Information Technology (IT) Identification and Authentication (IA) Standard

September 22, 2023

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.09.25 09:39:41 -04'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	1/06/2022	Initial draft of new standard which combines National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (rev.) 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	2/1/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with EO 14028.
1.2	10/11/2022	Update to include feedback from Governance, Risk and Policy (GRP) Security Assessment Team; remove IA-1 from privacy baseline; and incorporate multi-factor authentication requirements from OMB Memo 22-09, Federal Zero Trust Strategy.
5.3	9/22/2023	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, *Standards* was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Updated Section 4, *Acronyms* as appropriate. Updated language in controls IA-1, IA-2 ED-03, IA-2 ED-04, IA-2 ED-05, IA-2 ED-06, IA-2 ED-07, IA-2(1) ED-01, IA-2(2) ED-01, IA-2(5) ED-01, IA-2(12) ED-01, IA-2(12) ED-04, IA-2(12) ED-05, IA-4 ED-01, IA-4 ED-02, IA-4 ED-03, IA-5 ED-01, IA-5 ED-02, IA-5 ED-03, IA-5(1), IA-8 ED-01, IA-8(2), IA-8(4). Added controls IA-2(1) ED-03, IA-2(6), IA-3(1), IA-5(5), IA-5(7), IA-5(8), IA-5(12), IA-5(13), IA-8, IA-8 ED-02, IA-8 ED-03, IA-8 ED-04, IA-8(2) ED-01, IA-12(1).

Table of Contents

1 INTRODUCTION

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standard (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as amended, as baseline information system controls.

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) system identification and authentication controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Directives, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these identification and authentication control standards.

[1] Public Law 113-283-Dec.gover 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf

[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2 STANDARDS

The Department standards for IT system identification and authentication controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy baseline controls (e.g., Privacy (P) are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline.

In addition to the controls required by this standard, high value assets (HVAs) must implement and comply with the current version of the HVA Control Overlay[5] issued and maintained by the U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax return information (FTRI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[6], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[7].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to ***Section 5, APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY*** for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

2.1 IA-1 Policy and Procedures (L, M, H)

The Department shall develop, document, and disseminate to all Department employees, contractors, and users authorized to access to Department information systems, or systems operated or maintained on behalf of the Department, or Department information as defined in

[5] HVA Control Overlay https://www.cisa.gov/resources-tools/resources/high-value-asset-control-overlay

[6] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf

[7] FedRAMP baselines https://www.fedramp.gov/baselines/

ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level IT identification and authentication policy (e.g., this document) that:

(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as ACSD-OCIO-004, *Cybersecurity Policy*.

The Department CISO is designated to manage the development, documentation, and dissemination of the Department-level IT identification and authentication policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and Department policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISOs) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of this policy standard and the associated controls. The ISO and ISSO shall review system identification and authentication procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and Department policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 IA-2 Identification and Authentication (Organizational Users) (L, M, H and Control Overlay)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Control Overlay IA-2 ED-01 (L, M, H): Identify all Department users and authenticate user identities before accessing Department systems.

Control Overlay IA-2 ED-02 (L, M, H): Require network user accounts created after the initial issuance of this standard to match the user's legal first and last name.

[8] Also known as OCIO: 3-112

Control Overlay IA-2 ED-03 (L, M, H): Integrate all ED systems or applications that store, maintain, or consume user accounts with the ED Enterprise Identity, Credential, and Access Management (ICAM) system to manage the digital identity lifecycle and enable compliance auditing and reporting.

Control Overlay IA-2 ED-04 (L, M, H): Use ED Enterprise ICAM shared services for credentialing and identity proofing public consumers who require access to ED digital services.

