**Access Control**

**AC-1: Access Control Policy and Procedures**

NIST SP 800-53 Objective: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and

2. Access control procedures [*Assignment: organization-defined frequency*].

Control Translation: This control is to ensure that the organization has created access control policies and procedures that are organizational specific, available to all required personnel, and updated to ensure accuracy and contain specific information regarding the organization.

Notes: The organizational risk management strategy is a key factor in the development of the access control policy and procedures. Related control: PM-9. This control can be applied at the General level

How to test and evaluate: Examine SSP and Access Controls Policy and Procedures. Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency. Ensure access control policy and procedures are in place, sent to the organization defined personnel, and are updated in accordance with the organization defined time frame.

Technology specific: General

**AC-2: Account Management**

NIST SP 800-53 Objective: The organization:

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

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. 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;

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

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g. Monitors the use of, information system accounts;

h. Notifies account managers:

1. When accounts are no longer required;

2. When users are terminated or transferred; and

3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:

1. A valid access authorization;

2. Intended system usage; and

3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k. Establishes a process for reissuing shared

Control Translation: This control is to test the process of account management. Meaning, this control is to check to ensure only authorized accounts are created, accounts are monitored, documentation exists to provision accounts, a process is used for provisioning accounts, and accounts are reviewed.

Notes: This control is very long and easy to overlook some areas for testing. Make sure the all areas of the control are evaluated for the environment.

How to test and evaluate: Examine SSP and Access Controls Policy and Procedures. Request the ACL for each component. Review the ACL to ensure accounts are properly identified/labeled. Select 5 users from the ACL and request documentation to show the account is approved and the permissions to be assigned to the accounts. Review the ACL for temporary and/or emergency accounts and ensure they are removed in accordance with defined timeframes. Request audit logs that have been reviewed, ensuring the audit logs contain account provisioning information (save the test as this can be re-used in other controls). Obtain documentation showing that all accounts listed in the ACL have been reviewed in accordance with the required time frame.

Technology specific: General, ALL components

**AC-3: Access Enforcement**

NIST SP 800-53 Objective: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Control Translation: This control is to test to ensure the component ACLs are working as intended and allowing users access to only what is permitted.

How to test and evaluate: Utilize the ACLs and the sample obtained during the testing at AC-2. Compare the ACLs to the user access request forms to ensure users are assigned the proper permissions. Sit with the 5 selected users and try to perform actions that are not permitted by the ACLs. If the ACL is working properly the user should not be able to perform these type of actions.

Technology specific: ALL components.

**AC-4: Information Flow Enforcement**

NIST SP 800-53 Objective: 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].

Control Translation: This control is to test the flow of information within the organizations environment between applications and components.

Notes: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.

How to test and evaluate: Test this control by ensuring that only authorized users are able to manipulate the internal routers, switches, firewalls, and load balancers that control the information flow from component to component within the organization. Test this control by capturing the network device ACLs (sample may be used). Review firewall rules and Interconnection Security Agreements (ISA) to determine what information should be going where. Review network scans and penetration test results that identify open ports and running services. Ensure the packets are properly routed through the network. Ensure that administrator activities on the network devices are logged and reviewed.

Technology specific: Internal network devices.

**AC-5: Separation of Duties**

NIST SP 800-53 Objective: The organization:

a. Separates [Assignment: organization-defined duties of individuals];

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Control Translation: This control is to ensure that one user does not have the ability to perform all actions within an environment or component.

Notes: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.

How to test and evaluate: Test this control by reviewing the organization defined responsibilities that are to be segregated. Obtain the ACLs for the personnel that are assigned responsibilities that are to be segregated. Ensure the responsibilities are segregated or valid reasoning is documented as to why the separation of duties is not enforced. For administrators with super user abilities, ensure the administrator does not have development and production level access.

Technology specific: ALL components.

**AC-6: Least Privilege**

NIST SP 800-53 Objective: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

**Control Translation:** This control is to ensure that users are only assigned the permissions that are required to complete their assigned tasks.

How to test and evaluate: Test this control by reviewing the obtained ACLs that have already been collected. Reference the previously obtained user access request forms. Ensure privileges for each available role in the access control system match their assigned privileges in the Roles and Responsibilities documentation. Ensure that the user is only assigned the approved permissions. Obtain the responsibilities assigned to the user based off of the user designation (role). Ensure that the user is assigned the appropriate responsibilities and any deltas are documented and approved.

Technology specific: ALL components.

