Identification and Authentication Implementation Checklist

Policy and Documentation

- ☐ **IA-1**: Develop organization-level, mission/business process-level, and system-level identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination, and compliance
- ☐ **IA-1**: Ensure identification and authentication policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- ☐ **IA-1**: Document procedures to facilitate implementation of the identification and authentication policy and associated controls
- ☐ **IA-1**: Disseminate identification and authentication policy and procedures to organization-defined personnel or roles
- ☐ **IA-1**: Designate an organization-defined official to manage the development, documentation, and dissemination of the identification and authentication policy and procedures
- ☐ **IA-1**: Review and update identification and authentication policy at least every 3 years or when a significant change occurs
- ☐ **IA-1**: Review and update identification and authentication procedures at least annually or when a significant change occurs

User Identification and Authentication

- ☐ **IA-2**: Implement unique identification for all organizational users
- ☐ **IA-2**: Implement authentication for all organizational users
- ☐ **IA-2**: Associate unique user identifications with processes acting on behalf of those users
- ☐ **IA-2(1)**: Implement multi-factor authentication for access to privileged accounts
- ☐ **IA-2(2)**: Implement multi-factor authentication for access to non-privileged accounts
- ☐ **IA-2(5)**: When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources
- ☐ **IA-2(6)**: Implement multi-factor authentication for local access to privileged and non-privileged accounts

- [ ] **IA-2(6)**: Implement multi-factor authentication for network access to privileged and non-privileged accounts
- [ ] **IA-2(6)**: Implement multi-factor authentication for remote access to privileged and non-privileged accounts
- [ ] **IA-2(6)**: Ensure one authentication factor is provided by a device separate from the system gaining access
- [ ] **IA-2(6)**: Ensure the separate authentication device meets FIPS 140-2 validated or NSA-approved cryptography strength requirements
- [ ] **IA-2(8)**: Implement replay-resistant authentication mechanisms for access to privileged accounts
- [ ] **IA-2(8)**: Implement replay-resistant authentication mechanisms for access to non-privileged accounts
- [ ] **IA-2(12)**: Accept and electronically verify Personal Identity Verification (PIV)-compliant credentials

Device Identification and Authentication

- [ ] **IA-3**: Define devices and/or types of devices that require unique identification and authentication
- [ ] **IA-3**: Uniquely identify organization-defined devices before establishing local connections
- [ ] **IA-3**: Uniquely identify organization-defined devices before establishing remote connections
- [ ] **IA-3**: Uniquely identify organization-defined devices before establishing network connections
- [ ] **IA-3**: Authenticate organization-defined devices before establishing local connections
- [ ] **IA-3**: Authenticate organization-defined devices before establishing remote connections
- [ ] **IA-3**: Authenticate organization-defined devices before establishing network connections

Identifier Management

- [ ] **IA-4**: Define personnel or roles authorized to assign individual, group, role, service, or device identifiers
- [ ] **IA-4**: Receive authorization from organization-defined personnel or roles before assigning identifiers

- [ ] **IA-4**: Select identifiers that uniquely identify individuals, groups, roles, services, or devices
- [ ] **IA-4**: Assign identifiers to the intended individual, group, role, service, or device
- [ ] **IA-4**: Prevent reuse of identifiers for at least 2 years
- [ ] **IA-4(4)**: Manage individual identifiers by uniquely identifying each individual according to organization-defined characteristics identifying individual status

Authenticator Management

- [ ] **IA-5**: Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of initial authenticator distribution
- [ ] **IA-5**: Establish initial authenticator content for any authenticators issued by the organization
- [ ] **IA-5**: Ensure that authenticators have sufficient strength of mechanism for their intended use
- [ ] **IA-5**: Establish administrative procedures for initial authenticator distribution
- [ ] **IA-5**: Establish administrative procedures for lost, compromised, or damaged authenticators
- [ ] **IA-5**: Establish administrative procedures for revoking authenticators
- [ ] **IA-5**: Implement administrative procedures for initial authenticator distribution
- [ ] **IA-5**: Implement administrative procedures for lost, compromised, or damaged authenticators
- [ ] **IA-5**: Implement administrative procedures for revoking authenticators
- [ ] **IA-5**: Change default authenticators prior to first use
- [ ] **IA-5**: Define time periods for changing or refreshing authenticators by authenticator type
- [ ] **IA-5**: Define events that trigger authenticator changes or refreshes
- [ ] **IA-5**: Change or refresh authenticators according to organization-defined time periods by authenticator type or when organization-defined events occur
- [ ] **IA-5**: Protect authenticator content from unauthorized disclosure
- [ ] **IA-5**: Protect authenticator content from unauthorized modification
- [ ] **IA-5**: Require individuals to take specific controls to protect authenticators
- [ ] **IA-5**: Configure devices to implement specific controls to protect authenticators
- [ ] **IA-5**: Change authenticators for group or role accounts when membership to those accounts changes

Password-Based Authentication (IA-5(1))

