, activating, modifying, reviewing, disabling, and removing accounts.**
* **ABPS Application accounts are created after the ARA applicant cycle is over. The System Administrator has privileges within the ABPS Application including establishing, activating, modifying, reviewing, disabling, and removing accounts.**

**There is also a test environment that is used for testing updates to the application and also for training purposes. This application is accessed by trainees that attend on-site training at ABC but contains no sensitive data, only training data.**

**ABPS also maintains an internal component that is accessed by Alpha staff to administer the external portion, this configuration is the same as ARA.**

* **ARA: Applicants create their own accounts through the account creation process. This entails the user entering their data into the application and waiting for an email. Beyond the creation process, accounts are managed the same way as ABPS accounts.**

1. Creates, enables, modifies, disables, and removes information system accounts in accordance with [***Assignment:*** *ABC O 605 00 IT User Account Management Policy*];

**See e)**

1. Monitors the use of, information system accounts;

**Logging is enabled to monitor the use of accounts as described in the AU control family.**

1. Notifies account managers:
2. When accounts are no longer required;
3. When users are terminated or transferred; and
4. When individual information system usage or need-to-know changes;

**The ITSO monitors all accounts. Domain accounts that are used are disabled as a function of OCIO.**

**ABPS Application: Technology-Related Consideration: Accounts are disabled (made inactive within the internal management application) by the ITSO or the primary administrator at the end of every Award Process annual cycle, so there is no need to review accounts.**

**ARA: See Above. There is no access after the selection process.**

1. Authorizes access to the information system based on:
2. A valid access authorization;
3. Intended system usage; and
4. Other attributes as required by the organization or associated missions/business functions;

**The ITSO or the primary administrator monitors all accounts.**

1. Reviews accounts for compliance with account management requirements [***Assignment:*** *Annually. (ABC O 605 00 IT User Account Management Policy*]; and

**Accounts are reviewed on an ongoing basis by the ITSO, Alpha application administrators, as well as formally reviewed on an annual basis as part of the A&A process.**

1. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

**There are no group/shared accounts.**

***Control Enhancements: (Mod Only)***

1. *The organization employs automated mechanisms to support the management of information system accounts. (If access relies on ABC domain credentials, Common.)*

**Only the interfaces of the components are automated. 111-03 ABC Central account management procedures provide automated mechanisms under 111-03.**

1. *The information system automatically terminates temporary and emergency accounts in compliance with the* [*ABC Account Management Policy requirements (page 5)*](http://www-i.nist.gov/cio/itsd/pp_nist/policy/policy_AMS.pdf)*. (If access relies on domain credentials, ABC Common.)*

**There are no emergency accounts. Temporary accounts are created for certain tasks and circumstances and they are managed in a similar way as any other account.**

1. *(Hybrid) The information system automatically disables inactive accounts in compliance with the ABC Account Management Policy requirement.*

**A Technology-Related Consideration has been applied due to the fact that neither the ABPS and ARA Applications has this ability. ABPS Application accounts are disabled by the ITSO or the primary application administrators at the end of every Award Process annual cycle, so there is no need to review accounts and ARA accounts are active for less than 90 day intervals so password expirations are not necessary.**

1. *(Hybrid) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.*

**See AU Control family for implemented auditing controls.**

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific -**

**Access to the SQL DB’s managed by 111-02 is controlled through Microsoft SQL Server Management Studio using Central ACLs which is managed by 111-03.**

**Parent system account (ABC Central) are managed under 111-03. The Alpha ITSO does have rights to make changes within the Alpha OU under the ABC Domain Active Directory.**

[AC-3](#TOC), **Access Enforcement:** (System Specific)

The information system enforces approved authorizations for logical access to the system in accordance with applicable access control policy (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains).

**ABC Central accounts (SSP 111-03): managed into groups with appropriate access granted by group used for the following components:**

* **Windows Server**
* **Windows Workstations**
* **Mac OS Workstations and Laptops**
* **Mobile Devices managed under SSP 111-04**
* **SQL Database access**

**ABPS Application: Access is granted based on group membership only to projects for which a specific reviewer is working on. Role based access is maintained at a predetermined level within each project.**

**ARA External Application: The external website allows new users to create their own account in order to enter their application information. Each user account only has access to their own data and they cannot view other reviewer applicant’s data.**

**ARA Internal Management Application: The internal website accounts use the OCIO approved LDAP and allow the Alpha Applicant administrators to grant the proper roles to the user. There are 15 available roles. Account and role management all use the same procedures as the previously authorized ABPS website.**

[AC-4](#TOC),**Information Flow Enforcement:** (Mod Only) (Common)

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on *[****Assignment:*** *organization-defined information flow control policies]*.

**ABC common implementation of this control is described in the Common Controls SSP.**

[AC-5,](#TOC)**Separation of Duties:** (Mod Only) (System Specific)

The organization:

1. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; *[****Assignment:*** *organization-defined duties of individuals];*
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

**System Administration Duties are separate from Database administration duties.**

**System Owner authorizes all account management changes while the ITSO/Primary System Administrator applies all approved changes.**

[AC-6](#TOC), **Least Privilege:** (Mod Only) (System Specific)

The organization employs the concept 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 missions and business functions.

***Control Enhancements: (Mod only)***

1. *The organization explicitly authorizes access to [****Assignment:*** *organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].*
2. *The organization requires that users of information system accounts, or roles, with access to [****Assignment:*** *organization-defined security functions or security-relevant information], use non- privileged accounts or roles, when accessing non-security functions.*
3. *The organization restricts privileged accounts on the information system to [****Assignment****: organization-defined personnel or roles].*
4. *The information system audits the execution of privileged functions.*

*(10) The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.*

* **AlphaFS: The access to this is controlled through Central Accounts by the ITSO. Restricted access is controlled through group assignments and user privileges on the server. Users have access to only those files and directories required of their responsibilities (e.g., not all users have access to the applicant feedback reports that are prepared—only the Administrative Services Staff and the Award Process Team can access these).**
* **ABPS Application: Users are assigned roles within the role-based access system to restrict access to least privilege necessary to perform the necessary work.**
* **ARA: AC-2 explains access to the site where least privilege is enforced.**

[AC-7](#TOC), **Unsuccessful Login Attempts:** (System Specific)

The information system:

1. Enforces a limit of five consecutive invalid access attempts by a user during a 15 minute period;
2. Automatically *[****Selection:*** *locks the account/node for [****Assignment:*** *organization or System-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [****Assignment:*** *organization-defined delay algorithm]]* [**Selection:** locks the account/node for [**Assignment:** per the DOC ITSPP, (15) minutes]] when the maximum number of unsuccessful attempts is exceeded.

**Central Accounts: See SSP 111-03.**

**Follows the Secure Configurations for Windows Server, Windows Workstations, Mac OS Workstations.**

**See 111-02 for SQL DB Accounts.**

**See 111-03 for Mobile Device accounts**

**ABPS and ARA Applications: User accounts are locked after three unsuccessful attempts at entry. Users can reset their account after answering three (3) questions on the website if they haven’t already locked their account. In that case they would have to contact the ABPS help line.**

[AC-8](#TOC), **System Use Notification:** (System Specific)

The information system:

1. Displays an approved system use notification message or banner 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: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;
2. Retains the notification message or banner on the screen until users take explicit actions to logon to or further access the information system; and
3. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.
4. The system displays an approved system use notification DOC approved (logon banner) before granting system access.

You are accessing a U.S. Government information system, which includes: 1) this computer,   
2) this computer network, 3) all computers connected to this network, and 4) all devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; you have no reasonable expectation of privacy regarding any communication of data transiting or stored on this information system; at any time and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

The warning banner above is displayed before granting system access on every device. **Yes**

**ABC Secure Configuration Program has been applied to all internal Alpha components which ensures warning banner is displayed.**

**Alpha ABPS and ARA Applications displays the proper warning banner upon login.**

**See 111-02 for SQL database access.**

**See SSP 111-03 for Mobile Devices.**

[AC-11](#TOC)*,* **Session Lock:** (Mod Only) (System Specific)

The information system:

* 1. Prevents further access to the system by initiating a session lock after 30 minutes of inactivity for web applications, remote access and portable devices and 15 minutes (of inactivity for desktop systems) or (of inactivity or upon receiving a request from a user); and
  2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

***Control Enhancement: (Mod only)***

*(1)* *System conceals, via the session lock, information previously visible on the display with a publicly viewable image.*

**ABC common implementation of this control is documented in the Common Controls SSP for all OCIO managed servers, and all Desktops/Laptops, and Mobile Devices.**

**System Specific:**

**The system activates session lock mechanisms automatically after 15 minutes of inactivity and users can directly initiate session lock mechanisms.**

**See 111-02 for SQL DB logins**

**ABC Secure Configuration Program has been applied to all internal Alpha components which ensures that the screen saver is initiated after 15 minutes of inactivity. All Alpha internal components are members of the Alpha Domain.**

**ABPS Application has a 60-minute timeout if inactive. Users require more time to enter data in then 30 minutes or they lose their whole entry.**

**ARA: Set for 30 minutes for both internal and external.**

***\*****Note: Per the DOC ITSPP, session locks must be initiated after thirty (30) minutes of inactivity for web applications, remote access, and portable devices, and after fifteen (15) minutes of inactivity for desktop systems. “Inactivity” is defined as only those actions which require interaction of a user (i.e., system and application calls are not included).*

[AC-12](#TOC), **Session Termination:** (Mod Only) (System Specific)

The information system automatically terminates a user session after [***Assignment:*** *organization-defined conditions or trigger events requiring session disconnect]*.

*Apply same conditions to Session Termination as for Session Lock: \*Note: Per the DOC ITSPP, session locks must be initiated after thirty (30) minutes of inactivity for web applications, remote access, and portable devices, and after fifteen (15) minutes of inactivity for desktop systems. “Inactivity” is defined as only those actions which require interaction of a user (i.e., system and application calls are not included).*

**Central Accounts: See SSP 111-03.**

**See Secure Configurations for Windows Servers, Windows Workstations, Mac OS Workstations.**

**See 111-02 for SQL DB Accounts.**

**See 111-03 for Mobile Device accounts**

**ABPS and ARA Applications: ABPS sessions are terminated after 60 minutes of inactivity while ARA is terminated after 15 minutes of inactivity.**

[AC-14](#TOC), **Permitted Actions without Identification or Authentication:** (System Specific)

The organization:

1. Identifies specific user actions that can be performed on the information system without identification or authentication or authentication consistent with organizational missions/business functions; and
2. documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

**There are no actions permitted without I&A.**

[AC-17](#TOC), **Remote Access:** (Common)

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

***Control Enhancements: (Mod Only) (Common)***

1. *The information system monitors and controls remote access methods.*
2. *The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.*
3. *The information system routes all remote accesses through the designated managed network access control points.*
4. *The organization 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.*

**ABC common implementation of this control is documented in the Common Controls SSP.**

**ABC-wide remote access mechanisms are utilized for system configuration; no other mechanisms are employed.**

[AC-18](#TOC), **Wireless Access:** (Common)

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access;
2. Monitors for unauthorized wireless access to the information system;
3. Authorizes wireless access to the information system prior to connection; and
4. Enforces requirements for wireless connections to the information system.