Control Overlay IA-2 ED-05 (L, M, H): Designate ED Enterprise ICAM as the authoritative source for managing the digital identity lifecycle of all:

a. Person identities including all categories of ED personnel; as well as public citizens who require access to ED online services.

b. Non-person Entities (NPE) including service accounts and automated technologies, such as robotic process automation (RPA) tools and artificial intelligence (AI). Enterprise Identity Management System (EIMS) ensures the digital identity is distinguishable, auditable, and consistently managed.

Control Overlay IA-2 ED-06 (L, M, H): Use one of the approved enterprise authentication services as appropriate for the system use cases for all ED systems or applications that require authentication.

a. Enterprise Active Directory for ED's domain for end user office automation services

b. ED's privileged access system for privileged access

c. ED ICAM access management services for all web and mobile application access, including internal users and public citizens

Control Overlay IA-2 ED-07 (L, M, H): Ensure that a NIST SP 800-63 digital identity risk assessment (DIRA) is conducted and documented within Cyber Security Assessment and Management (CSAM).

2.2.1 IA-2(1) Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts (L, M, H and Control Overlay)

Implement multi-factor authentication for access to privileged accounts.

Control Overlay IA-2(1) ED-01 (L, M, H): Implement phishing-resistant multi-factor authentication to privileged accounts in accordance with the Department Zero Trust Architecture (ZTA) Strategy/Plan; phishing-resistant multi-factor authentication must be enforced at the application layer instead of the network layer.

Control Overlay IA-2(1) ED-02 (L, M, H): Use multi-factor authentication that is verifier impersonation resistant for all administrators of EO-critical software and EO-critical software platforms.

Control Overlay IA-2(1) ED-03 (L, M, H): All privileged accounts shall be managed leveraging an authorized enterprise privileged access management system.

2.2.2 IA-2(2) Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-privileged Accounts (L, M, H and Control)

Implement multi-factor authentication for access to non-privileged accounts.

Control Overlay IA-2(2) ED-01 (L, M, H): Implement phishing-resistant multifactor authentication to non-privileged accounts in accordance with Department Zero Trust Architecture (ZTA) Strategy/Plan; phishing-resistant multi-factor authentication must be enforced at the application layer instead of the network layer.

Control Overlay IA-2(2) ED-02 (L, M, H): Use multi-factor authentication that is verifier impersonation resistant for all users of EO-critical software and EO-critical software platforms.

2.2.3 IA-2(5) Identification and Authentication (Organizational Users) | Individual Authentication with Group Authentication (H and Control Overlay)

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Control Overlay IA-2(5) ED-01 (L, M, H): Use multi-factor authentication that is verifier impersonation resistant for all users of EO-critical software and EO-critical software platforms before granting access to shared accounts or resources.

2.2.4 IA-2(6) Identification and Authentication (Organizational Users) | Access to Accounts – Separate Device

Implement multi-factor authentication for remote access to privileged and non-privileged accounts such that:

a. One of the factors is provided by a device separate from the system gaining access; and

b. The device meets Authenticator Assurance Level (AAL) 2 as defined by NIST SP 800-63.

2.2.5 IA-2(8) Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant (L, M, H)

Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts.

2.2.6 IA-2(12) Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials (L, M, H and Control Overlay)

Accept and electronically verify PIV-compliant credentials.

Control Overlay IA-2(12) ED-01 (L, M, H): Require the use of Homeland Security Presidential Directive (HSPD)-12 compliant personal identity verification (PIV) (including Derived PIV) as the "primary" means of authentication to Federal information systems. Phishing-resistant authenticators, for systems that do not yet support PIV or Derived PIV (such as FIDO2 and Web Authentication-based authenticators), may be used in order to meet the requirements of this standard when PIV is not a practical option. To the greatest extent possible, centrally implement support for non-PIV authenticators in enterprise identity management systems, so that these authenticators are centrally managed and connected to enterprise identities.

Control Overlay IA-2(12) ED-02 (L, M, H): Require and implement the use of the PIV credential digital signature capability for internal and external business.