- [ ] **IA-5(1)**: Maintain a list of commonly-used, expected, or compromised passwords
- [ ] **IA-5(1)**: Update the password list at least annually
- [ ] **IA-5(1)**: Update the password list when organizational passwords are suspected to have been compromised directly or indirectly
- [ ] **IA-5(1)**: Verify that passwords are not found on the commonly-used, expected, or compromised password list when users create passwords
- [ ] **IA-5(1)**: Verify that passwords are not found on the commonly-used, expected, or compromised password list when users update passwords
- [ ] **IA-5(1)**: Transmit passwords only over cryptographically-protected channels
- [ ] **IA-5(1)**: Store passwords using an approved salted key derivation function, preferably using a keyed hash
- [ ] **IA-5(1)**: Require immediate selection of a new password upon account recovery
- [ ] **IA-5(1)**: Allow user selection of long passwords and passphrases
- [ ] **IA-5(1)**: Allow users to include spaces in passwords and passphrases
- [ ] **IA-5(1)**: Allow users to include all printable characters in passwords and passphrases
- [ ] **IA-5(1)**: Employ automated tools to assist users in selecting strong password authenticators
- [ ] **IA-5(1)**: Define password composition and complexity rules
- [ ] **IA-5(1)**: Enforce organization-defined password composition and complexity rules

Public Key-Based Authentication (IA-5(2))

- [ ] **IA-5(2)**: Enforce authorized access to the corresponding private key for public key-based authentication
- [ ] **IA-5(2)**: Map the authenticated identity to the account of the individual or group for public key-based authentication
- [ ] **IA-5(2)**: When using PKI, validate certificates by constructing and verifying a certification path to an accepted trust anchor
- [ ] **IA-5(2)**: When using PKI, check certificate status information during certificate validation
- [ ] **IA-5(2)**: When using PKI, implement a local cache of revocation data to support path discovery and validation

Additional Authenticator Controls

- [ ] **IA-5(6)**: Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access
- [ ] **IA-5(7)**: Ensure that unencrypted static authenticators are not embedded in applications
- [ ] **IA-5(7)**: Ensure that unencrypted static authenticators are not embedded in other forms of static storage

Authentication Feedback and Cryptographic Modules

- [ ] **IA-6**: Obscure feedback of authentication information during the authentication process to protect from exploitation
- [ ] **IA-6**: Obscure feedback of authentication information during the authentication process to protect from use by unauthorized individuals
- [ ] **IA-7**: Implement mechanisms for authentication to cryptographic modules that meet the requirements of applicable laws
- [ ] **IA-7**: Implement mechanisms for authentication to cryptographic modules that meet the requirements of applicable executive orders, directives, policies, regulations, standards, and guidelines

Non-Organizational User Authentication

- [ ] **IA-8**: Uniquely identify non-organizational users
- [ ] **IA-8**: Authenticate non-organizational users
- [ ] **IA-8**: Uniquely identify processes acting on behalf of non-organizational users
- [ ] **IA-8**: Authenticate processes acting on behalf of non-organizational users
- [ ] **IA-8(1)**: Accept Personal Identity Verification (PIV)-compliant credentials from other federal agencies
- [ ] **IA-8(1)**: Electronically verify Personal Identity Verification (PIV)-compliant credentials from other federal agencies
- [ ] **IA-8(2)**: Accept only external authenticators that are NIST-compliant
- [ ] **IA-8(2)**: Document a list of accepted external authenticators
- [ ] **IA-8(2)**: Maintain a list of accepted external authenticators
- [ ] **IA-8(4)**: Define identity management profiles for identity management

- [ ] **IA-8(4)**: Conform to organization-defined identity management profiles for identity management

Re-Authentication Requirements

- [ ] **IA-11**: Define circumstances or situations that require user re-authentication
- [ ] **IA-11**: Require users to re-authenticate when organization-defined circumstances or situations occur

Identity Proofing

- [ ] **IA-12**: Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines
- [ ] **IA-12**: Resolve user identities to a unique individual
- [ ] **IA-12**: Collect identity evidence
- [ ] **IA-12**: Validate identity evidence
- [ ] **IA-12**: Verify identity evidence
- [ ] **IA-12(2)**: Require evidence of individual identification be presented to the registration authority
- [ ] **IA-12(3)**: Define methods of validation and verification for presented identity evidence
- [ ] **IA-12(3)**: Require that presented identity evidence be validated through organization-defined methods
- [ ] **IA-12(3)**: Require that presented identity evidence be verified through organization-defined methods
- [ ] **IA-12(5)**: Deliver registration code or notice of proofing through an out-of-band channel to verify the user's address of record
- [ ] **IA-12(5)**: Support verification of physical addresses of record through out-of-band delivery
- [ ] **IA-12(5)**: Support verification of digital addresses of record through out-of-band delivery

Key Timeframes Summary

- ☐ **Policy review:** At least every 3 years or when significant changes occur
- ☐ **Procedure review:** At least annually or when significant changes occur
- ☐ **Password list updates:** At least annually and when compromise is suspected
- ☐ **Identifier reuse prevention:** At least 2 years
- ☐ **Authenticator changes:** Organization-defined by authenticator type