***Control Enhancement: (Mod Only)***

*(1) The information system protects wireless access to the system using authentication and encryption.*

**ABC common implementation of this control is documented in the Common Controls SSP.**

[AC-19](#TOC), **Access Control for Mobile Devices:** (Common)

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices;
2. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;
3. Monitors for unauthorized connections of mobile devices to organizational information systems;
4. Enforces requirements for the connection of mobile devices to organizational information systems;
5. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
6. 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
7. Applies [system defined inspection and preventativemeasures] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

***Control Enhancement: (Mod Only)***

*(5) The organization employs [****Selection:*** *full-device encryption; container encryption] to protect the confidentiality and integrity of information on [****Assignment:*** *organization-defined mobile devices,* ***per ABC O 621.00 Mobile Device and Media Encryption Policy:*** *Mobile devices and media include laptops; general purpose, portable tablet devices; personal digital assistants (PDAs); Smartphones; cell phones with data storage capability; removable media storage devices such as flash-based storage devices (e.g., USB flash drives, SD cards); portable disk drives; writable DVDs and CD-ROMs; magnetic tapes; and other devices that can operate as removable media storage devices (e.g., digital cameras, MP3 players)****].***

**ABC common implementation of this control is described in the Common Controls SSP.**

[AC-20](#TOC), **Use of External Information Systems:** (Hybrid)

The organization 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:

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

***Control Enhancements: (Mod Only)***

1. *The organization 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:*
2. *Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or*
3. *Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.*

*(2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific – There are no external connections.**

[AC-21](#TOC), **Information Sharing:** (Mod Only) (System Specific)

The organization:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for *[****Assignment:*** *organization-defined information sharing circumstances where user discretion is required]*; and
2. Employs *[****Assignment:*** *organization-defined automated mechanisms or manual processes]*to assist users in making information sharing/collaboration decisions.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific: Alpha information is shared via n-files to EXT and EXT sends paper copies to reviewers, reviewers, and judges, e.g. feedback reports, applicant applications, etc.**

[AC-22](#TOC), **Publicly Accessible Content:** (System Specific)

The organization:

* 1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;
  2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
  3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;
  4. Reviews the content on the publicly accessible organizational information system for nonpublic information annually and Removes such information, if discovered.

**See the Alpha Social Media Policies document and ABP Policy on reviewing file Content.**

[2.2 Awareness and Training (AT)](#TOC)

[AT-1](#TOC), **Security Awareness and Training Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Security Awareness and Training Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Security Awareness and Training Policy annually

**ABC common implementation of this control is described in the Common Controls SSP.**

[AT-1](#TOC), **Security Awareness and Training Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Security Awareness and Training Policy and associated security awareness and training controls; and
2. Reviews and updates the current Security Awareness and Training Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[AT-2](#TOC), **Security Awareness:** (Common)

The organization provides basic security awareness 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 at least annually thereafter.

***Control Enhancement: (Mod Only)***

*(2) The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[AT-3](#TOC), **Security Training:** (Common)

The organization provides role-based security-related training to personnel with assigned security roles and responsibilities: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) at least annually thereafter.

**ABC common implementation of this control is described in the Common Controls SSP.**

***\*****Note: Per the DOC ITSPP,* *role appointment notification must be made within the first 10 business days of appointment. Training for specialized roles must occur within 60 business days from role appointment notification (annual training requirements are based on fiscal year).*

[AT-4](#TOC), **Security Training Records:** (Common)

1. documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for *[****Assignment:*** *organization-defined time period.]*

**ABC common implementation of this control is described in the Common Controls SSP.**

[2.3 Audit and Accountability (AU)](#TOC)

[AU-1](#TOC), **Audit and Accountability Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] an Audit and Accountability Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Audit and Accountability Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[AU-1](#TOC), **Audit and Accountability Procedures:** (Hybrid)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current Audit and Accountability Procedures annually.

**The procedures for the system are documented in the SSP.**

[AU-2](#TOC), **Auditable Events:** (System Specific)

The organization:

1. Determines that the information system is capable of auditing the following events: *[****Assignment:*** *organization-defined auditable events* per DOC ITSPP AU-2, The list of auditable events to be recorded may include, but is not limited to: account logon events, account management events, directory service access events, object access failures, policy change failures, privilege use failures, and system events. Other events must be defined by the OU.]
2. Coordinates the security audit function with other organizational entities requiring **a**udit related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: *[****Assignment:*** *organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]*.

***Control Enhancement: (Mod Only)***

1. *The organization reviews and updates the list of auditable events annually.*

**AlphaFS is now using OCIO’s Splunk capability for the log reporting tool.**

**All auditable events are established through the ABC Secure Configuration Program for Windows and Mac OS machines.**

**ABPS Application: All auditable events are captured by the application, including account changes and login information. All OS and web service specific logging is fully managed under SSP 111-03.**

**The new ARA application replicates the logging features of ABPS**

**The system generates audit records for the following events:**

**Valid login Yes, all necessary components**

**Invalid login attempt Yes, all necessary components**

**Valid file/data access No**

**Invalid file/data access attempt No**

**Valid File/data edit No, except for SQL DB data changes.**

**Invalid File/data edit attempt No, except for SQL DB data changes.**

**Valid File/data delete No, except for SQL DB data changes.**

**Invalid File/data deletion attempt No, except for SQL DB data changes.**

**Logout Yes, all necessary components**

[AU-3](#TOC), **Content of Audit Records:** (System Specific)

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

***Control Enhancement: (Mod Only)***

1. *The information system generates audit records containing the following additional information:*

**All Components:**

* **Audit records include the information as noted below:**
* **Date and time of the event Yes**
* **The component(s) affected Yes**
* **The type of event Yes**
* **Subject identity Yes**
* **Outcome (success/failure) of the event Yes**
* **Additional information No**

**Windows Servers, Windows Workstations, Mac OS Workstations: Implemented through Secure Configurations for all operating systems.**

**ABPS Application user logins are managed by the Systems Administrators for Alpha. The OS and database logging is fully managed under SSP 111-03.**

**The new ARA application replicates the logging features of ABPS**

**SQL Database: See SSP 111-02**

**Mobile Devices managed under SSP 111-04**

[AU-4](#TOC), **Audit Storage Capacity:** (System Specific)

The organization allocates audit record storage capacity in accordance with *[****Assignment:*** *organization-defined audit record storage requirements]*.

**This system allocates an audit log storage capacity of 60 GB.**

**The Alpha server has 60 GB of free space which is monitored closely by the Primary System Administrator on a weekly basis. Secure Configuration settings have been applied to the Alpha server which details the log sizes.**

**ABPS Application: 7GB of space is allocated for audit storage.**

**The ARA application replicates the logging features of ABPS**

[AU-5](#TOC), **Response to Audit Processing Failures:** (System Specific)

The information system:

* 1. Alerts designated organizational officials in the event of an audit processing failure; and
  2. Takes the following additional actions noted within the control write-up below:

**In the event of an audit processing failure, this system must be configured to take the following action(s):**

* **Shutdown of system – No**
* **Overwrite oldest audit record – Yes**
* **Stop generating audit records – No**
* **Other - None**

**Response to audit failures are established through the ABC Secure Configuration Program for Windows and Mac OS machines.**

**ABPS Application: ABPS Application is configured to overwrite the oldest logs. The Application is under development stage and storage capacities are estimated at 7 GB space.**

**The ARA application replicates the logging features of ABPS**

[AU-6](#TOC), **Audit Review, Analysis, and Reporting:** (Hybrid)

The organization:

1. Reviews and analyzes information system audit records *[****Assignment****: Frequency not defined by DOC or ABC policy – System Defined]* for indications of inappropriate or unusual activity, and reports findings to designated organizational officials;
2. Reports findings to *[Assignment: organization-defined personnel or roles]*;
3. Adjusts 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.

***Control Enhancements: (Mod Only)***

*(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.*

*(3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.*

**AlphaFS is using OCIO’s Splunk capability for the log reporting tool.**

**SA reviews logs on a weekly basis for Server.**

**Mac OS and Windows workstations/laptops are OCIO Managed.**

**ABPS Application: OS logging, web server and DB logging is under SSP 111-03. Application logs are reviewed by the System Administrator as part of their daily job function. While daily reviews generally occur, the requirement is to review weekly or upon suspicious activity.**

**The ARA application replicates the log review procedures of ABPS.**

[AU-7](#TOC)***,*****Audit Reduction and Report Generation:** (Mod Only) (Hybrid)

The information system provides an audit reduction and report generation capability.

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

***Control Enhancement: (Mod Only)***

1. *The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific: ABPS Application: OS logging, web server and DB logging is under SSP 111-03. Application logs are reviewed by the System Administrator as part of their daily job function. While daily reviews generally occur, the requirement is to review weekly or upon suspicious activity.**

**The ARA application replicates the log review procedures of ABPS.**

[AU-8](#TOC), **Time Stamps:** (Hybrid)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [***Assignment:*** *Frequency not defined by DOC or ABC policy – System Defined granularity of time measurement]*.

***Control Enhancement: (Mod Only)***

*(1) The information system:*

1. *Compares the internal information system clocks [****Assignment:*** *Frequency not defined by DOC or ABC policy – System Defined frequency] with [****Assignment:*** *organization-defined authoritative time source]; and*
2. *Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [****Assignment:*** *Frequency not defined by DOC or ABC policy – System Defined time period].*

**System Specific –**

**Technology-Related Consideration that the content of the audit records is dependent on the OS and applications in use. This includes Time Stamps for all generated logs. All timestamps are linked to the ABC Domain time settings.**

[AU-9](#TOC), **Protection of Audit Information:** (System Specific)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

***Control Enhancement: (Mod Only)***

*(4) The organization authorizes access to management of audit functionality to only [****Assignment:*** *organization-defined subset of privileged users].*

**Audit information is protected by permissions on the audit files that allow only members of the administrators’ group access to the logs. This is enforced through the controls described in the AC section of this document.**

[AU-11](#TOC), **Audit Record Retention:** (System Specific)

The organization retains audit records for consistent with records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

* **Audit Retention established through the ABC Secure Configuration Program for Windows and Mac OS machines.**
* **ABPS Application: Audit records for this system are retained for 90 days.**
* **ARA Application: Audit records for this system are retained indefinitely.**

[AU-12](#TOC), **Audit Generation:** (System Specific)

The information system:

1. Provides audit record generation capability for the list of auditable events defined in AU-2 at *[****Assignment:*** *organization-defined information system components]*;
2. Allows [*Assignment: organization-defined personnel or roles]* to select which auditable events are to be audited by specific components of the system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

**Audit Generation details are provided in** [**AU-2**](#AU_2) **and** [**AU-3**](#AU_3) **above.**

2.4 Security Assessment and Authorization (CA)

**Refer to Cyber Security Assessment & Management (CSAM) tool for current assessment and authorization dates.**

This system is subject to external audits by DOC OIG, DOC OCIO (compliance reviews) and GAO. **[In the table below, provide information on the three most recent audits (enter N/A if no audits have been performed)]**:

|  |  |
| --- | --- |
| **Audit Conducted By:** | **Date** |
| **None** |  |
|  |  |
|  |  |

[CA-1](#TOC), **Security Assessment and Authorization, Policies:** (Common):

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Security Assessment and Authorization Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Security Assessment and Authorization Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CA-1](#TOC), **Security Assessment and Authorization, Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Security Assessment and Authorization Policy and associated security assessment and authorization controls; and
2. Reviews and updates the current Security Assessment and Authorization Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CA-2](#TOC): **Security Assessments:** (Common)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
2. Security controls and control enhancements under assessment;
3. Assessment procedures to be used to determine security control effectiveness; and
4. Assessment environment, assessment team, and assessment roles and responsibilities;
5. Assesses the security controls in the information system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
6. Produces a security assessment report that documents the results of the assessment; and
7. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

***Control Enhancement: (Mod Only)***

*(1) The organization employs assessors or assessment teams with [****Assignment:*** *ABC-defined level of independence] to conduct security control assessments.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[CA-3](#TOC), **Information System Connections:** (System Specific)

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements *[****Assignment:*** *Frequency not defined by DOC or ABC policy – System Defined frequency]*.

