EPA IT/IM DIRECTIVE
PROCEDURE

Information Security – Identification and Authentication (IA) Procedure

Directive No: CIO 2120-P-07.3

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

Information Security – Identification and Authentication (IA) Procedure

1. PURPOSE

To implement security control requirements for the Identification and Authentication (IA) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE

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

The procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that 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 must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document addresses the procedures and standards set forth by the EPA to implement the family of Identification and Authentication controls.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) as amended
- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)

- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act (44 USC 3501-3519), May 1995
- Privacy Act of 1974 (5 USC § 552a), as amended
- Office of Management and Budget (OMB) Memorandum M-04-04, E-Authentication Guidance for Federal Agencies*,* December 2003
- OMB Memorandum M-05-24, Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004
- OMB Memorandum M-06-16, “Protection of Sensitive Agency Information,” June 2006
- OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC),” November 2007
- OMB Memorandum M-08-22, “Guidance on the Federal Desktop Core Configuration (FDCC),” August 2008
- OMB Memorandum M-14-04, “Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management,” November 2013
- OMB Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” September 2022
- Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- Federal Information Processing Standards (FIPS) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Information Security – Roles and Responsibilities Procedures
- CIO Policy Framework and Numbering System

6. PROCEDURE

For the following section titles, the "IA" designator identified in each procedure represents the NIST-specified identifier for the Identification and Authentication *control family* and the number represents the *control identifier*, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Abbreviations including acronyms are summarized in Attachment A.

IA-2 – Identification and Authentication

For All Information Systems:

1) System Owners (SO), in coordination with Information Security Officers (ISO), Information Management Officers (IMO), Information Owners (IO), Information System

Security Officers (ISSO), Common Control Providers (CCP), and Security Control Assessors (SCA), for EPA-operated systems shall; and Service Managers (SM), in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure information systems to uniquely identify and authenticate users (or processes acting on behalf of users).

Note: Users include EPA employees, contractors, interns, and others that access EPA information and information systems.

i) Users shall be uniquely identified and authenticated for all access other than those accesses explicitly identified and documented as exceptions regarding permitted actions without identification and authentication.

(1) Refer to the latest version of the *EPA Information S*ecurity – *Access Control Procedures* for requirements on permitted actions without identification and authentication.

(2) Unique identification of individuals in group accounts (e.g., shared privilege accounts) may not be needed for detailed accountability of activity depending upon risks. SOs shall base their recommendation to not use unique identifiers for individuals in group accounts on a risk assessment.

b) Implement identification and authentication mechanisms at the application level, as determined by a risk assessment, to provide increased security for the information system and the information processes. This shall be in addition to identifying and authenticating users at the information system level (e.g., when initially logging into a desktop, laptop or smart phone).

c) Authenticate user identities through the use of passwords, personal identification numbers (PINs), tokens, biometrics, or in the case of multifactor authentication, some combination thereof[1].

IA-2(1) – Identification and Authentication | Network Access to Privileged Accounts

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Implement multifactor authentication with assurance level 4[2] for network access[3] to privileged accounts.

[1] *Multifactor authentication consists of factors of different types, e.g., for two-factor authentication, an acceptable combination is where one is something you know (PIN) and one is something you have (PIV card). Two of the same factor types, e.g., both factors are something you know, is not two-factor.*

[2] *Assurance levels are defined in National Institute for Standards and Technology, Special Publication 800-63 rev 2.*

[3] *Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access*

IA-2(2) – Identification and Authentication | Network Access to Non-Privileged Accounts

For Moderate and High impact Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Use multifactor authentication for network access to non-privileged accounts.

IA-2(3) – Identification and Authentication | Local Access to Privileged Accounts

For all Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Use multifactor authentication with assurance level 4 for local access to privileged accounts.

IA-2(4) – Identification and Authentication | Local Access to Non-Privileged Accounts

For High impact Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Implement multifactor authentication for local access to non-privileged accounts.

