

Information Security – Identification and Authentication (IA) Procedure

1. PURPOSE

The Environmental Protection Agency (EPA) is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. **All EPA information systems shall meet** the security requirements by implementing the security controls defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

The purpose of this procedure is to facilitate the implementation of the EPA security control requirements for the Identification and Authentication (IA) control family, as identified in NIST SP 800-53, Revision 5.

2. SCOPE

These procedures address all EPA information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
 - Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," July 2016
 - FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
-

- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020
- OMB Memorandum M-05-24, Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005
- OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," January 2022

5. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "IA" designator (e.g., IA-2, IA-3) identified for each procedure below corresponds to the NIST- identifier for the Identification and Authentication control family, as identified in NIST SP 800-53, Revision 5.

NIST defines the applicable IA baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations*. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name. EPA may deviate from the NIST 800-53B Security or Privacy Control Baselines by adding/removing controls or to applicable baselines and are notated with an asterisk.

IA-2 – Identification and Authentication (Organizational Users)

For All Systems:

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

IA-2(1) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts

For All Systems:

- 1) Implement multifactor authentication for access to privileged accounts.

IA-2(2) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-privileged Accounts

For All Systems:

- 1) Implement multifactor authentication for access to non-privileged accounts.

IA-2(5) – Identification and Authentication | Individual Authentication with Group Authentication

For High Systems:

- 1) 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) – Identification and Authentication | Access to Accounts – Separate Device

For All Systems*:

- 1) Implement multi-factor authentication for local; network; and remote access to privileged accounts 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 Identity Assurance Levels (IAL) based on the results from the Digital Identity Risk Assessments (DIRA) in accordance with the EPA DIRA guidance for each Federal Information Security Modernization Act (FISMA) system in conjunction with these events: (1) initial system deployment, (2) annual security assessments or (3) when significant changes are made to the information system.

IA-2(8) – Identification and Authentication | Access to Accounts – Replay Resistant

For All Systems:

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

IA-2(12) – Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

For All Systems:

- 1) Accept and electronically verify Personal Identify Verification-compliant credentials.

IA-3 – Device Identification and Authentication

For Moderate and High Systems:

- 1) Uniquely identify and authenticate end user-operated devices (e.g., workstations, laptops, voice-over-Internet Protocol (VoIP) phones, cell phones) and servers before establishing a local, remote, or network connection.

IA-4 – Identifier Management

For All Systems:

- 1) Manage system identifiers by:
 - a) Receiving authorization from the supervisor/sponsor and Information Management Officer (IMO), SO, or ISO to assign 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 three (3) years.

IA-4(4) – Identifier Management | Identify User Status

For Moderate and High Systems:

- 1) Manage individual identifiers by uniquely identifying each individual as either a federal staff member, contractor, non-organizational user (academic or researcher for example) or Foreign National.

IA-5 – Authenticator Management

For All Systems:

- 1) 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 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 or compromised or damaged authenticators, and for revoking authenticators;
 - e) Changing default authenticators prior to first use;
 - f) Changing or refreshing authenticators:
 - i) For systems that **enforce** multi-factor authentication (MFA), there is **no rotation requirement**;
 - ii) When an authenticator is lost, stolen, or compromised;
 - 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.

IA-5(1) – Authenticator Management | Password-based Authentication

For All Systems:

- 1) For password-based authentication:
 - a) Maintain a list of commonly-used, expected, or compromised passwords and update the list annually 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) 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:
 - i) Passwords shall be at least twelve (12) non-blank characters long;
 - ii) The PIN shall be at least eight (8) non-blank characters long;
 - iii) For systems that do not enforce MFA, all passwords, including initial passwords, shall be composed of a minimum of one (1) character from each of the four (4) categories listed below:
 - iv) English uppercase characters (e.g., A-Z);
 - v) English lowercase letters (e.g., a-z);
 - vi) Base 10 Digits/Numerals (e.g., 0-9); or
 - vii) Non-Alphanumeric special characters (e.g., ! @, #, \$, %, ^, &, etc.);
 - viii) Passwords shall not contain any of the following:
 - ix) Dictionary words (e.g., computer, work) or common names (e.g., Betty, Fred, Rover);
 - x) Portions of associated account names (e.g., user ID, login name);
 - xi) Consecutive character strings (e.g., abcdef, 12345);
 - xii) Simple keyboard patterns (e.g., QWERTY, asdfgh); or
 - xiii) Generic passwords (i.e., password consisting of a variation of the word “password” [e.g., P@ssw0rd1]).

