For High-Impact Information Systems

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

IA-1.1 – **Examine** identification and authentication policy and procedures; other relevant documents or records **and**

Interview organizational personnel with identification and authentication responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents identification and authentication policy and procedures;				
(ii)	The organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;				
(iii)	Responsible parties within the organization periodically review identification and authentication policy and procedures; and				
(iv)	The organization updates identification and authentication policy and procedures when organizational review indicates updates are required.				

IA-1.2 - Examine identification and authentication policy and procedures; other relevant documents or records **and**

Interview organizational personnel with identification and authentication responsibilities to determine if the following requirements are met:

Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;				
(ii)	The identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance and				
(iii)	The identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.				

IA-2 USER IDENTIFICATION AND AUTHENTICATION - The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

IA-2.1 – Examine identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system uniquely identifies and authenticates users (or processes acting on behalf of users); and				
(ii)	(ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST Special Publication 800-63.				

and

Test automated mechanisms implementing identification and authentication capability for the information system to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Test the information system to determine if passwords, tokens, or biometrics meet Level 2, 3, or 4 requirements consistent with NIST Special Publication 800-63				

IA-2(1).1 – Examine identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system security plan (for organization-selected authentication levels); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the NIST Special Publication 800-63 authentication levels for the information system; and				
(ii)	The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3, level 3 using a hardware authentication device, or level 4.				

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION - The information system identifies and authenticates specific devices before establishing a connection.

IA-3.1- Examine identification and authentication policy; information system design documentation; procedures addressing device identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines specific devices requiring identification and authentication before establishing connections to the information system; and				
(ii)	The information system identifies and authenticates specific devices identified by the organization before establishing connections.				

and

Test Automated mechanisms implementing device identification and authentication.

Test Steps		S	N	Findings	Initials & Date
1					

IA-4 IDENTIFIER MANAGEMENT - The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.

IA-4.1- Examine identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization manages user identifiers by uniquely identifying each user;				
(ii)	The organization manages user identifiers by verifying the identity of each user;				
(iii)	The organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official;				
(iv)	The organization manages user identifiers by issuing the identifier to the intended party;				
(v)	The organization defines the time period of inactivity after which a user identifier is to be disabled;				
(vi)	The organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and				
(vii)	The organization manages user identifiers by archiving identifiers.				

and

Test identity verification capability for the information system and for organizational facilities to determine if the following requirements are met:

	Test Steps	S	N	Findings	Initials & Date
1	Test the appropriate components of the information system to determine if a combination of passwords, tokens, or biometrics is used to employ multifactor authentication.				

IA-4.2- Examine identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST Special Publications 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records, to determine if the following requirements are met:

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization uses a personal identity verification (PIV) card token to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.				

and

Test identity verification capability for the information system and for organizational facilities to determine if the following requirements are met:

	Test Steps	S	N	Findings	Initials & Date
1	Verify that the identification control settings are in compliance with the agency's security hardening guide.				

IA-5 AUTHENTICATOR MANAGEMENT - The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.

IA-5.1- Examine identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization manages information system authenticators by defining initial authenticator content;				
(ii)	The organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;				
(iii)	The organization manages information system authenticators by changing default authenticators upon information system installation; and				
(iv)	The organization manages information system authenticators by changing/refreshing authenticators periodically.				

and

Test automated mechanisms implementing authenticator management functions to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Verify that the authentication control settings are in compliance with the agency's security hardening guide.				

IA-6 AUTHENTICATOR FEEDBACK - The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-6.1 – Examine identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.				

and

Test automated mechanisms implementing authenticator feedback to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Test the information system to determine if the feedback provides sufficient information for a legitimate user to understand why access is not granted (e.g., made a keystroke mistake, forgot the password), but does not provide information that would allow an unauthorized user to compromise the authentication mechanism.				

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION - The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

IA-7.1 – Examine identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for				

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).				

and

Test automated mechanisms implementing cryptographic module authentication to determine if the following requirements are met:

	Test Steps	S	N	Findings	Initials & Date
1	Verify that the authentication control settings are in compliance with the agency's security hardening guide.				