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

For FedRAMP[4] Moderate Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
    a) Requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

IA-2(6) – Identification and Authentication | Network Access to Privileged Accounts – Separate Device

Not selected as part of the control baseline.

to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses).

[4] *The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.*

IA-2(7) – Identification and Authentication | Network Access to Privileged Accounts – Separate Device

Not selected as part of the control baseline.

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

For Moderate and High impact Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Use replay-resistant authentication protocols for network access to privileged accounts.
      i) Techniques used to address this include protocols that use challenges (e.g., Transport Layer Security TLS), and time synchronous or challenge-response one- time authenticators.

IA-2(9) – Identification and Authentication | Network Access to Non-Privileged Accounts – Replay Resistant

For High impact Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Use replay-resistant authentication protocols for network access to non-privileged accounts.
      i) Techniques used to address this include protocols that use challenges (e.g., Transport Layer Security TLS), and time synchronous or challenge-response one- time authenticators.

IA-2(10) – Identification and Authentication | Single Sign-On

Not selected as part of the control baseline.

IA-2(11) – Identification and Authentication | Remote Access – Separate Device

For Moderate and High impact Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Use multifactor authentication with assurance level 4 for remote access to privileged and non-privileged accounts such that a device separate from the system gaining access provides one of the factors and the device meets minimum token requirements.

b) Conduct Electronic Authentication (E-Authentication) Risk Assessments (e-RA) for agency information systems[5] that require authentication of public users remotely over an open network, such as the Internet.

i) e-RAs shall be conducted in accordance with OMB M-04-04, OMB M-14-04 and NIST SP 800-63, Revision 2 or its successors and shall be used to determine the compliance requirements for access consistent with FIPS 190, as amended.

ii) The e-RA shall be conducted as part of conducting a general risk assessment or it may be a separate activity, in which case it shall be informed by a general risk assessment for the information system.

(1) Refer to the latest version of the *EPA Information Security – Risk Assessment Procedures* for requirements on risk assessments.

iii) The e-RA process shall identify potential impacts should proper authentication fail or should there be an authentication error.

(1) These impacts are rated as low, moderate, or high risks.

iv) The identified risks shall be mapped to the appropriate assurance level. OMB M- 04-04 sets four identity authentication assurance levels:

(1) Level 1: Little or no confidence in the asserted identity's validity.
(2) Level 2: Some confidence in the asserted identity's validity.
(3) Level 3: High confidence in the asserted identity's validity.
(4) Level 4: Very high confidence in the asserted identity's validity.

v) The information system's System Security Plan (SSP) IA-2 control description shall state if E-Authentication is required and, if not required, an explanation shall be included (e.g., the system is a public site or the system does not require user authentication).

vi) Technologies for E-Authentication shall be selected and implemented based on technical guidance provided in NIST SP 800-63, Revision 2 as amended.

(1) Authenticators (e.g., passwords, randomly generated PINs, tokens, biometric, and other authenticators) and the selected technologies shall comply with Level 2, 3 or 4 requirements.
(2) Technology selection shall be based first on technology standards or approved technologies within the EPA's approved technology and security architecture.
(3) If available technologies and mechanisms prove inadequate, alternatives that are consistent with NIST guidance may be proposed.

vii) The guidance provided by NIST SP 800-63, Revision 2 shall apply to both local and remote access to the information system.

[5] *As defined in OMB issued Memorandum M-14-04, an e-authentication application is an application that meets the following criteria: 1) Is web-based; 2) Requires authentication; and 3) Extends beyond the borders of the enterprise (e.g. multi- agency, government-wide, or public facing). For additional e-authentication requirements, refer to NIST SP 800-63, Electronic Authentication Guidance, at http://csrc.nist.gov/publications.*

(1) Remote access connections shall be both authenticated and authorized to be accepted.

viii) Validation shall be conducted to ensure that the implemented system has met the required assurance level.

2) Identity Assurance Level (IAL): The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing errors.