Control Overlay IA-2(12) ED-03 (L, M, H): Ensure use of the PIV credential for physical access to federal facilities and secured areas is implemented in accordance with Department Physical Security policy.

Control Overlay IA-2(12) ED-04 (L, M, H): Maintain exception procedures for emergency situations and account recovery processes; design recovery processes with the expectation that they are exceptional and require high-friction methods that are costly for an adversary to overcome, such as in-person verification, live video interaction, or other similar methods.

Control Overlay IA-2(12) ED-05 (L, M, H): Require approved Federal Public Key Infrastructure (PKI) credentials to validate digital signatures for individuals that fall outside the scope of PIV applicability.

2.3 IA-3 Device Identification and Authentication (M, H)

Uniquely identify and authenticate Department authorized devices and system components before establishing a local, remote, or network connection.

2.3.1 IA-3(1) Cryptographic Bidirectional Authentication

Authenticate all devices before establishing a remote network connection using bidirectional authentication that is cryptographically based.

2.4 IA-4 Identifier Management (L, M, H)

Manage system identifiers by:

a. Receiving authorization from Information System Owners or authorized delegate to assign an individual, group, role, service, or device identifier;

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

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

d. Preventing reuse of identifiers for one year.

Control Overlay IA-4 ED-01 (L, M, H): Require the assessment of identity risks in an identity-proofing scenario to be ranked by Identity Assurance Level (IAL), as defined by NIST SP 800-63A. Each defined user role must be evaluated through a NIST SP 800-63 digital identity risk assessment and assigned an appropriate Identity Assurance Level. Using the high watermark, values must be entered into the CSAM Digital Identity screen.

Control Overlay IA-4 ED-02 (L, M, H): Require stakeholders to annually re-evaluate assurance levels through a NIST SP 800-63 digital identity risk assessment and record the results within the Department approved Governance, Risk and Compliance (GRC) tool.

Control Overlay IA-4 ED-03 (L, M, H): Require changes in system/application design, related to user roles, entitlements, or risk profiles to trigger a full IAL re-evaluation process using a NIST SP 800-63 digital identity risk assessment.

2.4.1 IA-4(4) Identifier Management | Identify User Status (M, H)

Manage individual identifiers by uniquely identifying each individual as a federal employee (including unpaid positions), or contractor.

2.5 IA-5 Authenticator Management (L, M, H and Control Overlay)

Manage system authenticators by:

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

b. Establishing initial authenticator content for any authenticators issued by the Department;

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 or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators in accordance with Federal Zero Trust Strategy, Department Zero Trust Architecture Strategy/Plan or 90 days when zero trust architecture is not implemented or when compromised, recovered/forgotten, or due to incident related events occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts' changes.

Control Overlay IA-5 ED-01 (L, M, H): Require the assessment of authenticator risks in an authenticator proofing scenario to be ranked by Authenticator Assurance Level (AAL), as defined by NIST SP 800-63B. Each defined user role must be evaluated through a NIST SP 800-63 digital identity risk assessment and assigned an appropriate Authenticator Assurance Level. Using the high watermark, values must be entered into the CSAM Digital Identity screen.

Control Overlay IA-5 ED-02 (L, M, H): Require stakeholders to annually re-evaluate assurance levels through a NIST SP 800-63 digital identity risk assessment and record the results within the Department approved GRC tool.

Control Overlay IA-5 ED-03 (L, M, H): Require changes in system/application design, related to user roles, entitlements, or risk profiles to trigger a full AAL re-evaluation process using a NIST SP 800-63 digital identity risk assessment.

2.5.1 IA-5(1) Authenticator Management | Password-based Authentication (L, M, H)

For password-based authentication:

a. Maintain a list of commonly used, expected, or compromised passwords and update the list annually (i.e., each fiscal year) and when organizational passwords are suspected to have been compromised directly or indirectly;

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-5(1)(a);

c. Transmit passwords only over cryptographically protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the following composition and complexity rules:

   1. Passwords have a minimum length of 12 characters and must contain at least three types of characters:

      a. English uppercase letters (A-Z)

      b. English lowercase letters (a-z)

      c. Arabic numerals (0-9)

      d. Non-alphanumeric special characters ($,!, &, etc.)