***Control Enhancement: (Mod Only)***

*(5) The organization employs [****Selection:*** *allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [****Assignment:*** *organization-defined information systems] to connect to external information systems.*

**See section 1.6 for details on system interconnections and the DOC ITSPP states the following requirements:**

* **Interconnection with entities within DOC (OU to OU) requires establishment of an ISA, MOA or MOU.**
* **Interconnection with entities external to DOC requires establishment of a contract, ISA, MOA or MOU.**
* **Interconnection agreements within an OU are at the discretion of the OU.**

**System Specific – There are no interconnections for this system.**

[CA-5](#TOC), **Plan of Action and Milestones (POA&Ms):** (Hybrid)

The organization:

1. Develops a plan of action and milestones for the information system 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
2. Updates existing plan of action and milestones [***Assignment:*** *organization-defined frequency]* based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific: POA&Ms are entered and tracked with CSAM, Accepted Risks are tracked through the A&A documentation.**

[CA-6](#TOC), **Security Authorization:** (Common)

The organization:

1. Assigns a senior-level executive or manager to the role of authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CA-7](#TOC), **Continuous Monitoring:** (Common)

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of *[****Assignment:*** *organization-defined metrics]* to be monitored;
2. Establishment of *[****Assignment:*** *organization-defined frequencies]* for monitoring and *[****Assignment:*** *organization-defined frequencies]* for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to appropriate organizational officials on an ongoing basis.

***Control Enhancement: (Mod Only)***

*(1) The organization employs assessors or assessment teams with [****Assignment:*** *organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[CA-9](#TOC), **Internal System Connections:** **(**Common**)**

The organization:

1. Authorizes internal connections of *[****Assignment:*** *organization-defined information system components or classes of components]* to the information system; and
2. documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

**ABC common implementation of this control is for OCIO-managed systems only and described in the Common Controls SSP.**

**System Specific** – **none, reliant upon common control.**

[2.5 Configuration Management (CM)](#TOC)

[CM-1](#TOC), **Configuration Management Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Configuration Management Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Configuration Management Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CM-1](#TOC), **Configuration Management Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Configuration Management Policy and associated configuration management controls; and
2. Reviews and updates the current Configuration Management Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CM-2](#TOC), **Baseline Configuration:** **(**Hybrid)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

***Control Enhancements: (Mod Only)***

1. *(Hybrid) The organization reviews and updates the baseline configuration of the information system:*
2. *annually;*
3. *When required due to significant changes; and*
4. *As an integral part of information system component installations and upgrades.*
5. *(Hybrid) The organization retains older versions of baseline configurations as deemed necessary to support rollback.*

*(7) The organization:*

1. *Issues [****Assignment:*** *organization-defined information systems, system components, or mobile devices] with [****Assignment:*** *organization-defined baseline configurations] to individuals traveling to locations that the organization deems to be of significant risk; and*
2. *Applies [****Assignment:*** *organization-defined security safeguards] to the devices when the individuals return.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific** - **The system baseline is contained in sections** [**1.4 through 1.6**](#SysEnviron) **of the SSP, hardware (asset) and software inventories and system diagram(s). These documents are reviewed and updated as the system changes, or at least annually, as part of continuous monitoring.**

[CM-3](#TOC), **Configuration Change Control:** (Mod Only) (System Specific)

The organization:

1. Determines the types of changes to the information system that are configuration controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system
5. Retains records of configuration-controlled changes to the information system for *[****Assignment:*** *organization-defined time period]*;
6. Audits activities associated with configuration-controlled changes to the information system; and
7. Coordinates and provides oversight for configuration change control activities through [***Assignment:*** *organization-defined configuration change control element (e.g., committee, board]* that convenes [Selection (one or more): *[****Assignment:*** *organization-defined frequency]*; *[****Assignment:*** *organization-defined configuration change conditions]*.

***Control Enhancement: (Mod Only)***

1. *The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.*

**ABC common implementation of this control is for OCIO-managed systems only as described in the Common Controls SSP.**

**System Specific** - **A Scalability-Related Consideration is applied for the Alpha Server as this server has one Primary System Administrator approving changes.**

**Mac OS and Windows workstations/laptops are OCIO Managed.**

**See SSP 111-02 for SQL Database and SSP 111-04 for Mobile Devices.**

**The application administrator works with OCIO to manage the changes for the ABPS and ARA applications so there is a common control related consideration as they follow OCIO change management procedures.**

[CM-4](#TOC), **Security Impact Analysis:** (System Specific)

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

**ABC common implementation of this control is for OCIO-managed systems only as described in the Common Controls SSP.**

**System Specific** – **See CM-3**

[CM-5](#TOC), **Access Restrictions for Change:** (Mod Only) (System Specific)

The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

**ABC common implementation of this control is for OCIO-managed systems only and described in the Common Controls SSP.**

**System Specific** – **The same controls described in AC-2, AC-3 provide access restrictions for change management.**

[CM-6](#TOC), **Configuration Settings:** (Hybrid)

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using the applicable ABC Secure Configuration Guide(s) and/or system-defined security configuration checklists noted below that reflect the most restrictive mode consistent with operational requirements;
2. Implements the configuration settings;
3. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
4. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

**ABC mandates use of the following secure configuration guides for system configuration and enforces the settings as noted in** [**CM-1**](#CM_1) **policies and procedures.**

**The DOC ITSPP provides for compliance with security baseline requirements.**

**See *DOC CITR-017, Baseline Configuration* for further guidance.**

**The ABC-approved secure configuration guides are used.**

**In environments for which there is no ABC approved secure baseline, configuration standards from the Center for Internet Security (CIS) Benchmarks and Scoring Tools (**[**http://www.cisecurity.org/**](http://www.cisecurity.org/)**), National Security Agency (NSA) Security Configuration Guides (**[**http://www.nsa.gov/ia/guidance/security\_configuration\_guides/index.shtml**](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml)**), or Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) (**[**http://iase.disa.mil/stigs/stig/**](http://iase.disa.mil/stigs/stig/)**) must be used.**

|  |  |
| --- | --- |
| **IT Products (excluding OSs listed above)** | **Secure Configuration Benchmark** |
| Windows 7 | USGSB |
| Windows Server 2008 R2 | ABC Windows Server 2008 R2 Secure Configuration |
| MAC OS | ABC MAC OSX Secure Configuration |
|  |  |

[CM-7](#TOC), **Least Functionality:** (System Specific)

The organization configures the information system to provide only essential capabilities and prohibits or restricts the use of the following functions, ports, protocols, and/or services [**Assignment:** organization-defined restrictions on *chargen, echo, finger, ftp, telnet, k-commands, and r-commands*].

***Control Enhancements: (Mod Only) (System Specific)***

*(1) The organization:*

1. *Reviews the information system [****Assignment:*** *organization-defined frequency per ITSPP CM-7: Annually] to identify unnecessary and/or non-secure functions, ports, protocols, and services; and*
2. *Disables [****Assignment:*** *organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure per ITSPP CM-7: Annually].*
3. *The information system prevents program execution in accordance with [Selection (one or more): [****Assignment:*** *Frequency not defined by DOC or ABC policy – System Defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].*

*(4) The organization:*

1. *Identifies [****Assignment:*** *organization-defined software programs not authorized to execute on the information system];*
2. *Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and*
3. *Reviews and updates the list of unauthorized software programs [****Assignment:*** *organization-defined frequency].*

**Secure configurations are implemented as noted in** [**CM-6**](#CM_6)**. The secure configurations restrict the use of insecure ports and allow only essential capabilities. Deviations from the secure configurations to accommodate mission objectives are documented/ referenced in** [**CM-6**](#CM_6)**.**

[CM-8](#TOC), **Information System Component Inventory:** (System Specific)

The organization:

1. develops, documents, and maintains an inventory of information system components that:
2. Accurately reflects the current information system;
3. Is consistent with the authorization boundary of the information system;
4. Is at the level of granularity deemed necessary for tracking and reporting;
5. Includes property number, SSP identifier, MAC address, system name, IP address, and description, where description is a one or two word descriptor (such as router, workstation, administrative desktop, Blackberry, etc.); and
6. Reviews and updates the information system component inventory [**Assignment:** organization-defined frequency per DOC CITR-003 and ITSPP CM-8: annually].

***Control Enhancements: (Mod Only)***

1. *(System Specific) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.* *The organization:*
2. *(Common) The organization:*
3. *Employs automated mechanisms [****Assignment:*** *organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and*
4. *Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles][Assignment: System Owner, Information System Security Officer(s), privileged users]].*
5. *(System Specific) The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.*

**All \*networkable\* assets must be entered into the ABC asset inventory system, whether currently networked or not. Exceptions include a) printers connected locally. Records are maintained on at least an annual basis as per ABC Certification and Accreditation Policy.**

[CM-9](#TOC), **Configuration Management Plan:** (Mod Only) (System Specific)

The organization develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures.
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan from unauthorized disclosure and modification.

**Configuration Management Plan details are provided in** [**CM-1 through CM-8**](#CM_1) **above.**

[CM-10](#TOC), **Software Usage Restrictions:** (Common)

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. 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.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CM-11](#TOC), **User Installed** **Software:** (Common)

The organization:

1. Establishes *[****Assignment:*** *organization-defined policies]* governing the installation of software by users;
2. Enforces software installation policies through *[****Assignment:*** *organization-defined methods]*; and
3. Monitors policy compliance at [***Assignment:*** *organization-defined frequency*].

**ABC common implementation of this control is described in the Common Controls SSP.**

[2.6 Contingency Planning (CP)](#TOC)

[CP-1](#TOC), **Contingency Planning Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Contingency Planning Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Contingency planning policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CP-1](#TOC), **Contingency Planning Procedures: (**Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users]: the Procedures to facilitate the implementation of the Contingency Planning Policy and associated contingency planning controls; and
2. Reviews and updates the current Contingency Planning Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CP-2](#TOC), **Contingency Plan:** (Hybrid)

The organization:

1. Develops a contingency plan for the information system that:
2. Identifies essential missions and business functions and associated contingency requirements;
3. Provides recovery objectives, restoration priorities, and metrics;
4. Addresses contingency roles, responsibilities, assigned individuals with contact information;
5. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
6. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
7. Is reviewed and approved by designated officials within the organization;
8. Distributes copies of the contingency plan key contingency personnel and organizational elements noted in the CP;
9. Coordinates contingency planning activities with incident handling activities;
10. Reviews the contingency plan for the information annually;
11. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and
12. Communicates contingency plan changes to key contingency personnel and organizational elements noted in the CP.
13. Protects the contingency plan from unauthorized disclosure and modification.