**AC-7: Unsuccessful Logon Attempts**

NIST SP 800-53 Objective: The information system:

a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay

Control Translation: This control is to ensure that user accounts are locked after a certain amount of failed logon attempts and stay locked until the appropriate action occurs.

How to test and evaluate: Test this control by reviewing the policy to determine the requirements for locking after so many consecutive failed logon attempts and the means that must occur to unlock the account. Obtain the screenshots detailing the configuration used to enforce the failed logon requirement and how long the account is locked. If possible, test this by exceeding the allowed consecutive failed logon limit and then follow the process to unlock the account.

Technology specific: ALL components.

**AC-8: System Use Notification**

NIST SP 800-53 Objective: The information system:

a. Displays to users [Assignment: organization-defined 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:

1. Users are accessing a U.S. Government information system;

2. Information system usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

4. Use of the information system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:

1. Displays system use information [Assignment: organization-defined conditions], before granting further access;

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Includes a description of the authorized uses of the system.

Control Translation: This control is to ensure that a user must accept a warning banner before access to the component is permitted.

How to test and evaluate: Test this control by reviewing the policy to determine the warning banner requirements. Capture a screenshot of the component warning banner and compare the screenshot to the documented requirement. Ensure the user must agree to the warning banner before authentication occurs or the warning banner contains language stating that by logging into the component the user by default excepts the warning banner.

Technology specific: ALL components.

**AC-10: Concurrent Session Control**

NIST SP 800-53 Objective: The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

Control Translation: This control is to ensure that a user is only permitted to utilize the organization number of defined component session at the same time.

How to test and evaluate: Test this control by reviewing the policy to determine the allowed number of concurrent sessions. Obtain a screenshot from the sampled component to detail the configuration setting to enforce this requirement. If the setting is not available, test this control by having the administrator log into the application and then use a VM or colleague workspace to log into the same device through the same means while the original session remains active. Do this as many times as needed to test the organization defined requirement. For example if the requirement is 5, performs this activity 6 times and record the results.

Technology specific: ALL components.

**AC-11: Session Lock**

NIST SP 800-53 Objective: The information system:

a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Control Translation: This control is to ensure that an authenticated session is locked after the organization time frame of inactivity preventing any further actions through the session until re-authentication occurs.

How to test and evaluate: Test this control by reviewing the policy to determine the time frame allotted for user inactivity before a user session is locked. Obtain a screenshot of the configuration and compare the configuration against the organizational requirement. Test the setting by having the administrator log into the components. Take a screenshot of the logon being sure to capture the time. Perform no activity for the allotted time frame plus one minute. Then attempt to perform activity on the component to determine if the session is locked capturing a screenshot of the activity and time. Obtain the audit logs showing the user logon, forced session lock, and user re-authentication. Verify that the administrator must re-authenticate before the administrator can perform any further actions on the component.

Technology specific: ALL components.

**AC-12: Session Termination**

NIST SP 800-53 Objective: The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Control Translation: This control is to ensure that an authenticated session is terminated after certain events of actions occur.

How to test and evaluate: Test this control by reviewing the policy to determine the events and actions that will terminate a user session if the event of action occurs. Obtain a screenshot of the component configuration that monitors for the defined events or actions that will terminate a user session. Obtain written permission from the client to perform the stated event or action Perform the event of action and record whether or not the component terminates the session. If this is not possible, request tickets or audit logs that detail an event that has occurred and the actions associated with the event to include terminating the session.

Technology specific: ALL components.

**AC-14: Permitted Actions Without Identification OR Authentication**

NIST SP 800-53 Objective: The organization:

a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Control Translation: This control is to ensure that if the organization allows actions to be performed without unique identification or authentication, the actions are documented and approved.

Note: This control is frequently not applicable.

How to test and evaluate: Test this control by reviewing the policy to determine the actions allowed to be performed without identification and authentication. Review the SSP to ensure the organization has stated the supporting rationale as to why the specific user and actions do not require identification or authentication. Review the supporting rationale for feasibility and if the rationale provides any type of security issues. Read-only is a type of action the may not require identification and authentication. Test the component to ensure that only the allowed functionality is available.

Technology specific: General.

**AC-16: Security Attributes**

NIST SP 800-53 Objective: The organization:

a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission;

b. Ensures that the security attribute associations are made and retained with the information;

c. Establishes the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined information systems]; and

d. Determines the permitted [Assignment: organization-defined values or ranges] for each of the established security attributes.

Control Translation: This control is to ensure that the identified component has the ability and adds additional information (metadata) to the packets, processed, or stored information.