   2. Password complexity is not required after implementation of zero trust architectures in accordance with Department Zero Trust Architecture Strategy/Plan. Allow for up to 64 characters in length, using any characters.

3. Remove requirements for composition and complexity rules and regular password rotation from all systems within one year of the issuance of OMB Memorandum, M-22-09.

2.5.2 IA-5(2) Authenticator Management | Public Key-based Authentication (M, H and Control Overlay)

a. For public key-based authentication:

   1. Enforce authorized access to the corresponding private key; and

   2. Map the authenticated identity to the account of the individual or group; and

b. When public key infrastructure (PKI) is used:

   1. Validate certificates by constructing and verifying a certification path to the Federal PKI trust anchor, including checking certificate status information; and

   2. Implement a local cache of revocation data to support path discovery and validation.

Control Overlay IA-5(2) ED-01 (M, H): Ensure public key certificates used by the Department are issued, managed, and revoked in accordance with Federal PKI policy.

Control Overlay IA-5(2) ED-02 (M, H): Validate public key certificates used by the Department to the Federal PKI trust anchor for all uses, including but not limited to encryption, authentication, and authorization applications.

Control Overlay IA-5(2) ED-03 (M, H): Use a key recovery mechanism on all devices containing sensitive information so that authorized personnel with legitimate need can access encrypted information.

Control Overlay IA-5(2) ED-04 (M, H): Prohibit the use of encryption keys which are not recoverable by authorized personnel.

Control Overlay IA-5(2) ED-05 (M, H): Allow a non-owner of an encryption key to request key recovery; however, such requests must be explicitly authorized by the ED Chief Information Security Officer (CISO).

2.5.3 IA-5(5) Authenticator Management | Change Authenticators Prior to Delivery

Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

2.5.4 IA-5(6) Authenticator Management | Protection of Authenticators (M, H)

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

2.5.5 IA-5(7) Authenticator Management | No Embedded Unencrypted Static Authenticators

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

2.5.6 IA-5(8) Authenticator Management | Multiple System Accounts

Implement different authenticators in different user authenticator domains to manage the risk of compromise due to individuals having accounts on multiple systems.

2.5.7 IA-5(12) Authenticator Management | Biometric Authentication Performance

For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements as defined in NIST SP 800-63.

2.5.8 IA-5(13) Authenticator Management | Expiration of Cached Authenticators

Prohibit the use of cached authenticators after baseline configuration (e.g., security technical implementation guides [STIGs]) defined time period.

2.6 IA-6 Authentication Feedback (L, M, H)

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

2.7 IA-7 Cryptographic Module Authentication (L, M, H)

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

2.8 IA-8 Identification and Authentication (Non-organizational Users) (L, M, H and Control Overlay)

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Control Overlay IA-8 ED-01 (L, M, H): Determine system role and account requirements for external users (i.e., users who are not Department employees or contract personnel) prior to authorizing access to access ED information systems.

Control Overlay IA-8 ED-02 (L, M, H): Conduct a NIST SP 800-63 digital identity risk assessment for all non-organizational user roles and record the results within Department approved GRC tool.

Control Overlay IA-8 ED-03 (L, M, H): All privilege accounts shall be managed leveraging an authorized enterprise privileged access management system.

Control Overlay IA-8 ED-04 (L, M, H): All non-organization users shall have the capability of enabling MFA capabilities for non-privileged access to the information system.

2.8.1 IA-8(1) Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies (L, M, H)

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

2.8.2 IA-8(2) Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators (L, M, H)

a. Accept only external authenticators that are NIST-compliant; and

b. Document and maintain a list of accepted external authenticators.