**The contingency plan was documented and updated. The CP is included within this Assessment and Authorization package.**

***Control Enhancements: (Mod Only)***

1. *(System Specific) The organization coordinates contingency plan development with organizational elements responsible for related plans.*
2. *(Common) The organization plans for the resumption of essential missions and business functions within [****Assignment:*** *organization-defined time period] of contingency plan activation.*
3. *(Common) The organization identifies critical information system assets supporting essential missions and business functions.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific – There is no need to coordinate the contingency plan with other contingency plans.**

[CP-3](#TOC), **Contingency Training:** (System Specific)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [***Assignment:*** *organization-defined time period]* of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. Annually thereafter.

**Per DOC ITSPP policy, personnel with CP roles are trained annually.**

[CP-4](#TOC), **Contingency Plan Testing and Exercises:** (Hybrid)

The organization:

1. Tests the contingency plan for the information system [**Assignment: per** ABC O 610.00 Certification and Accreditation policy: annually] as described in the CP to determine the plan’s effectiveness and the organization’s readiness to execute the plan; and
2. Reviews the contingency plan test results and
3. Initiates corrective actions, if needed.

***Control Enhancement: (Mod Only)***

1. *The organization coordinates contingency plan testing with organizational elements responsible for related plans.*

**System Specific - The contingency plan is tested annually in accordance with the ABC-wide CP testing procedures as noted in** [**CP-1**](#CP_1)**. Tabletop testing is used when operational requirements would be adversely affected by full testing. See the attached CP for testing details.**

[CP-6](#TOC), **Alternate Storage Sites:** (Mod Only) (Common)

The organization;

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information and.
2. The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

***Control Enhancements: (Mod Only)***

* 1. *The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same threats.*

1. *The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.*

**ComVault backups (SSP 111-03) are used. See SSP 111-03 for details.**

**ABC common implementation of this control is described in the Common Controls SSP.**

[CP-7](#TOC), **Alternate Processing Sites:** (Mod Only) (Hybrid)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [**Assignment:** organization-defined information system operations outlined in the OU System Contingency plans] for essential missions/business functions within [**Assignment:** organization-defined time period consistent with recovery time and recovery point objectives outlined in the OU System Contingency plans] when the primary processing capabilities are unavailable;
2. 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 delivery to the site within the organization-defined time period for resumption.
3. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

***Control Enhancements: (Mod Only)***

1. *The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same threats.*
2. *The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.*
3. *The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization’s availability requirements.*

**Common Control - ABC OCIO has identified numerous systems and applications for inclusion in the ABC Disaster Recovery Plan that includes an alternate site arrangement with a vendor.**

**System Specific –** **Security-Objective Related Consideration: This system has low availability requirement.**

[CP-8](#TOC), **Telecommunications Services:** (Mod Only) (Common)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption [**Assignment:** organization-defined information system operations outlined in the OU System Contingency plans] for essential missions and business functions within [**Assignment:** organization-defined time period outlined in the OU System Contingency plans] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

***Control Enhancements: (Mod Only) (Common)***

*(1) The organization:*

1. *Develops primary and alternate telecommunications service agreements that contain priority of service provisions in accordance with the organization’s availability requirements; (including recovery time objectives); and*
2. *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.*
3. *The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services*.

**ABC common implementation of this control is described in the Common Controls SSP.**

[CP-9](#TOC), **Information System Backup:** (Hybrid)

The organization:

1. Conducts backups of user-level information contained in the information system [**Assignment:** organization-defined frequency consistent with recovery time and recovery point objectives ];
2. Conducts backups of system-level information contained in the information system [**Assignment:** organization-defined frequency consistent with recovery time and recovery point objectives];
3. Conducts backups of information system documentation including security-related documentation [**Assignment:** organization-defined frequency consistent with recovery time and recovery point objectives]; and
4. Protects the confidentiality, integrity, and availability of backup information at the storage locations.

***Control Enhancement: (Mod Only) (System Specific)***

1. *The organization tests backup information* [Assignment: per DOC ITSPP CM-9, annually]*to verify media reliability and information integrity.*

**OCIO staff conducts backups of system data (including system configuration) for OCIO-managed systems and stores the backed up information as noted in the contingency plan included within this Assessment and Authorization package and described in** [**CM-1 through CM-8**](#CM_1) **of this Security Plan.**

**System Specific: System staff conduct backups of system data (including system configuration) and store the backed up information as noted in the contingency plan included within this Assessment and Authorization package and described in CM-1 through CM-8 of this Security Plan.**

[CP-10](#TOC), **Information System Recovery and Reconstitution:** (Common)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

***Control Enhancement: (Mod Only)***

1. *The information system implements transaction recovery for systems that are transaction-based.*

**The Contingency Plan document provides full details for recovery and reconstitution. The system is not transaction based.**

[2.7 Identification and Authentication (IA)](#TOC)

[IA-1](#TOC), **Identification and Authentication Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] an Identification and Authentication Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Identification and Authentication Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[IA-1](#TOC), **Identification and Authentication Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Identification and Authentication Policy and associated identification and authentication controls; and
2. Reviews and updates the current Identification and Authentication Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[IA-2](#TOC), **Identification and Authentication (Organizational Users):** **(**Hybrid)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

***Control Enhancements: (Mod, and Low needs 1 and 12) (Common)***

*The following controls are provided by ABC through the Personal Identity Verification (PIV) Project.*

1. *The information system uses multifactor authentication for network access to privileged accounts.*
2. *(System Specific) The information system uses multifactor authentication for network access to non-privileged accounts.*
3. *The information system uses multifactor authentication for local access to privileged accounts.*
4. *The information system uses system defined replay-resistant authentication mechanisms for network access to privileged accounts.*

*(11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [****Assignment:*** *organization-defined strength of mechanism requirements].*

*(12) The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.*

**Control Enhancements 1, 2, 3, 8, 11 and 12 have been designated as Common and compliance with these requirements is described in the ABC Common Controls Security Plan**.

**Except as noted in** [**AC-14**](#AC_14)**, all users of this system must be uniquely identified with a ABC user name as created and managed by the ABC Account Management System (SSP 111-07) and authenticate with a password. For control enhancement one, see** [**AC-17**](#AC_17)**.**

**SQL DB Accounts are managed under 111-02.**

**Account Management System (AMS) (SSP 111-07) assigns a unique user ID for each user and authentication is through ABC domain (SSP 111-03) using that unique user ID and password. The ABC Central unique user ID and domain authentication are used to access the Alpha server and all file shares on the server, for both Mac OS workstations, and all Windows workstations. Alpha staff also use the ABC Central unique user ID and domain authentication to access the database files stored on the file share on the Alpha server.**

**ABPS Application: A unique user ID and password is created within the database used for account management for the ABPS Application. This application is managed through the OCIO ASD, but is mentioned here because a portion of the account administration for ABPS Application is managed as part of this system. Users can reset their password by using the reset component within the application and new temporary passwords are sent to via a separate email. User must change password at first login.**

**ARA: Each user has a unique account**

[IA-3](#TOC), **Device Identification and Authentication:** (Mod Only) (System Specific)

The information system uniquely identifies and authenticates [***Assignment:*** *organization-defined specific and/or types of devices]* before establishing a [*Selection (one or more): local; remote; network]* connection

**Mobile devices (iPhones and iPad) follow the OCIO settings for this control.**

[IA-4](#TOC), **Identifier Management:** (Hybrid)

The organization manages information system identifiers by:

1. Receiving authorization from a designated organizational official to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for one year; and
5. Disabling the identifier after 90 days (per ITSPP).

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific –**

**SQL DB Accounts are managed under 111-02**

**ABC Central accounts are managed under (SSP 111-03).**

* **Windows Server**
* **Windows Workstations**
* **Mac OS Workstations and Laptops**
* **Mobile Devices managed under SSP 111-04**
* **SQL Database accounts SSP 111-02**

**ABPS Application:**

* Uniquely identifying each user—**unique user accounts are created for each user and stored in the application database. User accounts are created using first name initial and last name initial with 4 digit reviewer ID.**
* Verifying the identity of each user— **The application produces automated emails user ID to individuals.**
* Receiving authorization from a designated organizational official to assign an individual, group, role, or device identifier;
* Selecting an identifier that identifies an individual, group, role, or device
  + —**Authorization is granted through extraction processes from the Microsoft Access Database that maintains reviewer information. System owner approves these extractions and a spreadsheet is given to the OCIO ASD management team to create the accounts in the application.**
* Assigning the identifier to the intended individual, group, role, or device **The application produces automated emails user i.d. to individuals.**
* Preventing reuse of identifiers for one year; **ITSO ensures identifiers are not reused.**
* Disabling the identifier after 90 days (per ITSPP). **ABPS Application accounts are disabled by the ITSO at the end of every Award Process annual cycle.**

**ARA Application:**

* Uniquely identifying each user—**unique user accounts are created for each user and stored in the application database.**
* Verifying the identity of each user**— An email is generated that contains the account information and the password must be changed at first login. Another email is sent to verify the user that the first login has occurred and the password was changed.**
* Receiving authorization from a designated organizational official to assign an individual, group, role, or device identifier;
* Selecting an identifier that identifies an individual, group, role, or device
  + **Authorization is automatic because anyone can apply to be an reviewer and create their own account.**
* Assigning the identifier to the intended individual, group, role, or device; **An email is generated that contains the account information and the password must be changed at first login. Another email is sent to verify the user that the first login has occurred and the password was changed.**

Disabling the identifier after 90 days (per ITSPP). **External accounts are active for less than 90 day intervals so password expirations are not necessary.**

Archiving user identifiers— **External accounts are active for less than 90 day intervals so password expirations are not necessary.**

[IA-5](#TOC), **Authenticator Management:** (Hybrid)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
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 prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators
7. Changing/refreshing authenticators *[****Assignment:*** *organization-defined time period by authenticator type]*;
8. Protecting authenticator content from unauthorized disclosure and modification
9. Requiring users to take, and having devices implement, specific measures to safeguard authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes

***Control Enhancements: (Mod, and Low needs 1 and 11)***

*(1) The information system, for password-based authentication:*

1. *Enforces ABC minimum password complexity requirements: at least 12 non blank characters, from at least 3 of the following groups of characters as a mix of upper-case letters, lower-case letters, numbers, and special characters;*
2. *Enforces at least 12 character minimum password length when new passwords are created;*
3. *Stores and transmits only encrypted representations of passwords;*
4. *Enforces password minimum (1 day) and maximum lifetime restrictions (90 days); and*
5. *Prohibits password reuse.*
6. *Allows the use of a temporary password for system logons with an immediate change to a permanent password.*