3) Authenticator Assurance Level (AAL): The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication errors (i.e., a false claimant using a credential that is not rightfully theirs). Federation Assurance Level (FAL): The robustness of the assertion protocol the federation uses to communicate authentication and attribute information (if applicable) to a relying party. optional as not all digital systems will leverage federated identity architectures. FAL is selected to mitigate potential federation errors (i.e., an identity assertion is compromised).

c) Reassess the information system periodically, subsequent to the e-RA and in accordance with requirements of the information system's life cycle stage and Security Assessment and Authorization (SA&A) requirements, to determine technology refresh requirements.

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

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Configure systems to accept and electronically verify Personal Identity Verification (PIV) credentials. FIPS 201-1 and NIST SP 800-73, 800-76, and 800-78 shall be used as guidance on PIV credentials for use in the unique identification and authentication of federal employees and contractors[6].

IA-2(13) – Identification and Authentication | Out-of-Band Authentication

Not selected as part of the control baseline.

IA-3 – Device Identification and Authentication

For Moderate and High impact Information Systems:

[6] *Note: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use challenges (e.g., Transport Layer Security TLS), and time synchronous or challenge-response one-time authenticators.*

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Configure information systems to 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 network connection.
    b) Determine the required strength of the device authentication mechanism by the security categorization of the information system as well as an assessment of risk incurred.
    c) Use only approved procedures, mechanisms, or protocols for host or device authentication.
        i) Approved mechanisms and protocols include, but are not limited to, the following:
            (1) Media Access Control (MAC) address filtering, which provides basic filtering based on Open Systems Interconnection (OSI) Layer 2 (Data Link Layer) address information.
            (2) Vendor-specific solutions such as Cisco's Port Security, which provide basic identification and authentication for devices in a wired network on a per-port basis.
            (3) Wi-Fi Protected Access 2 (WPA2) in combination with MAC filtering.
            (4) Institute of Electrical and Electronics Engineers (IEEE) 802.1x.
            (5) Network Access Control (NAC) technology, which is most commonly built on the foundations of 802.1x.
    d) Document the procedures, mechanisms, or protocols used for device identification and authentication clearly, with diagrams, in the SSP.

IA-3(1) – Device Identification and Authentication | Cryptographic Bidirectional Authentication

Not selected as part of the control baseline.

IA-3(2) – Device Identification and Authentication | Cryptographic Bidirectional Network Authentication

Incorporated into IA-3(1).

IA-3(3) – Device Identification and Authentication | Dynamic Address Allocation

Not selected as part of the control baseline.

IA-3(4) – Device Identification and Authentication | Device Attestation

Not selected as part of the control baseline.

IA-4 – Identifier Management

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Receive authorization from a designated EPA official (e.g., system administrator, technical lead or system owner) to assign individual, group, role, or device identifiers.

   b) Select and assign information system identifiers that uniquely identify an individual, group, role, or device.
      i) Assignment of individual, group, role, or device identifiers shall ensure that no two users or devices have the same identifier.

   c) Prevent reuse of identifiers for seven (7) years.

   d) Disable identifiers after 30 days of inactivity.

   e) Delete or archive user accounts with more than 365 days of non-use.

IA-4(1) – Identifier Management | Prohibit Account Identifiers as Public Identifiers

Not selected as part of the control baseline.

IA-4(2) – Identifier Management | Supervisor Authorization

Not selected as part of the control baseline.

IA-4(3) – Identifier Management | Multiple Forms of Certification

Not selected as part of the control baseline.

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

For Moderate impact Information Systems hosted by a FedRAMP compliant cloud environment:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:

   a) Manage individual identifiers by uniquely identifying each individual as either Contractors or Foreign Nationals.

IA-4(5) – Identifier Management | Dynamic Management

Not selected as part of the control baseline.

IA-4(6) – Identifier Management | Cross-Organizational Management

Not selected as part of the control baseline.