IA-5(2) – Authenticator Management | Public Key-based Authentication

For Moderate and High Systems:

- 1) For public key-based authentication:
 - a) Enforce authorized access to the corresponding private key; and
 - b) Map the authenticated identity to the account of the individual or group; and
- 2) When public key infrastructure (PKI) is used:
 - a) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
 - b) Implement a local cache of revocation data to support path discovery and validation.

IA-5(6) – Authenticator Management | Protection of Authenticators

For Moderate and High Systems:

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

IA-6 – Authenticator Feedback

For All Systems:

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

IA-7 – Cryptographic Module Authentication

For All Systems:

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

IA-8 – Identification and Authentication (Non-organizational Users)

For All Systems:

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

IA-8(1) – Identification and Authentication (Non-organizational Users) | Acceptance PIV Credentials from Other Agencies

For All Systems:

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

IA-8(2) – Identification and Authentication (Non-organizational Users) | Acceptance of External Authenticators.

For All Systems:

- 1) Accept only external authenticators that are NIST-compliant; and
- 2) Document and maintain a list of accepted external authenticators.

IA-8(4) – Identification and Authentication (Non-organizational Users) | Use of Defined Profiles

For All Systems:

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

IA-11 – Re-authentication

For All Systems:

- 1) Require users to re-authenticate when switching roles, such as, from a non-privileged role to a role with elevated privileges and vice versa; when the system or session times out (see AC-2(5), AC-7, AC-11, AC-12); and when authenticators or credentials change.

IA-12 – Identity Proofing

For Moderate and High Systems:

- 1) 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;
- 2) Resolve user identities to a unique individual; and
- 3) Collect, validate, and verify identity evidence.

IA-12(2) – Identity Proofing | Identity Evidence

For Moderate and High Systems:

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

IA-12(3) – Identity Proofing | Identity Evidence Validation and Verification

For Moderate and High Systems:

- 1) Require that the presented identity evidence be validated and verified through the office or entity (e.g., login.gov for external users) that issued the credential.

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

For High Systems:

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

IA-12(5) – Identity Proofing | Address Confirmation

For Moderate and High Systems:

- 1) Require that a registration code (e.g., temporary code sent to email or telephone) or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

COMMON CONTROL PROVIDER (CCP)

- 1) CCPs have the following responsibilities with respect to identification and authentication:
 - a) Coordinate with the CIO, CISO, IOs, SOs, ISOs, IMOs, and SMs regarding information security requirements, and determine and carry out responsibilities for defining, developing, documenting, implementing, assessing, and monitoring all controls to include common and hybrid controls.
 - b) Assist the SOs and IOs with developing, implementing, assessing, configuring, continuously monitoring and determining common controls to adequately protect information stored, processed or transmitted within acceptable risks.
 - c) Coordinate with SOs and IOs to identify controls required to adequately protect information stored, processed, or transmitted by assigned systems.
 - d) Assist SOs and IOs with determining information systems security controls in accordance with the Agency’s security requirements)

INFORMATION OWNERS (IO)

- 1) The IO has the following responsibilities with respect to identification and authentication:
 - a) Authorize and approve all special accounts; ensure they are monitored while in use; and that they are removed, disabled or otherwise secured when not in use. Special accounts include guest, training, anonymous maintenance or temporary emergency accounts.

INFORMATION MANAGEMENT OFFICER (IMO)

- 1) IMOs have the following responsibilities with respect to identification and authentication:
 - a) Ensure independent assessors and/or assessment teams conduct assessments.
 - b) Ensure testing and exercises are conducted in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

INFORMATION SECURITY OFFICERS (ISO)

- 1) ISOs have the following responsibilities with respect to identification and authentication:
 - a) Provide expert advice in developing and updating enterprise and local information security documents to include policy, procedures, standards, and guides.
 - b) Coordinate with and supporting the IMO and AODR in implementing EPA Information Security Program requirements.
 - c) Provide expert advice in:
 - i) developing and updating mandatory configurations for information technology products and solutions used by EPA;
 - ii) determining local controls to ensure compatibility and interoperability with enterprise tools and controls; and
 - iii) implementing, operating, and maintaining enterprise tools and controls.

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

- 1) The ISSO has the following responsibilities with respect to identification and authentication:
 - a) Ensure the day-to-day security operations of an information system, including verifying security controls (technical or otherwise) are functioning as intended.

OFFICE OF MISSION SUPPORT (OMS)

- 1) OMS has the following responsibilities with respect to identification and authentication:
 - a) Ensure that smart card certificates are compatible and

capable of implementing identification and authentication requirements.

- b) Register and issue HSPD-12 PIV cards.