*(2) The information system, for PKI-based authentication:*

1. *Validates certificates by constructing a certification path with status information to an accepted trust anchor including checking certificate status information;*
2. *Enforces authorized access to the corresponding private key*
3. *Maps the authenticated identity to the account of the individual or group; and.*
4. *Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network*
5. *The organization requires that the registration process to receive [****Assignment:*** *organization-defined types of and/or specific authenticators] be conducted in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).*
6. *The information system, for hardware token-based authentication, employs mechanisms that satisfy [****Assignment:*** *organization-defined token quality requirements].*

**See** [**IA-6**](#IA_6) **for a description of how passwords are prohibited from being displayed when entered.**

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific –**

**SQL DB Accounts are managed under 111-03**

**ABC Central accounts are managed under (SSP 111-03).**

* **Windows Server**
* **Windows Workstations**
* **Mac OS Workstations and Laptops**
* **Mobile Devices managed under SSP 111-04**
* **SQL Database access**

**ABPS Application:**

**ABC Password Policy compliant for permanent passwords. Password must be changed at first login by reviewer.**

**The password is sent through a separate email to the user where the user must change the password at initial login. The user can access no moderate data at this time.**

* **Users can reset their password by using the reset component within the application and new temporary passwords are sent to them via a separate email. User must change password at first login.**
* **The Alpha ABPS administrators will revoke accounts and generate reset passwords from within the account administration portion of the ABPS Application.**
* **Technology-Related Consideration. The ABPS application is a web-based application and is authenticated against a SQL database in the back end.**
* **Users are very well trained during required training courses on how to protect authenticators.**
* **TLS is enforced.**
* **Asterisks or dots are used so as to not compromise the authentication process.**
* **All Passwords are compliant with the ABC Password Policy.**

**ARA Application:**

**ABC Password Policy compliant for permanent passwords. Password must be changed at first login.**

* **An email is generated that contains the account information and the password must be changed at first login. Another email is sent to verify the user that the first login has occurred and the password was changed.**
* **Users can reset their password by answering previously answered question /responses, which if answered correctly will generate an email which follows the account initialization procedures described above.**
* **The authority to revoke passwords is reserved for the Alpha ITSO.**
* **Technology-Related Consideration. The application is a web-based application and is authenticated against a SQL database in the back end.**
* **Users are very well trained during required training courses on how to protect authenticators.**
* **TLS is enforced.**
* prohibits passwords from being displayed when entered **–Asterisks or dots are used so as to not compromise the authentication process.**
* **All Passwords are compliant with the ABC Password Policy.**

[IA-6](#TOC), **Authenticator Feedback:** (System Specific)

The system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals (displaying asterisks when a user types in a password is an example of obscuring feedback).

**Only dots or asterisks are shown.**

[IA-7,](#TOC) **Cryptographic Module Authentication:** **(**Hybrid)

The information system implements 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.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific – No cryptographic modules are in use for authentication.**

[IA-8](#TOC), **Identification and Authentication (Non-Organizational Users):** (System Specific)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

**Identification and authentication for non-organizational users is implemented the same as for organizational users, see** [**IA-2, IA-4, IA-5.**](#IA_2)

***Control Enhancements: (Apply to both Low and Mod.) (Common)***

1. *The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.*
2. *The information system accepts only FICAM-approved third-party credentials.*
3. *The organization employs only FICAM-approved information system components in [****Assignment:*** *organization-defined information systems] to accept third-party credentials.*
4. *The information system conforms to FICAM-issued profiles.*

[2.8 Incident Response Capability (IR)](#TOC)

[IR-1](#TOC), **Incident Response Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] an Incident Response Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Incident Response Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-1](#TOC), **Incident Response Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users]: the Procedures to facilitate the implementation of the Incident Response Policy and associated incident response controls; and
2. Reviews and updates the current Incident Response Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-2,](#TOC) **Incident Response Training:** (Common)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

1. Within *[****Assignment:*** *organization-defined time period]* of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. Annually thereafter (per ITSPP.)

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-3](#TOC), **Incident Response Testing:** (Mod Only) (Common)

The organization tests the incident response capability for the information system *[****Assignment:*** *organization-defined frequency]* using [***Assignment:*** *organization-defined tests]* to determine the incident response effectiveness and documents the results.

***Control Enhancement: (Mod Only) (System Specific)***

1. *The organization coordinates incident response testing with organizational elements responsible for related plans.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-4](#TOC), **Incident Handling:** (Common)

The organization:

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

***Control Enhancement: (Mod Only)***

*(1) The organization employs automated mechanisms to support the incident handling process.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-5](#TOC), **Incident Monitoring:** (Common)

The organization tracks and documents information system security incidents.

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-6](#TOC), **Incident Reporting:** (Common)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within *[****Assignment:*** *organization-defined time period]*; and
2. Reports security incident information to designated authorities.

***Control Enhancement: (Mod Only)***

*(1) The organization employs automated mechanisms to assist in the reporting of security incidents.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-7](#TOC), **Incident Response Assistance:** (Common)

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

***Control Enhancement: (Mod Only)***

1. *The organization employs automated mechanisms to increase the availability of incident response related information and support.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[IR-8](#TOC), **Incident Response Plan:** (Common)

The organization:

1. Develops an incident response plan that:
2. Provides the organization with a roadmap for implementing its incident response capability;
3. Describes the structure and organization of the incident response capability;
4. Provides a high-level approach for how the incident response capability fits into the overall organization;
5. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
6. Defines reportable incidents;
7. Provides metrics for measuring the incident response capability within the organization.
8. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
9. Is reviewed and approved by designated officials within the organization;
10. Distributes copies of the incident response plan to key incident response personnel and organizational elements noted in the incident response plan;
11. Reviews the incident response plan annually;
12. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
13. Communicates incident response plan changes to key incident response personnel and organizational elements noted in the incident response plan.
14. Protects the incident response plan from unauthorized disclosure and modification

**ABC common implementation of this control is described in the Common Controls SSP.**

[2.9 Maintenance (MA)](#TOC)

[MA-1](#TOC), **System Maintenance Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users]: a System Maintenance Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current System maintenance policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[MA-1](#TOC), **System Maintenance Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the System Maintenance Policy and associated system maintenance controls; and
2. Reviews and updates the current System Maintenance Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[MA-2](#TOC), **Controlled Maintenance:** (Common)

The organization:

1. 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;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. 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;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
6. Includes *[****Assignment:*** *organization-defined maintenance-related information]* in organizational maintenance records.

**Maintenance records are kept in ServiceNow tickets as part of the OCIO change management procedures. Media Sanitization procedures (as noted in** [**MP-1**](#MP_1)**) are followed to sanitize magnetic media prior to removal.**

**System Specific: Media Sanitization procedures (as noted in MP-1) are followed to sanitize magnetic media prior to removal.**

* **The Primary System Administrator performs maintenance every thirty days. The reviewing and purging of log files, purging of the file sharing directory structure, checking the health of the system resources through Performance Monitor, updating software that has become outdated or requires patches are all conducted during the monthly routine.**
* **ABC’s on-site Dell certified technicians would be deployed to identify the problem.**
* **Time period may be 2-5 business days to receive the defective hardware when ordered.**
* **Mac OS and Windows workstations/laptops are OCIO Managed.**
* **Managed desktops do not have maintenance performed, they just address problems as they occur.**
* **Printer service calls are handled by OCIO staff and/or local printer repair vendors, as needed. Service requests are coordinated by the administrative support staff.**

[MA-3](#TOC), **Maintenance Tools:** (Mod Only) (Common)

The organization approves, controls, and monitors information system maintenance tools.

***Control Enhancements: (Mod Only)***

1. *The organization inspects all maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.*
2. *The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.*

**There are no system specific maintenance tools for this system.**

[MA-4](#TOC), **Non-Local Maintenance:** (Common)

The organization:

1. Approves and monitors non-local maintenance and diagnostic activities;
2. 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;
3. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
4. Maintains records for non-local maintenance and diagnostic activities; and
5. Terminates all sessions and network connections when non-local maintenance is completed.

***Control Enhancement: (Mod Only)***

1. *The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**Remote maintenance is not permitted except as managed by common controls noted for AC-17.**

[MA-5](#TOC), **Maintenance Personnel:** (Common)

The organization:

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

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific: ABC Domain Administrators have access to the Alpha components and are available to perform maintenance in emergency cases.**

**Under normal circumstances, the following administrative personnel are authorized:**

**There is a Primary DBA that performs all maintenance. This is ensured through the same controls cited in AC-2 and AC-3.**

**There is also a Primary System Administrator that has the following responsibilities has full administrative access to all system components and performs the following:**

* **Continuous monitoring of security Functionality for Alpha System.**
* **Perform maintenance on the Alpha server.**
* **Administer the Alpha OU on the ABC organization Active Directory structure. (manages User Accounts, Group memberships, and computer accounts).**
* **Coordinate desktop support activities with the OCIO desktop support team (SSP 111-04).**

[MA-6](#TOC), **Timely Maintenance:** (Mod Only) (Common)

The organization obtains maintenance support and/or spare parts for critical system components within specified timeframes of failure as noted in the CP.

**ABC common implementation of this control is described in the Common Controls SSP.**

[2.10 Media Protection (MP)](#TOC)

800‑53 definition of “Media” – Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

800‑53 definition of “Controlled Area” – Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

[MP-1](#TOC), **Media Protection Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Media Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Media Protection Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[MP-1](#TOC), **Media Protection Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Media Protection Policy and associated media protection controls; and
2. Reviews and updates the current Media Protection Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[MP-2](#TOC), **Media Access:** (System Specific)

The organization restricts access to *[****Assignment:*** *organization-defined types of digital and/or non-digital media]* to *[Assignment: organization-defined personnel or roles]*.

**ABC common implementation of this control is described in the Common Controls SSP.**

**Media access is based on job function as defined and approved by system owner/designee (generally user’s supervisor).**

**System printers are located in secure locations and users are responsible to immediately retrieve sensitive data.**

**The Fax machine is located in a secure environment and authorized users are instructed to receive faxes immediately when they receive notification through a phone call that a fax is being sent.**

**Accepted Risk: While media protection controls are fully implemented within the Alpha office, there are external users that store data on non-ABC equipment. There is a compensating control that the Reviewer group is comprised of specially selected individuals that receive onsite training that includes training on media protection. In addition, the guidelines for handling of this data are well documented within the Reviewer Resources website, which is accessible from the Alpha home-page. These guidelines are also included within the** [**current Code of Ethical Conduct**](http://www.baldrige.nist.gov/Word_files/2011_Code_of_Ethical_Conduct.doc) **that reviewers are required to sign. Interviews also confirmed that there is a strong culture of security awareness regarding these processes within the Alpha community. There is another compensating control that the data cannot be traced to a particular company, which greatly reduces the sensitivity of the data.**

[MP-3](#TOC), **Media Marking:** (Mod Only) (Common)

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts *[****Assignment:*** *organization-defined types of information system media]* from marking as long as the exempted items remain within ABC.

