**Identification and Authentication (IA)**

**IA-1: Identification and Authentication Policy and Procedures**

NIST SP 800-53 Objective: The organization:

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

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

2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:

1. Identification and authentication policy [Assignment: organization-defined frequency]; and

2. Identification and authentication procedures [Assignment: organization-defined frequency].

Control Translation: This control is to ensure that the organization has created identification and authentication 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 Identification and Authentication 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 identification and authentication 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

**IA-2: Identification and Authentication (Organizational Users)**

NIST SP 800-53 Objective: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Control Translation: This control ensures that all access to the component is done through a unique user identifier for organizational users.

Notes: This control is specific to organizational users. The enhancements to this control also require the testing of multi-factor authentication (MFA). Obtain screenshots to show the process of MFA use. Typical MFA technologies are an RSA token, Google Authenticator, and organization specific soft tokens.

How to test and evaluate: Obtain the component access control lists (ACL). Verify that each organizational user is assigned only one user ID. Check the actual name associated with the user against the user ID. May sure only active user identifiers are tested.

Technology specific: All components

**IA-3: Device Identification and Authentication**

NIST SP 800-53 Objective: 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.

Control Translation: This control ensures that all access to the component is done through a unique identifier for devices, systems, and processes.

Notes: This control is specific to devices, systems, and processes.

How to test and evaluate: Examine organizational and component specific policies to determine the devices that connect to the component. Utilize the ACL obtained during testing IA-2. This time concentrate on device identifiers. Verify that each devices, system, and process are assigned a unique identifier. May sure only active user identifiers are tested.

Technology specific: All components

**IA-4: Identifier Management**

NIST SP 800-53 Objective: The organization manages information system identifiers by:

a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, or device;

c. Assigning the identifier to the intended individual, group, role, or device;

d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and

e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].

Control Translation: This control ensures that only authorized user identifiers are created, the identifiers are unique, and active only when required for use.

How to test and evaluate: Examine organizational and component specific policies to determine the personnel that are able to approve user identifiers. Select 5 personnel from the ACL used for IA-2 testing. Request and review their user access request form that has been approved. Review the organizational and component level policies to determine if user identifiers are to have a common nomenclature. An example would be all system administrators’ user identifiers are to have –sa (jsmith-sa). Review the 5 selected account to ensure they identifiers are named properly. Review the user access request form and the ACL to ensure the 5 users are assigned to the proper groups, assigned to the proper device, and assigned the proper roles. Obtain a setting to show that user identifiers can’t be re-used for the organization defined time frame (obtain the time frame from organizational and component level policies). Obtain a setting to show the time period identifiers are disabled if not used (obtain the time frame from organizational and component level policies). The easiest way to test this is to have the password expiration time frame. Meaning that if the user does not log into change the password, the password will be no longer valid, thus making the account disabled. This needs to be verified for device accounts as the password setting may not apply.

Technology specific: General, All components

**IA-5: Authenticator Management**

NIST SP 800-53 Objective: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Control Translation: This control ensures that only authorized passwords are created for specific user accounts and the password are not easily guessed or broken.

Notes: Pay Specific attention to each part of the requirement, this control is long and areas can easily be overlooked. For this control, authenticators could be passwords, pins, tokens, PIV cards, etc.

How to test and evaluate: Interview the key point of contact for the assessment to determine how initial authenticators are distributed paying specific attention as to how the organization/component ensure that the authenticator is delivered to the correct person. Obtain a screenshot to show the setting that are enforced for initial authenticator content (number of letters (upper case and lower case), special character, number, and length). Review the organizational and component level policies to determine the process for initial authenticator distribution, for lost/compromised/damaged authenticators, and for revoking authenticators. Obtain 5 total tickets to show incidents were authenticators were revoked, lost, compromised, and damaged. For the revoked authenticators, check the ACL to ensure the associated user of device is disabled/deleted/deactivated. Obtain 2 pieces of evidence to prove that the authenticator distribution is working as intended. (face-to-face hand off, email (most likely), ticket (most likely). Check the ACL to determine if any default accounts are on the component. If so, check to see if the default account has had the password changed. Review the organizational and component level policies to determine the password requirement for maximum and minimum lifetimes and changing authenticators. Check the authenticator setting to ensure they match the requirements. Check the authenticator database to ensure the databases uses encryption and can only be altered by authorized personnel. Ensure the audit logs capture the updates to the authenticators and the audit logs are reviewed. Review the rules of behavior and security awareness training to determine the user requirement of safeguarding authenticators.

Technology specific: General, All components

**IA-6: Authenticator Feedback**

NIST SP 800-53 Objective: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Control Translation: This control ensures that an authenticator can’t be compromised through a screen share or shoulder surfing incident.

How to test and evaluate: Obtain a screenshot from the component to show that the authenticator is masked (\*\*\*\*\*\*\*) during an authentication attempt. Have the administrator enter the wrong identifier and the correct authenticator. Capture a screenshot of the error message returned by the component (could be an ssh message). Have the administrator enter the wrong authenticator and the correct identifier. Capture a screenshot of the error message returned by the component (could be an ssh message). The error messages should not specifically say whether the identifier or the password is wrong or correct. The message should be ambiguous are require another authentication attempt.

Technology specific: All components

**IA-7: Cryptographic Module Authentication**

NIST SP 800-53 Objective: 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.

Control Translation: This control ensures that the cryptographic module in place at the component level meeting the required federal standards.

Notes: The best way to test this is to get a screenshot of the encryption/cryptographic mechanisms and compare to the FIPS standards. Additionally, if the module is embedded in hardware such as a switch or router, refer to the FIPS Module Validation List.

How to test and evaluate: Obtain a screenshot to show the encryption and cryptographic mechanisms being utilized by the component. Check the FIPS standards to ensure the mechanisms are FIPS validated and/or compliant. Capture a screenshot detailing the results of the FIPS comparison.

Technology specific: All components

**IA-8: Identification and Authentication (Non-Organizational Users)**

NIST SP 800-53 Objective: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Control Translation: This control ensures that all access to the component is done through a unique user identifier for non-organizational users.

Notes: This control is specific to non-organizational users, for example, the public.

How to test and evaluate: Obtain the component access control lists (ACL). Verify that each non-organizational user is assigned only one user ID. Check the actual name associated with the user against the user ID. May sure only active user identifiers are tested.

Technology specific: All components