Note: Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. These attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the information system state. This is being discussed as this is a FedRAMP control but is not selected at the FISMA level.

How to test and evaluate: Test this control by reviewing the organization network devices and databases. Review the network device audit log showing the packets of information sent across the network devices to ensure the time frame, packet review, trace routes, and defined security attributes are included in the sent packets. Take a screenshot of the internal databases information that is added to the stored data detailing the date stored, last modified, who modified, etc.

Technology specific: Network Devices, Databases.

**AC-17: Remote Access**

NIST SP 800-53 Objective: The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

Control Translation: This control is to ensure that only authorized remote access connections occur to the organizational network and components.

Note: VPN actions to a component is not considered remote access. The VPN itself is tested for remote access as it creates the tunnel from the user to the network. Once the user is authenticated to the network through the VPN, the user is access is considered local access and not remote.

How to test and evaluate: Test this control by reviewing the organization policy detailing the remote access usage restrictions, connection requirements, and implementation guidance. Obtain documentation from the organization that details specific remote access connections. Obtain permissions from the client to attempt a remote authentication. Locate a remote access point and attempt to connect to the organization through the remote access point.

Technology specific: VPN, Network Devices.

**AC-18: Wireless Access**

NIST SP 800-53 Objective: The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b. Authorizes wireless access to the information system prior to allowing such connections.

Control Translation: This control is to ensure that only authorized wireless access connections occur to the organizational network and components.

How to test and evaluate: Test this control by reviewing the organization policy detailing the wireless access usage restrictions, connection requirements, and implementation guidance. Obtain documentation from the organization that details specific wireless access connections. Obtain permissions from the client to attempt a wireless authentication. Locate a wireless access point and attempt to connect to the organization through the wireless access point. Ensure the network devices and components that are not identified have the wireless capabilities disabled.

Technology specific: Wireless Routers, Network Devices.

**AC-19: Access Control For Mobile Devices**

NIST SP 800-53 Objective: The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b. Authorizes the connection of mobile devices to organizational information systems.

Control Translation: This control is to ensure that only authorized mobile device connections occur to the organizational network and components.

Note: This control is referring to phones, laptops, tablets, etc. This control is frequently not applicable.

How to test and evaluate: Test this control by reviewing the organization policy detailing the mobile device access usage restrictions, connection requirements, and implementation guidance. Obtain documentation from the organization that details specific mobile devices connections. Review mobile connection configurations at policy enforcement points. Obtain permissions from the client to attempt a mobile device connection to the network. Locate a mobile device connection point and attempt to connect to the organization through a mobile device.

Technology specific: Phone, laptops, tablets.

**AC-20: User of External Information Systems**

NIST SP 800-53 Objective: 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:

a. Access the information system from external information systems; and

b. Process, store, or transmit organization-controlled information using external information systems.

Control Translation: This control is to ensure that only authorized and trusted systems and organizations are able to access the organizational network, components, and data.

Note: This control is frequently not applicable.

How to test and evaluate: Test this control by reviewing the organization policy detailing the entities that the organization permits to access the organizational network, components, and data. Obtain a copy of the SLA/MOU/ISA between the connecting entity and organization. Ensure the document requires the entity to meet the organization defined security measures.

Technology specific: General.

**AC-21: Information Sharing**

NIST SP 800-53 Objective: The organization:

a. 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

b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

Control Translation: This control is to ensure that entities sharing organizational information and following the organization requirements.

Note: This control is frequently not applicable.

How to test and evaluate: Test this control by reviewing the organization policy detailing the entities that the organization permits to access the organizational network, components, and data. Review tickets and audit logs to show that actions performed by the entity are being monitored. Review tickets that detail the actions that occurred within the entity performed actions that were not permitted by the entity and organizational agreements(s).

Technology specific: General.

**AC-22: Publicly Accessible Content**

NIST SP 800-53 Objective: The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.

Control Translation: This control is to ensure that the organization post only vetted and public information that does not contain organizational information.

Note: This control is frequently not applicable.

How to test and evaluate: Test this control by reviewing the organization policy detailing who is responsible for posting information to the public. Review the training that the assigned individual is to take before posting information to the public. Review the training records to ensure the personnel took the required training. Review logs or commensurate evidence (email) to show that required personnel reviewed the information for organization specific content before the information is posted to the public. Logs or commensurate evidence (email) to show that the publicly posted information is vetted in the organization defined time frame for organization specific information.

Technology specific: General.