**ABC common implementation of this control is described in the Common Controls SSP.**

[MP-4](#TOC), **Media Storage:** (Mod Only) (System Specific)

The organization:

1. Physically controls and securely stores [***Assignment:*** *organization-defined types of digital and/or non-digital media]* within [***Assignment:*** *organization-defined controlled areas]*; and
2. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

**ABC common implementation of this control is described in the Common Controls SSP.**

**Storage of sensitive printed material is maintained in both central locked file cabinets and a cipher-locked local storage room. Key/Cipher lock access is only available to authorized Alpha staff. Off-line storage (tape backup) is maintained in a fireproof safe in a separate room from the server and tapes are moved to the DATA CENTER Tape storage monthly.**

**Accepted Risk: While media protection controls are fully implemented within the Alpha office, there are external users that store data on non-ABC equipment. There is a compensating control that the Reviewer group is comprised of specially selected individuals that receive onsite training that includes training on media protection. In addition, the guidelines for handling of this data are well documented within the Reviewer Resources website, which is accessible from the Alpha home-page. These guidelines are also included within the** [**current Code of Ethical Conduct**](http://www.baldrige.nist.gov/Word_files/2011_Code_of_Ethical_Conduct.doc) **that reviewers are required to sign. Interviews also confirmed that there is a strong culture of security awareness regarding these processes within the Alpha community. There is another compensating control that the data cannot be traced to a particular company, which greatly reduces the sensitivity of the data.**

[MP-5](#TOC), **Media Transport:** (Mod Only) (System Specific)

The organization:

1. Protects and controls *[****Assignment:*** *organization-defined types of information system media]* during transport outside of controlled areas using *[****Assignment:*** *organization-defined security safeguards]*;
2. Maintains accountability for information system media during transport outside of controlled areas;
3. documents activities associated with the transport of information system media; and
4. Restricts the activities associated with transport of information system media to authorized personnel.

***Control Enhancements: (Mod Only)***

1. *The organization implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**Per the DOC ITSPP:**

* **For information deemed as non-sensitive (i.e., low category as defined in FIPS 199) may be transported on mobile devices or media without the use of FIPS 140-2 validated cryptographic modules. (refer to DOC CITR-05)**
* **Information deemed as sensitive (i.e., moderate or high categories as defined in FIPS 199) shall be transported on mobile devices or media using FIPS 140-2 validated cryptographic modules (refer to DOC CITR-05).**
* **Users shall ensure the physical security of portable or mobile devices while in transit (i.e., do not check with luggage), and while on foreign travel and/or foreign duty (i.e., do not leave unattended) for data categorized as low, moderate, and high (refer to DOC CITR-20).**
* **The DOC requires the OUs to protect and control media during transport (refer to DOC CITR-20).**

**System Specific** –

* **Transport of sensitive data is done through ABC approved encryption methods.**
* **Alpha sends program data to EXT by making files available through the ABPS secure application. All of the access controls and other data protection mechanisms are in place as described throughout the SSP for the ABPS application.**
* **Alpha sends feedback reports that contain BII to Alpha award applicants through encrypted approved ABC methods.**
* **Alpha sends applicant information that contains BII to judges through encrypted approved ABC methods.**
* **Offsite meetings are held where moderate confidentiality data is transported on laptops and in printed forms. The ABC laptops are running Full Disk Encryption (FDE).**

[MP-6](#TOC), **Media Sanitization:** (Common)

The organization:

1. Sanitizes [***Assignment:*** *organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [***Assignment:*** *organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

**All digital media is sanitized using approved equipment, techniques and procedures in accordance with the ABC Media Sanitization Procedures referenced in** [**MP-1**](#MP_1)**. Any non-digital media containing moderate impact data must be shredded.**

[MP-7](#TOC), **Media Use:** (Common)

The organization *[****Selection:*** *restricts; prohibits]* the use of [***Assignment:*** *organization-defined types of information system media*] on [***Assignment:*** *organization-defined information systems or system components*] using [***Assignment:*** *organization-defined security safeguards*].

***Control Enhancement: (Mod Only)***

1. *The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.*

[2.11 Physical and Environmental Protection (PE)](#TOC)

[PE-1](#TOC), **Physical and Environmental Protection Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Physical and Environmental Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Physical and Environmental Protection Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-1](#TOC), **Physical and Environmental Protection Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Physical and Environmental Protection Policy and associated physical and environmental protection controls; and
2. Reviews and updates the current Physical and Environmental Protection Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-2](#TOC), **Physical Access Authorizations:** (Hybrid)

The organization:

1. Develops, approves, and maintains 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);
2. Issues authorization credentials for facility access;
3. Reviews the access list and authorized facility access by individuals annually; and
4. Removes individuals from the facility access list when access is no longer required

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific: The server room has control access through the use of a cipher lock for which the combination is only known by the ITSO/SA and a copy of the combination is stored in the Director of Alpha’s office. This room where the AlphaFS server and travel laptops (SSP 111-04) are stored.**

[PE-3](#TOC), **Physical Access Control:** (Hybrid)

The organization:

1. Enforces physical access authorizations at [***Assignment:*** *organization-defined entry/exit points to the facility where the information system resides*] by;
2. Verifying individual access authorizations before granting access to the facility; and
3. Controlling ingress/egress to the facility using physical access devices and/or guards;
4. Maintains physical access audit logs for [***Assignment:*** *organization-defined entry/exit points*];
5. Controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk;
6. Escorts visitors and monitors visitor activity [***Assignment:*** *organization-defined circumstances requiring visitor escorts and monitoring*];
7. Secures keys, combinations, and other physical access devices;
8. Inventories physical access devices annually and
9. Changes combinations and keys [***Assignment:*** *organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific** – **The System Owner ensures that cipher lock combinations are changed when the combination is compromised or individuals with access transfer or terminate employment.**

**A cipher lock is also on the doors to the Alpha’s "confidential room" The confidential room is the repository for prior and current year feedback reports as well as other applicant-specific data that is retained for historical and retention schedule purposes. It houses the Alpha “secure fax” (Secure because only authorized individuals may enter the room to send or receive a fax), but no other equipment is in the room. However, for this room, all Alpha staffs have access but the room has a different access code than the server room.**

[PE-4](#TOC), **Access Control for Transmission Medium:** (Mod Only) (Common)

The organization controls physical access to information system distribution and transmission lines within organizational facilities using *[****Assignment:*** *organization-defined security safeguards]*.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-5](#TOC), **Access Control for Output Devices:** (Mod Only) (System Specific)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Output devices are positioned so that unauthorized personnel cannot view them.**

[PE-6](#TOC), **Monitoring Physical Access:** (Common)

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs *[****Assignment:*** *organization-defined frequency]* and upon occurrence of *[****Assignment:*** *organization-defined events or potential indications of events]*; and
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

***Control Enhancement:*** *(Mod Only)*

*(1) The organization monitors physical intrusion alarms and surveillance equipment.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-8](#TOC), **Access Records:** (Common)

The organization:

1. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) for *[****Assignment:*** *organization-defined time period]*; and
2. Reviews visitor access records at least annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-9](#TOC), **Power Equipment and Power Cabling:** (Mod Only) (Common)

The organization protects power equipment and power cabling for the information system from damage and destruction.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-10](#TOC), **Emergency Shutoff:** (Mod Only) (Common)

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [***Assignment:*** *organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-11](#TOC), **Emergency Power:** (Mod Only) (Hybrid)

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific –**

**The AlphaFS server has an Uninterrupted Power Source, that is, if the main power supply for the server is shut down, then a smart UPS is configured to automatically provide power to the server without interruption. The server is connected to a "smart" UPS that maintains server operations for 30 minutes and provides for a smooth shutdown if the UPS power is drained.**

**All laptop system components have battery backup and all desktop machines and the Mac OS’s are running UPS.**

[PE-12](#TOC), **Emergency Lighting:** (Common)

The organization 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.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-13](#TOC), **Fire Protection:** (Hybrid)

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

***Control Enhancement: (Mod Only)***

1. *The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System specific - There is no system specific fire suppression in the Alpha Server Room. This is a Scalability objective related consideration because there is only one server located in the server room and a security objective related consideration due to the low availability of the system.**

[PE-14](#TOC), **Temperature and Humidity Controls:** (Common)

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at *[****Assignment:*** *organization-defined acceptable levels]*; and
2. Monitors temperature and humidity levels [***Assignment:*** *organization-defined frequency*].

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-15](#TOC), **Water Damage Protection:** (Common)

The organization 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.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-16](#TOC), **Delivery and Removal:** (Common)

The organization authorizes, monitors, and controls all IT components entering and exiting the facility and maintains records of those items.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PE-17](#TOC), **Alternate Work Site:** (Mod Only) (System Specific)

The organization:

1. Employs *[****Assignment:*** *organization-defined security controls]* at alternate work sites;
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

**Scalability-Related Consideration - The only alternate worksites associated with this system are user residences. Logical Access Controls are in place for access to internal ABC networks from user residences (**[**See AC-17**](#AC_17)**) and users working from home must complete and sign ABC Form DN27** **which requires them to agree to safeguard government data to prevent unauthorized access, release, or alteration; however, physical and environmental controls cannot be imposed at private homes, nor would it be cost effective to do so.**

[2.12 Planning (PL)](#TOC)

[PL-1](#TOC), **Security Planning Policies:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Security Planning Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Security Planning Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PL-1](#TOC), **Security Planning Procedures:** (Hybrid)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Security Planning Policy and associated security planning controls; and
2. Reviews and updates the current Security Planning Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

**No System Specific Procedures.**

[PL-2](#TOC), **System Security Plan:** (Hybrid)

The organization:

1. Develops a security plan for the information system that:
2. Is consistent with the organization’s enterprise architecture;
3. Explicitly defines the authorization boundary for the system;
4. Describes the operational context of the information system in terms of missions and business processes;
5. Provides the security categorization of the information system including supporting rationale;
6. Describes the operational environment for the information system and relationships with or connections to other information systems;
7. Provides an overview of the security requirements for the system;
8. Identifies any relevant overlays, if applicable;
9. Describes the security controls for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
10. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
11. Distributes copies of the security plan and communicates subsequent changes to the plan to *[Assignment: organization-defined personnel or roles]* [Assignment: System Owner, Information System Security Officer(s), privileged users];
12. Reviews the security plan for the information system annually (per ITSPP); and
13. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
14. Protects the security plan from unauthorized disclosure and modification.

***Control Enhancement: (Mod Only) (System Specific)***

1. *The organization plans and coordinates security-related activities affecting the information system with [****Assignment:*** *organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific – Common Control procedures are implemented. SSP and all security related documentation is updated as needed and at a minimum annually.**

[PL-4](#TOC), **Rules of Behavior:** (Hybrid)

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and
2. Receives signed acknowledgment from such individuals indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
3. Reviews and updates the rules of behavior [**Assignment:** organization-defined frequency per ABC O 610.00 Certification and Accreditation Policy]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

***Control Enhancement: (Mod Only) (Common)***

1. *The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific** **– Rules of Behavior applies.**

[PL-8](#TOC), **Information Security Architecture:** (Mod Only) (Hybrid)

The organization:

1. Develops an information security architecture for the information system that:
2. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
3. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
4. Describes any information security assumptions about, and dependencies on, external services;
5. Reviews and updates the information security architecture [***Assignment:*** *per ABC O 610.00 Certification and Accreditation Policy: Updated any time a change to the IT system configuration occurs and reviewed annually*] to reflect updates in the enterprise architecture; and
6. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

**ABC common implementation of this control is described in the Common Controls SSP and the Technical Reference Model for the ABC IT Architecture.**

**System Specific** **– The architecture of this system is simplistic and was described in section 1.5 of this document and in the system diagram.**

[2.13 Personnel Security (PS](#TOC))

[PS-1](#TOC), **Personnel Security Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Personnel Security Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Personnel Security Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PS-1](#TOC), **Personnel Security Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Personnel Security Policy and associated personnel security controls; and
2. Reviews and updates the current Personnel Security Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PS-2](#TOC), **Position Categorization:** (System Specific)

The organization:

1. Assigns a risk designation to all organizational positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and updates position risk designations at least annually.