OFFICE OF INFORMATION TECHNOLOGY OPERATIONS (OITO)

- 1) OITO has the following responsibilities with respect to identification and authentication:
 - a) Provide central management of identification and authentication to ensure unique naming of users and devices.
 - b) Develop enterprise identification and authentication standards as needed to ensure consistency.
 - c) Coordinate with the Office of Mission Support (OMS) on personnel and identification requirements associated with smart card issuance and implementation.

SERVICE MANAGERS (SM)

- 1) SMs have the following responsibilities with respect to identification and authentication:
 - a) Establish and administer privileged user accounts in accordance with a role- based access scheme that organizes information system and network privileges into roles.

SECURITY CONTROL ACCESSORS (SCA)

- 1) SCAs have the following responsibilities with respect to identification and authentication:
 - a) Test security controls according to the security assessment plan in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
 - b) Provide SO and IO with documented information system security assessment results (i.e., SAR).

SYSTEM OWNER (SO)

- 1) The SO has the following responsibilities with respect to identification and authentication:
 - a) Conduct a DIRA
 - b) Manage user and device identifiers, as applicable.
 - c) Ensure that upgrades or patches do not reinstall factory default passwords or other types of backdoors.
 - d) Ensure that appropriate identification,

Policy No: CIO 2120-P-7.4

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

authentication, and authorization are implemented.

USERS/INDIVIDUALS

- 1) Users/individuals have the following responsibilities with respect to identification and authentication:
 - a) Notify their supervisors immediately if they suspect their password, PIN, or other authenticator has been compromised.
 - b) Report a known or potential security breach to the EPA Call Center.
 - c) Change a compromised password or request the EPA Call Center to reset or change their password immediately.
 - d) Take reasonable measures to safeguard authenticators.

7. RELATED INFORMATION

- NIST SP 800-63B, Digital Identity Guidelines: Authentication & Lifecycle Management, June 2017
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **Assurance** – for identity authentication, (1) the degree of confidence in the vetting process used to establish the identity of the individual or device to which the credential was issued, and (2) the degree of confidence that the individual or device that uses the credential is the resource to which the credential was issued.
- **Authentication** – the process of verifying the identity of an individual, group, role, process or device, often as a prerequisite to allowing access to resources in an information system.
- **Identity** – the unique representation of a subject, for example, a person, a device, a non-person entity (NPE), or an automated technology, that is engaged in a transaction involving at least one Federal subject or a Federal resource, for example, Federal information, a Federal information system, or a Federal facility or secured area.
- **Local Access** – access to an organizational information system by a user, or process acting on behalf of a user, where such access is obtained by direct connection without the use of a network.

- **Memorized Secret** – a type of authenticator comprised of a character string intended to be memorized or memorable by the user, permitting the user to demonstrate something they know as part of an authentication process.
- **Multifactor Authentication** – the process of using two or more different factors for verifying identity. Factors are typically categorized as “something you know” (e.g., a password), “something you have” (e.g., a token) and “something you are” (e.g., a biometric).
- **Network Access** – access to an organizational information system by a user, or process acting on behalf of a user, where such access is obtained through a network connection.
- **Non-organizational Users** – all information system users other than organizational users explicitly covered by IA-2.
- **Non-Person Entity (NPE)** – An entity with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts
- **Organizational Users** – organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations).
- **Out of Band (OOB)** - Used to refer to information transmitted through a separate communications channel.
- **Remote Access** – a type of network access that involves communication through an external network (e.g., the Internet).
- **Signature** (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance or obligation (can be accomplished manually, sometimes referred to as a “wet signature,” or electronically).
- **Significant Change** – A significant change is defined as a change that is likely to affect the security state of an information system. Significant changes to an information system may include for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.
- **Written** (or in writing) – to officially document the action or decision, either manually or electronically, and includes a signature.

Policy No: CIO 2120-P-7.4

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

9. WAIVERS

Waivers or deviation may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. POLICY(S) SUPERSEDED

This procedure supersedes Information Directive: CIO 2120-P-07.3, Information Security – Identification and Authentication Procedure, January 30, 2023

11. CONTACTS

For information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

Carter Farmer
Chief Information Officer
U.S Environmental Protection Agency

Policy No: CIO 2120-P-7.4

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
DIRA	Digital Identity Risk Assessments
EPA	Environmental Protection Agency
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD-12	Homeland Security Presidential Directive 12
IA	Identification and Authentication
IAL	Identity Assurance Levels
IMO	Information Management Officer
ISO	Information Security Officer
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
OMB	Office of Management and Budget
OMS	Office of Mission Support
OISP	Office of Information Security and Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SO	System Owner
SP	Special Publication
U.S.C.	United States Code
VOIP	Voice-Over-Internet Protocol