IA-4(7) – Identifier Management | In-Person Registration

Not selected as part of the control baseline.

IA-5 – Authenticator Management

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Verify the identity of the individual, group, role, or device receiving an information system authenticator as part of the initial authenticator distribution.

      i) Unique initial authenticator content shall be established for information system authenticators.

         Note: Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length).

      ii) Authenticators for individuals, groups, roles, or devices shall have sufficient strength of mechanism for their intended use[7].

      iii) Administrative procedures shall be established and implemented for initial authenticator distribution, lost/compromised, or damaged authenticators, and for revoking authenticators.

         (1) If a user knows or suspects that their password has been compromised, they shall immediately:

            (a) Notify their supervisor.
            (b) Report a known or potential security breach to the EPA Call Center.
            (c) Request the EPA Call Center reset or change their password, or if self- service password mechanisms are used, immediately change their own password.

      iv) Default content of authenticators (i.e., passwords provided for initial entry to a system) shall be changed *before* implementation of the information system or component (e.g., routers, switches, firewalls, printers, workstations, servers).

         (1) The information system owner shall confirm that software and/or hardware upgrades, updates, and patches do not reinstall default passwords.

      v) Authenticators shall be changed or replaced periodically.

         (1) All newly assigned passwords shall be changed the first time a user logs into the information system.
         (2) For non-memorized secret authenticators[8], there is no rotation requirement.
         (3) For memorized secret authenticators:
            (a) For systems that enforce multi-factor authentication (MFA), there is no rotation requirement;

[7] *User authenticators include, for example, tokens, Public Key Infrastructure (PKI) certificates, biometrics, passwords, and key cards ("smart cards").*

[8] *A memorized secret authenticator – commonly referred to as a password or, if numeric, a PIN as defined in NIST SP 800-63B.*

(b) For systems that do not enforce MFA, authenticators must be rotated every sixty (60) days;

(4) When an authenticator is lost, stolen, or compromised.

(5) PIV (Smart Cards) certificates shall be renewed every three (3) years.

vi) The following minimum and maximum lifetime restrictions and re-use conditions shall be adhered to regarding authenticators:

(1) For systems that do not enforce MFA, passwords shall have a minimum lifetime of one (1) day and a maximum lifetime of 60 days.

(a) Passwords cannot be changed in less than one (1) day.

(2) Password reuse for a specific account is prohibited for 24 generations or four (4) years.

(a) Password history shall be set with a history of at least 24 passwords, so a user cannot quickly re-use a previous password.

vii) Authenticator content shall be protected from unauthorized disclosure and modification.

viii) Users shall take reasonable and specific measures to safeguard authenticators.

(1) Users shall maintain possession of their individual authenticators, not loan or share authenticators with others, and report lost or compromised authenticators immediately to their supervisor and the EPA Call Center as a security event.

(2) Devices shall be configured to safeguard authenticators (e.g., certificates, passwords).

ix) Authenticators for shared group/role accounts shall be changed when membership to those accounts changes.

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

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Ensure the information system enforces the following for password-based and PIN- based authentication:

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 enforce MFA, passwords, including initial passwords, shall be composed of a minimum of one (1) character from at least three (3) of the following four (4) categories, as provided in the application or operating system schema:

(1) English uppercase characters (e.g., A-Z);

(2) English lowercase letters (e.g., a-z);

(3) Non-Alphanumeric special characters (e.g., ! @, #, $, %, ^, &, etc.); and

(4) Base 10 Digits/Numerals (e.g., 0-9).

iv) 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 above.

(a) Passwords shall not contain any of the following:

(i) Dictionary words (e.g., computer, work) or common names (e.g., Betty, Fred, Rover).

(ii) Portions of associated account names (e.g., user ID, login name).

(iii) Consecutive character strings (e.g., abcdef, 12345).

(iv) Simple keyboard patterns (e.g., QWERTY, asdfgh).