**System personnel (those with elevated system access/privileges) must be cleared to the level commensurate with their system role and the system sensitivity rating. The ABC Position Sensitivity Guidance as noted in PS-1 must be followed.**

**The level of clearance required by the guidance for this system is: Moderate**

**Have all personnel requiring clearance (i.e. those with privileged/administrative access) been identified? Yes**

**Have all applicable personnel been cleared at the required level? yes**

**The System Owner, in coordination with relevant managers, reviews and revises position risk designations for all positions.**

[PS-3](#TOC), **Personnel Screening:** (Hybrid)

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to OSY policy.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific: All employees for the Alpha system are screened according to ABC requirements and badges are checked before being granted any privileges to any aspect of the system.**

**Accepted Risk: There is a risk of reviewers accessing ABC moderate impact data without background checks, but that is determined to be an accepted risk because the reviewers are volunteers to the Alpha program and background checks are too imposing and discourage volunteering. There is also a compensating control the application process to become an reviewer is rigorous and requires the recommendation of distinguished members of the Alpha community.**

[PS-4](#TOC), **Personnel Termination:** (Hybrid)

The organization, upon termination of individual employment:

1. Disables information system access within *[****Assignment:*** *organization-defined time period]*;
2. Conducts exit interviews that include a discussion of *[****Assignment:*** *organization-defined information security topics]*;
3. Retrieves all security-related organizational information system-related property;
4. Retains access to organizational information and information systems formerly controlled by terminated individual.
5. Terminates/revokes any authenticators/credentials associated with the individual;
6. Notifies *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s)] within *[****Assignment:*** *organization-defined time period]*.

**ABC common implementation of this control is described in the Common Controls SSP. General and Business Domain credentials are automatically revoked upon departure.**

**System Specific – The Primary System Administrator/ITSO audits the Alpha OU once a month and deletes any unnecessary accounts from this container. The Alpha Primary System Administrator/ITSO has been granted access to manage these accounts that exist in this one OU of the ABC AD structure, but all accounts are still subject to ABC-wide management through parent OU’s group policies in the Active Directory Structure. Alpha requires that SAs remove user and privileged accounts within 24 hours of personnel departing the divisions. Notification is provided to SA via email with person’s name and EOD (Enter on Duty) date.**

[PS-5](#TOC), **Personnel Transfer:** (Hybrid)

The organization

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [***Assignment:*** *organization-defined transfer or reassignment actions*] within *[****Assignment:*** *organization-defined time period following the formal transfer action*];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s)] within [***Assignment:*** *organization-defined time period*].

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific - The Primary System Administrator/ITSO audits the Alpha OU once a month and deletes any unnecessary accounts from this container. The Alpha Primary System Administrator/ITSO has been granted access to manage these accounts that exist in this one OU of the ABC AD structure. Alpha requires that SA remove user and privileged accounts within 24 hours of personnel change in duties that no longer requires the given system component access. A current list of users is available on the ABC central server within the Directors Office (DO)/450 container within Active Directory (AD). Authorized users are identified by Alpha Management’s hiring actions.**

[PS-6](#TOC), **Access Agreements:** (Hybrid)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements annually (per ITSPP and ABC O 605.00 IT User Account Management Policy); and
3. Ensures that individuals requiring access to organizational information and information systems:
4. Sign appropriate access agreements prior to being granted access; and
5. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific** – **The Code\_of\_Ethical\_Conduct.DOC form is signed for all applicants seeking to become reviewers for the award process. Additionally, each person is required to complete another copy of the Code\_of\_Ethical\_Conduct.DOC, attached as part of the reviewer application form Reviewer\_App.pdf.**

[PS-7](#TOC), **Third-Party Personnel Security:** (Hybrid)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. documents personnel security requirements;
4. Requires third-party providers to notify *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [***Assignment:*** *organization-defined time period*]; and
5. Monitors provider compliance.

**ABC common implementation of this control is described in the Common Controls SSP.**

[PS-8](#TOC), **Personnel Sanctions:** (Common)

The organization:

1. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
2. Notifies *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s)] within *[****Assignment:*** *organization-defined time period]* when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

**ABC common implementation of this control is described in the Common Controls SSP.**

[2.14 Risk Assessment (RA)](#TOC)

[RA-1](#TOC)**, Risk Assessment Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a Risk Assessment Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current Risk Assessment Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[RA-1](#TOC), **Risk Assessment Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the Risk Assessment Policy and associated risk assessment controls; and
2. Reviews and updates the current Risk Assessment Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[RA-2](#TOC), **Security Categorization:** (System Specific)

The organization:

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

**System Security Categorization is reviewed as part of the yearly A&A process or for significant changes.**

[RA-3](#TOC), **Risk Assessment:** (System Specific)

The organization:

1. 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;
2. documents risk assessment results in the risk assessment report
3. Reviews risk assessment results annually;
4. Disseminates risk assessment results to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s)]; and
5. Updates the risk assessment as needed annually 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.

**System Risk Assessment**

**System risk assessments are reviewed, and updated as necessary, at least annually. RA findings are included in the RA report as part of each annual Security Assessment Report.** **The RA working document is kept on file in the security plan share.**

**e-Authentication Risk Assessment – An e-Authentication Risk Assessment is required if the system authenticates public users for access to federal information systems.**

**Does this system authenticate public users for access?** **Yes**

**An e-Authentication Risk Assessment has been conducted and is located in the security plan share.**

[RA-5](#TOC), **Vulnerability Scanning:** (Hybrid)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;
2. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
3. Enumerating platforms, software flaws, and improper configurations;
4. Formatting and making transparent, checklists and test procedures; and
5. Measuring vulnerability impact;
6. Analyzes vulnerability scan reports and results from security control assessments;
7. Remediates legitimate vulnerabilities [***Assignment:*** *organization-defined response times*] in accordance with an organizational assessment of risk; and
8. 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).

***Control Enhancement: (Mod Only) (Common)***

1. *The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.*
2. *The organization updates the information system vulnerabilities scanned [Selection (one or more): [****Assignment:*** *organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].*
3. *(Hybrid) The information system implements privileged access authorization to [****Assignment:*** *organization-identified information system components] for selected [****Assignment:*** *organization-defined vulnerability scanning activities].*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific – All assets are scanned for vulnerabilities (Weekly), compliance (Monthly), Web scanned yearly and all as needed.**

[2.15 System and Services Acquisition (SA)](#TOC)

[SA-1](#TOC) **System and Services Acquisition Policy:** (Common)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s)] a System and Services Acquisition Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current System and Services Acquisition policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SA-1](#TOC), **System and Services Acquisition Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s)] the Procedures to facilitate the implementation of the System and Services Acquisition Policy and associated system and services acquisition controls; and
2. Reviews and updates the current System and Services Acquisition Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SA-2](#TOC), **Allocation of Resources:** (Common)

The organization:

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

**ABC common implementation of this control is for OCIO-managed systems and OCIO-developed applications only as described in the Common Controls SSP.**

[SA-3](#TOC), **Life Cycle Support:** (Common)

The organization:

1. Manages the information system using a system development life cycle methodology that includes information security considerations;
2. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
3. Identifies individuals having information system security roles and responsibilities.
4. Integrates the organizational information security risk management process into system development life cycle activities.

**ABC common implementation of this control is for OCIO-managed systems and OCIO-developed applications only as described in the Common Controls SSP.**

[SA-4](#TOC), **Acquisitions:** (Common)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contracts information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

***Control Enhancements: (Mod, and Low need 10)***

1. *The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.*
2. *(System Specific)The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [****Assignment:*** *organization-defined design/implementation information]] at [****Assignment:*** *organization-defined level of detail].*
3. *(Systems Specific) The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.*
4. *(System Specific) The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.*

**ABC common implementation of this control is for OCIO-managed systems and OCIO-developed applications only as described in the Common Controls SSP.**

**System Specific** - **See CM-8 and CM-9.**

[SA-5](#TOC), **Information System documentation:** (System Specific)

The organization:

1. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system, system component, or information system that describes:
2. Secure configuration, installation, and operation of the information system;
3. Effective use and maintenance of security features/functions; and
4. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and
5. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system, system component, or information system that describes:
6. User-accessible security features/functions and how to effectively use those security features/functions;
7. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
8. User responsibilities in maintaining the security of the information and information system; and
9. documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent and *[****Assignment:*** *organization-defined actions]* in response;

**Information System documentation is maintained in a few different locations:**

* **Operating System documentation and all COTS product documentation is maintained on the individual vendor’s website.**
* **ABPS and ARA Applications documentation is maintained by the OCIO ASD staff.**
* **Desktop system (SSP 111-04) documentation is maintained by the OCIO as part of the system plan.**
* **Alpha server system configuration documentation is a Scalability-Related Consideration because the system component is simply a file server configured in accordance with the ABC Secure Configuration policy and no specific configuration data is necessary beyond the backups that are described in the Contingency plan.**

[SA-8](#TOC), **Security Engineering Principles:** (Mod Only) (System Specific)

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

**System Specific - Securing engineering principles that meet the security and operational requirements of this system were applied in the initial design of the system architecture and during all significant subsequent modifications.**

[SA-9](#TOC), **External Information System Services:** (Hybrid)

The organization:

1. 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;

1. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
2. Employs *[****Assignment:*** *organization-defined processes, methods, and techniques]* to monitor security control compliance by external service providers on an ongoing basis.

***Control Enhancement: (Mod Only) (System Specific)***

1. *The organization requires providers of [****Assignment:*** *organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.*

**System Specific –**

* **Contracts with EXT clearly define the services and expectations for this outsourced subsystem. The contract is in hard copy form and available with the 111-01 ITSO.**

[SA-10](#TOC), **Developer Configuration Management:** (Mod Only) (Common)

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during information system, component, or service design, development, implementation, and operation;
2. document, Manage and control changes to the information system;
3. Implement only organization-approved changes;
4. document approved changes to the information system, component, or service and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to *[****Assignment:*** *organization-defined personnel]*.

**ABC common implementation of this control is for OCIO-managed systems and OCIO-developed applications only as described in the Common Controls SSP.**

[SA-11](#TOC), **Developer Security Testing:** (Mod Only) (Common)

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

1. Create and implement a security assessment plan;
2. Perform *[Selection (one or more): unit; integration; system; regression]* testing/evaluation at *[****Assignment:*** *organization-defined depth and coverage]*;
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

**ABC common implementation of this control is for OCIO-managed systems and OCIO-developed applications only as described in the Common Controls SSP.**

SA-22, **Unsupported System Components:** (System Specific)

The organization:

1. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and

Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs

***Control Enhancements:***

1. *The organization provides [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]] for unsupported information system components.*

All are within the supported lifecycle? **[Yes]**

**If No - List those components that are obsolete/no longer supported, their location (Domain, REN, non-networked, etc), and justification for not upgrading.**

[2.16 System and Communication Protection (SC)](#TOC)

[SC-1](#TOC), **System and Communications Protection Policy:** (Common)

The organization

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a System and Communications Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current System and Communications Protection Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SC-1](#TOC), **System and Communications Protections Procedures:** (Common)

The organization:

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the System and Communications Protection Policy and associated system and communications protection controls; and
2. Reviews and updates the current System and Communications Protection Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SC-2](#TOC), **Application Partitioning:** (Mod Only) (System Specific)

The information system separates user functionality (including user interface services) from information system management functionality.