Control Overlay IA-8(2) ED-01 (L, M, H): Use one of the approved enterprise authentication services as appropriate for the system use cases for all ED systems or applications that require authentication.

a. Approved federated service providers (e.g., Login.gov) for externally facing (internet facing) authentication requirements.

2.8.3 IA-8(4) Identification and Authentication (non-organizational Users) | Use of Defined Profiles (L, M, H)

Conform to the following profiles for identity management: Federal Identity, Credential, and Access Management (FICAM) issued implementation profiles.

2.9 IA-11 Re-authentication (L, M, H)

Require users to re-authenticate when:

a. Required by zero trust architecture policies, standards, guidance, and memorandums provided by CISA, OMB and NIST;

b. Re-establishing authenticated access following activation of a device lock (e.g., screensaver);

c. Passwords are reset;

d. Privileged functions are executed; and

e. Periodic reauthentication time limits are met.

2.10 IA-12 Identity Proofing (M, H and Control Overlay)

a. 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;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Control Overlay IA-12 ED-01 (L, M, H): Authenticate the claimed identity of each user in such a way that the authentication is resistant to impersonation, forgery, or other misuse; and possesses strength and assurance that is commensurate with the sensitivity of the assets and information being protected.

2.10.1 IA-12(1) Identity Proofing | Supervisor Authorization

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

2.10.2 IA-12(2) Identity Proofing | Identity Evidence (M, H)

Require evidence of individual identification be presented to the registration authority.

2.10.3 IA-12(3) Identity Proofing | Identity Evidence Validation and Verification (M, H)

Require that the presented identity evidence be validated and verified through methods which are consistent with the risks to the systems, roles, and privileges associated with the user’s account.

2.10.4 IA-12(4) Identity Proofing | In-person Validation and Verification (H)

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

2.10.5 IA-12(5) Identity Proofing | Address Confirmation (M, H)

Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

Acronym	Definition
AAL	Authenticator Assurance Level
ACSD	Administrative Communications System Directive
AI	Artificial Intelligence
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
CT.DP-P	Control-P: Disassociated Processing
DE.DP	Detect: Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
ED	U.S. Department of Education
EIMS	Enterprise Identity Management System
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GRC	Governance, Risk and Compliance
GV.MT-P	Govern-P: Monitoring and Review
GV.PO-P	Govern-P: Governance Policies, Processes, and Procedures
H	High
HVA	High Value Asset
IA	Identification and Authentication Family
IAL	Identity Assurance Level
IAS	Information Assurance Services
ICAM	Identity, Credential, and Access Management
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
NPE	Non-person Entities
OCIO	Office of the Chief Information Officer
ODP	Organization Defined Parameter
OMB	Office of Management and Budget
P	Privacy

Acronym	Definition
PF	Privacy Framework
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PR.AC	Protect: Identity Management and Access Control
PR.AC-P	Protect-P: Identity Management, Authentication, and Access Control
PUB	Publication
RAF	Risk Acceptance Form
Rev.	Revision
RPA	Robotic Process Automation
SP	Special Publication
STIG	Security Technical Implementation Guide
ZTA	Zero Trust Architecture