(v) Generic passwords (i.e., password consisting of a variation of the word “password” [e.g., P@ssw0rd1]).

v) At least 50% of the characters shall be changed when new passwords are created.

vi) Passwords and PINs shall not be displayed when entered.

vii) Passwords and PINs shall be encrypted when stored and transmitted.

viii) Temporary passwords can be used to facilitate password changes or initial account establishment if the system forces an immediate change to a permanent password.

ix) A waiver of the password requirements and standards may be requested, provided the request includes at a minimum:

(1) Specific designation of which requirement(s) the waiver request is addressing.

(2) A detailed analysis of the password resistance to compromise in accordance with password entropy and strength factors detailed in Appendix A of NIST SP 800-63, Revision 2, as amended.

(a) FIPS 201-1 and NIST SP 800-73, 800-76, and 800-78 shall be used as guidance on PIV credentials.

(b) NIST SP 800-63, Revision 2 shall be used as guidance on remote electronic authentication.

(c) The information system, for hardware token-based authentication, such as PKI-based tokens, employs mechanisms that satisfy EPA-defined specific requirements and NIST SP 800-25 requirements on PKI technology.

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

For Moderate and High impact Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Enforce the following for PKI-based authentication on applicable information systems:

i) Certificates are validated by constructing a certification path with status information (e.g., certificate revocation lists, online certificate status protocol responses) to an accepted trust anchor.

ii) Authorized access is enforced to the corresponding private key.

iii) The authenticated identity is mapped to the user account.

IA-5(3) – Authenticator Management | In-Person or Trusted Third-Party Registration

For Moderate and High impact Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Enforce the registration process for EPA employees and contractors to receive HSPD- 12 Personal Identity Verification (PIV) Cards. The registration process shall be carried out in person with the Office of Administration and Resources (OARM) with authorization by a designated organizational official (e.g., a supervisor or manager).

   b) Enforce the registration process for EPA employees and contractors to receive an account with privileged access to the information system. The registration process shall be carried out in person with the Office of Technology Operations and Planning (OTOP) with authorization by a designated organizational official (e.g., a supervisor or manager).

IA-5(4) – Authenticator Management | Automated Support for Password Strength Determination

For Moderate impact Information Systems hosted by FedRAMP compliant cloud solutions:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:

   a) Employ automated tools to determine if password authenticators are sufficiently strong to satisfy defined requirements.

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

Not selected as part of the control baseline.

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

For Moderate impact Information Systems hosted by FedRAMP compliant cloud solutions:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:

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

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

For Moderate impact Information Systems hosted by FedRAMP compliant cloud solutions:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
    a) Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

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

Not selected as part of the control baseline.

IA-5(9) – Authenticator Management | Cross-Organization Credential Management

Not selected as part of the control baseline.

IA-5(10) – Authenticator Management | Dynamic Credential Association

Not selected as part of the control baseline.

IA-5(11) – Authenticator Management | Hardware Token-Based Authentication

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Employ mechanisms that satisfy NIST SP 800-63, Level 4 requirements for hardware token-based authentication.

IA-5(12) – Authenticator Management | Biometric Authentication

Not selected as part of the control baseline.

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

Not selected as part of the control baseline.

IA-5(14) – Authenticator Management | Managing Content of PKI Trust Stores

Not selected as part of the control baseline.

IA-5(15) – Authenticator Management | FICAM-Approved Products and Services

Not selected as part of the control baseline.

IA-6 – Authenticator Feedback

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs,

CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Ensure the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.
   i) Passwords shall be masked upon entry (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text.

b) Ensure feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

IA-7 – Cryptographic Module Authentication

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Configure the information system to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

      i) The applicable federal standard for authenticating to a cryptographic module is FIPS 140-2. Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use until a validation certificate is specifically revoked.