**Alpha server: System files are on a separate partition from shared directories of the File Server.**

**Alpha ABPS and ARA Applications partitioning is managed by SSP 111-03.**

[SC-4](#TOC), **Information in Shared Resources:** (Mod Only) (System Specific)

The system prevents unauthorized and unintended information transfer via shared system resources.

**N/A. There are no Information in Shared Resources**

[SC-5](#TOC), **Denial of Service Protection:** (Common)

The DOC requires that OUs ensure that the information system protects against or limits the effects of the following types of denial of service attacks( hardware, software, or communications failures, ii) lack of communication bandwidth of web sites or internal networks, and iii) directed malicious attacks originating internally or externally to the networks) by employing *[****Assignment:*** *organization-defined security safeguards]*.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SC-7](#TOC), **Boundary Protection:** (Common)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
3. Implements subnetworks for publicly accessible system components that are *[****Selection:*** *physically; logically]* separated from internal organizational networks; and

***Control Enhancements: (Mod Only)***

1. *The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.*
2. *The organization:*
3. *Implements a managed interface for each external telecommunication service;*
4. *Establishes a traffic flow policy for each managed interface;*
5. *Protects the confidentiality and integrity of the information being transmitted across each interface;*
6. *documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and*
7. *Reviews exceptions to the traffic flow policy [****Assignment:*** *organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need.*
8. *The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).*
9. *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.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[SC-8](#TOC), **Transmission Confidentiality and Integrity:** (Mod Only) (System Specific)

The information system protects the *[Selection (one or more): confidentiality; integrity]* of transmitted information.

***Control Enhancement: (Mod only)***

1. *The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].*

**Parent system information is transmitted only internally so the integrity of system information is protected by the ABC Main Firewall/Network IDS (SSP 111-05), Network Router segmentation/subnetting/ACLs/Network Switches (SSP 111-06).**

[SC-10](#TOC), **Network Disconnect:** (Mod Only) (System Specific)

The information system terminates the network connection associated with a communications session at the end of the session or thirty minutes of inactivity.

**A Technology-Related Consideration is applied as the software in use for the Parent plan is not capable of providing this control.**

**However, screen savers are initiated after 15 minutes of inactivity on all system components in Alpha and require passwords to unlock the system component and all system components belong to the ABC domain.**

**ABPS Application has a 60 minute timeout if inactive.**

**ARA: Application has a 15 minute timeout if inactive.**

[SC-12](#TOC), **Cryptographic Key Establishment and Management:** (System Specific)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [***Assignment:*** *organization-defined requirements for key generation, distribution, storage, access, and destruction*].

**N/A There are no cryptographic keys managed within the system boundaries.**

[SC-13](#TOC), **Use of Cryptography:** (System Specific)

The information system implements *[****Assignment:*** *organization-defined cryptographic uses and type of cryptography required for each use]* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**ABPS and ARA Applications: using a TLS 1.0 algorithm and that is FIPS 140-2 validated.**

**Alpha sends feedback reports that contain BII to Alpha award applicants through ABC approved encryption methods.**

**Alpha sends applicant information that contains BII to judges through ABC approved encryption methods.**

[SC-15](#TOC), **Collaborative Computing Devices:** (System Specific)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions: *[****Assignment:*** *organization-defined exceptions where remote activation is to be allowed]*;and
2. Provides an explicit indication of use to users physically present at the devices.

**N/A: There are collaborative computing devices in this system.**

[SC-17](#TOC), **Public Key Business Certificates:** (Mod Only) (System Specific)

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

**N/A: There is no PKI.**

[SC-18](#TOC), **Mobile Code:** (Mod Only) (System Specific)

The organization:

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

**Scalability-Related Consideration - ABC policy does not restrict use of mobile code due to its useful functionality for web pages and web applications. Compensating controls include implementation of** [**SC-8 and SC-9**](#SC_8)**,** [**SI-2 and SI-3**](#SI_2)**, plus overall access controls, identification and authentication controls, and audit and accountability controls.**

[SC-19](#TOC), **Voice over Internet Protocol (VoIP):** (Mod Only) (System Specific)

The organization:

1. 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
2. Authorizes, monitors, and controls the use of VoIP within the information system.

**N/A: There is no VOIP.**

[SC-20](#TOC), **Secure Name/Address Resolution Service (Authoritative Source):** (Common)

The information system:

1. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child networks and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SC-21](#TOC), **Secure Name/Address Resolution Service (Authoritative Source):** (Common)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SC-22](#TOC), **Architecture and Provisioning for Name/Address Resolution Service:** (Common)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SC-23](#TOC), **Session Authenticity:** (Mod Only) (System Specific)

The information system protects the authenticity of communications sessions.

**TLS is used for all communications on ABPS and ARA.**

[SC-28](#TOC), **Protection of Information at Rest:** (Mod Only) (Hybrid)

The information system protects the confidentiality and integrity of information at rest.

**Data is protected by the operating systems on which it resides. See AC-2, AC-3 for access controls to the operating systems.**

[SC-39](#TOC), **Process Isolation:** (Common)

The information system maintains a separate execution domain for each executing process.

**ABC common implementation of this control is described in the Common Controls SSP.**

[2.17System and Information Integrity (SI)](#TOC)

[SI-1](#TOC), **System and Information Integrity Policy:** (Common)

The organization;

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] a System and Information Integrity Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Reviews and updates the current System and Information Integrity Policy annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SI-1](#TOC), **System and Information Integrity Procedures:** (Common)

The organization;

1. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] the Procedures to facilitate the implementation of the System and Information Integrity Policy and associated system and information integrity controls; and
2. Reviews and updates the current System and Information Integrity Procedures annually.

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific – No system specific procedures.**

[SI-2](#TOC), **Flaw Remediation:** (Hybrid)

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation;
3. Installs security-relevant software and firmware updates within *[****Assignment:*** *organization-defined time period]* of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

***Control Enhancement: (Mod Only)***

1. *The organization employs automated mechanisms [****Assignment:*** *organization-defined frequency] to determine the state of information system components with regard to flaw remediation.*

**System Specific –**

**Alpha server: Notification for patches is received via OCIO email or vendor email notification and patches are then applied after non-working hours unless identified as a critical patch. Non-Critical patches are applied within one week, while critical patches are applied within one day. Patches are applied manually using Windows Update.**

**Mac OS and Windows workstations/laptops are OCIO Managed.**

[SI-3](#TOC), **Malicious Code Protection:** (Hybrid)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points network to detect and eradicate malicious code:
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
4. Perform periodic scans of the information system weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
5. Quarantines malicious code; and sends alerts to the administrator; in response to malicious code detection; and
6. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

***Control Enhancements: (Mod Only) (Common Control)***

1. *The organization centrally manages malicious code protection mechanisms.*
2. *The information system automatically updates malicious code protection mechanisms (including signature definitions).*

**ABC common implementation of this control is described in the Common Controls SSP.**

**System Specific – The antivirus is managed within 111-04 for workstations and the Alpha Server and 111-03 for OCIO managed hosting servers.**

[SI-4](#TOC), **Information System Monitoring:** (Common)

The organization:

1. Monitors the information system to detect:
2. Attacks and indicators of potential attacks in accordance with [***Assignment:*** *organization-defined monitoring objectives*]; and
3. Unauthorized local, network, and remote connections;
4. Identifies unauthorized use of the information system through *[****Assignment:*** *organization-defined techniques and methods]*;
5. 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;
6. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
7. 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
8. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
9. Provides *[****Assignment:*** *organization-defined information system monitoring information]* to *[Assignment: organization-defined personnel or roles]*[Assignment: System Owner, Information System Security Officer(s), privileged users] *[Selection (one or more): as needed; [****Assignment:*** *organization-defined frequency]]*.

***Control Enhancement: (Mod Only) (Common)***

1. *The organization employs automated tools to support near real-time analysis of events.*
2. *The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.*
3. *The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [system defined list of compromise indicators.]*

**ABC common implementation of this control is described in the Common Controls SSP.**

[SI-5](#TOC), **Security Alerts, Advisories and Directives:** (Common)

The organization:

1. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to (system administrators, System Security Officers, OU IT Security Officers, and users*)*; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

**ABC common implementation of this control is described in the Common Controls SSP.**

[SI-7](#TOC), **Software, Firmware, and Information Integrity:** (Mod, and all Public Facing Websites) (System Specific)

The organization employs integrity verification tools to detect unauthorized changes to *[****Assignment:*** *organization-defined software, firmware, and information]*.

***Control Enhancement: (Mod Only)***

1. *The information system performs an integrity check of software and information [Selection (one or more): at startup; at [****Assignment:*** *organization-defined transitional states or security-relevant events]; [****Assignment:*** *organization-defined frequency][***Assignment:** per CITR-003, annually*].*
2. *(Common) The organization incorporates the detection of unauthorized [****Assignment:*** *organization-defined security-relevant changes to the information system] into the organizational incident response capability.*

**Provided by the OS for all internal components**

**Provided by the hosting platform and ensured by running annual or as needed WebInspect scans for all applications.**

[SI-8](#TOC), **Spam Protection:** (Mod Only) (Common)

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

***Control Enhancements: (Mod Only)***

*(1) The organization centrally manages spam protection mechanisms.*

*Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.*

*(2) The information system automatically updates spam protection mechanisms.*

**ABC common implementation of this control is described in the Common Controls SSP.**

[SI-10](#TOC), **Information Input Validation:** (Mod Only) (System Specific)

The information system checks the validity of information inputs.Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

**Mac OS and Windows workstations/laptops are OCIO Managed.**

**Input validation checks are determined by the DBAs when modifying or writing code for the SQL Databases (111-02)**

**ABPS and ARA Application has these checks built into the software code and associated restrictions on database input.**

[SI-11](#TOC), **Error Handling:** (Mod Only) (System Specific)

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to authorized personnel.

**Technology-Related Consideration - Error handling is at the OS level, and is not configurable.**

**Domain administrators, SA, and DBA are the only privileged personnel accessing this system. Systems error messages are controlled by Windows and Mac Operating Systems and do not reveal any system compromising information by default.**

**ABPS and ARA Application has generic error messages built in.**

**Ordering Component: No user log in.**

[SI-12](#TOC), **Information Output Handling and Retention:** (System Specific)

The organization handles and retains information within information system and information output from the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**System staff handle and retain output from the system in accordance with organizational policy and operational requirements as noted in** [**SI-1**](#SI_1)**.**

[SI-16](#TOC), **Memory Protection:** (Mod Only) (Common)

The information system implements *[Assignment: organization-defined security safeguards]* to protect its memory from unauthorized code execution.