5 APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
IA-1	Policy and Procedures		x	x	x	PR.AC, DE.DP, GV.PO-P, GV.MT-P, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.AC-P1, PR.AC-P6
IA-2	Identification and Authentication (organizational Users)		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-2(5)	Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication				x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
IA-2(6)	Identification and Authentication (organizational Users) | Access to Accounts — Separate Device					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-2(10)	Identification and Authentication (organizational Users) | Single Sign-on					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-2(12)	Identification and Authentication (organizational Users) | Acceptance of PIV Credentials		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-2(13)	Identification and Authentication (organizational Users) | Out-of-band Authentication					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-3	Device Identification and Authentication			x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication					PR.AC, PR.AC-P	PR.AC-1, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-3(3)	Device Identification and Authentication | Dynamic Address Allocation					PR.AC, PR.AC-P	PR.AC-1, PR.AC-7, PR.AC-P1, PR.AC-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
IA-3(4)	Device Identification and Authentication | Device Attestation					PR.AC, PR.AC-P	PR.AC-1, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-4	Identifier Management		x	x	x	PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, CT.DP-P2, PR.AC-P1, PR.AC-P6
IA-4(1)	Identifier Management | Prohibit Account Identifiers as Public Identifiers					PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, CT.DP-P2, PR.AC-P1, PR.AC-P6
IA-4(4)	Identifier Management | Identify User Status			x	x	PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, CT.DP-P2, PR.AC-P1, PR.AC-P6
IA-4(5)	Identifier Management | Dynamic Management					PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, CT.DP-P2, PR.AC-P1, PR.AC-P6
IA-4(6)	Identifier Management | Cross-organization Management					PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, CT.DP-P2, PR.AC-P1, PR.AC-P6
IA-4(8)	Identifier Management | Pairwise Pseudonymous Identifiers					PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, CT.DP-P2, PR.AC-P1, PR.AC-P6
IA-4(9)	Identifier Management | Attribute Maintenance and Protection					PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, CT.DP-P2, PR.AC-P1, PR.AC-P6
IA-5	Authenticator Management		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
IA-5(1)	Authenticator Management | Password-based Authentication		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(2)	Authenticator Management | Public Key-based Authentication			x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(5)	Authenticator Management | Change Authenticators Prior to Delivery					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(6)	Authenticator Management | Protection of Authenticators			x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(8)	Authenticator Management | Multiple System Accounts					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(9)	Authenticator Management | Federated Credential Management					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(10)	Authenticator Management | Dynamic Credential Binding					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
IA-5(12)	Authenticator Management | Biometric Authentication Performance					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(14)	Authenticator Management | Managing Content of PKI Trust Stores					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(15)	Authenticator Management | GSA-approved Products and Services					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(16)	Authenticator Management | In-person or Trusted External Party Authenticator Issuance					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(17)	Authenticator Management | Presentation Attack Detection for Biometric Authenticators					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-5(18)	Authenticator Management | Password Managers					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-6	Authentication Feedback		x	x	x		
IA-7	Cryptographic Module Authentication		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-P1

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
IA-8	Identification and Authentication (non-organizational Users)		x	x	x	PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6
IA-8(1)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies		x	x	x	PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6
IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators		x	x	x	PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6
IA-8(4)	Identification and Authentication (non-organizational Users) | Use of Defined Profiles		x	x	x	PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6
IA-8(5)	Identification and Authentication (non-organizational Users) | Acceptance of PIV-I Credentials					PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6
IA-8(6)	Identification and Authentication (non-organizational Users) | Disassociability					PR.AC, CT.DP-P, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-7, CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
IA-9	Service Identification and Authentication					PR.AC, PR.AC-P	PR.AC-1, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-10	Adaptive Authentication					PR.AC, PR.AC-P	PR.AC-1, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-11	Re-authentication		x	x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-7, PR.AC-P1, PR.AC-P6
IA-12	Identity Proofing			x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-P1, PR.AC-P6
IA-12(1)	Identity Proofing | Supervisor Authorization					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-P1, PR.AC-P6
IA-12(2)	Identity Proofing | Identity Evidence			x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-P1, PR.AC-P6
IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification			x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-P1, PR.AC-P6
IA-12(4)	Identity Proofing | In-person Validation and Verification				x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-P1, PR.AC-P6
IA-12(5)	Identity Proofing | Address Confirmation			x	x	PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-P1, PR.AC-P6
IA-12(6)	Identity Proofing | Accept Externally-proofed Identities					PR.AC, PR.AC-P	PR.AC-1, PR.AC-6, PR.AC-P1, PR.AC-P6