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

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Configure the information system to uniquely identify and authenticate non-EPA users or processes acting on behalf of non-EPA users. *(Non-EPA users include all information system users other than organizational users explicitly covered by IA-2 including individuals and processes that simply receive data/information from federal information systems. These individuals and processes are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14, "Permitted Actions without Identification or Authentication.")*
      i) Non-EPA users shall be uniquely identified and authenticated for all access other than those accesses explicitly identified and documented as exceptions regarding permitted actions without identification and authentication in control AC-14.

(1) Refer to the latest version of the *EPA Information Security – Access Control Procedures* for requirements on permitted actions without identification and authentication.

b) Use the results of the information system risk assessment to determine the authentication needs of the organization.

i) In accordance with the *E-Authentication E-Government* initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems).

ii) Scalability, practicality, and security shall be simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to EPA's operations, EPA's assets, individuals, other organizations, and the Nation.

IA-8(1) – Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials From Other Agencies

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure the information system to accept and electronically verify PIV credentials from other federal agencies.

IA-8(2) – Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure the information system to accept only Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials. This applies to organizational information systems that are accessible to the public. Third-party credentials are those credentials issued by nonfederal government entities approved by the FICAM Trust Framework Solutions initiative.

IA-8(3) – Identification and Authentication (Non-Organizational Users) | Use of FICAM- Approved Products

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs,

CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ only FICAM-approved information system components in public-facing systems to accept third-party credentials.

IA-8(4) – Identification and Authentication (Non-Organizational Users) | Use of FICAM- Issued Profiles

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs, and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Ensure the information system conforms to FICAM-issued profiles.

   b) Refer to IA-2 for identification and authentication requirements regarding information system access by organizational users.

IA-8(5) – Identification and Authentication (Non-Organizational Users) | Acceptance of PIV-I Credentials

Not selected as part of the control baseline.

IA-9 – Service Identification and Authentication

Not selected as part of the control baseline.

IA-9(1) – Service Identification and Authentication | Information Exchange

Not selected as part of the control baseline.

IA-9(2) – Service Identification and Authentication | Transmission of Decisions

Not selected as part of the control baseline.

IA-10 – Adaptive Identification and Authentication

Not selected as part of the control baseline.

IA-11 – Re-Authentication

Not selected as part of the control baseline.

7. ROLES AND RESPONSIBILITIES

Common Control Provider (CCP)

1) CCPs have the following responsibilities with respect to identification and authentication:

   a) Coordinate with the CIO, SAISO, 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 Administration and Resources Management (OARM)

1) OARM has the following responsibilities with respect to identification and authentication:
   a) Coordinate with OEI on personnel and identification requirements associated with smart card issuance and implementation.
   b) Ensure that smart card certificates are compatible and capable of implementing identification and authentication requirements.
   c) Register and issue HSPD-12 PIV cards.

Office of Technology Operations and Planning (OTOP), Office of Environmental Information (OEI)

1) OEI, OTOP 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 Administration and Resources Management (OARM) 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 an e-RA.
   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, 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.

8. RELATED INFORMATION

- NIST Special Publications, 800 series
- Federal Identity, Credential and Access Management (FICAM)

Related policy and procedures are available on OEI's Policy Resources website.
http://intranet.epa.gov/oei/imitpolicy/policies.htm

Related standards and guidelines are available on OEI's website.

9. 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* – a unique name of an individual, group, role, or device. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
- *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.
- *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.
- *Organizational Users* – organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations).
- *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).
- *Written* (or in writing) – to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- Substantive business case need(s)
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the agency.

The SAISO and Director, OTOP shall coordinate to maintain a central repository of all waivers.

11. MATERIAL SUPERSEDED

- Information Security – Identification and Authentication Procedure, CIO 2120-P-07.2, August 31, 2021.
- Information Security – Interim Identification and Authentication Procedures, CIO 2120-P-07.1, July 13, 2012.

12. CONTACTS

For further information about this procedure, please contact the Office of Mission Support – Environmental Information, Office of Information Security and Privacy.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.01.30 08:31:30 -05'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information
and Chief Information Officer
U.S. Environmental Protection Agency