

Department of the Interior
Security Control Standard
Identification and Authentication

January 2012

Version: 1.4



Signature Approval Page

| Designated Official | |
|---|--------------|
| Bernard J. Mazer, Department of the Interior, Chief Information Officer | |
| Signature: | Date: |

REVISION HISTORY

| Author | Version | Revision Date | Revision Summary |
|--------------------|---------|-------------------|---|
| Chris Peterson | 0.1 | January 10, 2011 | Initial draft |
| Timothy Brown | 0.2 | January 12, 2010 | Incorporated comments into body text |
| Timothy Brown | 0.21 | February 15, 2011 | Checked/added moderate cloud to high |
| Chris Peterson | 1.0 | February 18, 2011 | Final review of controls; removed margin notes. Retained margin notes re: “service provider” and/or “Joint Approval Board (JAB)” |
| Lawrence K. Ruffin | 1.1 | April 29, 2011 | Final revisions and version change to 1.1 |
| Lawrence K. Ruffin | 1.2 | May 10, 2011 | Incorporated recommended changes to IA-5 |
| Lawrence K. Ruffin | 1.3 | July 26, 2011 | Modified the IA-5 Control Enhancement 1 language in the Enhancement Supplemental Guidance to eliminate specific reference to AES 256 to instead require NIST FIPS 140-2 compliant/validated cryptographic modules |
| Lawrence K. Ruffin | 1.4 | January 18, 2012 | Revisions for closer alignment to FedRAMP Baseline Security Controls.v1.0 dated 1/6/2012 |
| | | | |
| | | | |
| | | | |
| | | | |

TABLE OF CONTENTS

REVISION HISTORY3

TABLE OF CONTENTS4

SECURITY CONTROL STANDARD: IDENTIFICATION AND AUTHENTICATION5

 IA-1 IDENTIFICATION AND AUTHENTICATION POLICIES AND PROCEDURES5

 IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)6

 IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION7

 IA-4 IDENTIFIER MANAGEMENT8

 IA-5 AUTHENTICATOR MANAGMENT8

 IA-6 AUTHENTICATOR FEEDBACK11

 IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION11

 IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)11

SECURITY CONTROL STANDARD: IDENTIFICATION AND AUTHENTICATION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Identification and Authentication (IA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

IA-1 IDENTIFICATION AND AUTHENTICATION POLICIES AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

- a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary.

The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy.

Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P1 | LOW IA-1 | MOD IA-1 | HIGH IA-1 |
|-----------|-----------------|-----------------|------------------|

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Applicability: All Information Systems

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local or network. Local access is any 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. Network access is any 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. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8. The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Related controls: AC-14, AC-17, AC-18, IA-4, IA-5.

Control Enhancements:

1. The information system uses multifactor authentication for network access to privileged accounts.
2. The information system uses multifactor authentication for network access to non-privileged accounts.
3. The information system uses multifactor authentication for local access to privileged accounts.
4. The information system uses multifactor authentication for local access to non-privileged accounts.
8. The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts.

Enhancement Supplemental Guidance: 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 nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators. The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.

9. The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.

Enhancement Supplemental Guidance: 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 nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

References: HSPD 12; OMB Memorandum 04-04; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

| | | | |
|-----------|---------------------|---------------------------------|--|
| P1 | LOW IA-2 (1) | MOD IA-2 (1) (2) (3) (8) | HIGH IA-2 (1) (2) (3) (4) (8) (9) |
|-----------|---------------------|---------------------------------|--|

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Applicability: Moderate and High Impact Information Systems

Control: The information system uniquely identifies and authenticates [Assignment: organization defined list of specific and/or types of devices] before establishing a connection.

Supplemental Guidance: The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

| | | | |
|-----------|-------------------------|-----------------|------------------|
| P1 | LOW Not Selected | MOD IA-3 | HIGH IA-3 |
|-----------|-------------------------|-----------------|------------------|

IA-4 IDENTIFIER MANAGEMENT

Applicability: All Information Systems

Control: The organization manages information system identifiers for users and devices by:

- a. Receiving authorization from a designated organizational official to assign a user or device identifier;
- b. Selecting an identifier that uniquely identifies an individual or device;
- c. Assigning the user identifier to the intended party or the device identifier to the intended device;
- d. Preventing reuse of user or device identifiers for at least two years; and
- e. Disabling the user identifier after 90 days of inactivity.

Supplemental Guidance: Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). Related control: AC-2, IA-2.

Control Enhancements:

4. The organization manages user identifiers by uniquely identifying the user as contractors; foreign nationals.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|---------------------|----------------------|
| P1 | LOW IA-4 | MOD IA-4 (4) | HIGH IA-4 (4) |
|-----------|-----------------|---------------------|----------------------|

IA-5 AUTHENTICATOR MANAGEMENT

Applicability: All Information Systems

Control: The organization manages information system authenticators for users and devices by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined 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/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators upon information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
- g. Changing/refreshing authenticators at least every 60 days, unless specified and allowed to be greater by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles specific to mobile devices (e.g., device authenticators for Portable Electronic Devices and Personal Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices), but not greater than 90 days;
- h. Protecting authenticator content from unauthorized disclosure and modification; and
- i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Supplemental Guidance: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.

Control Enhancements:

1. The information system, for password-based authentication:
 - a. Enforces minimum password complexity of 12 or more case sensitive characters, with a minimum of one character from at least three of the following four categories: uppercase, lowercase, numeric, and special (non-alphanumeric); unless other acceptable complexity rules or pattern checks are specified and allowed to be less complex by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles specific to mobile devices (e.g., device authenticators for Portable Electronic Devices and Personal Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices).
 - b. Enforces at least one changed character when new passwords are created;
 - c. Encrypts passwords in storage and in transmission;
 - d. Enforces password minimum and maximum lifetime restrictions of one day minimum; and 60 day maximum, unless specified and allowed to be greater by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles specific to mobile devices (e.g., device authenticators for Portable Electronic Devices and Personal

- Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices), but not greater than 90 days; and
- e. Prohibits password reuse for 24 generations.

Enhancement Supplemental Guidance: This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does *not* apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

Mobile devices, configured with content protection enabled using NIST FIPS 140-2 compliant/validated cryptographic modules and to automatically wipe all data after ten failed login attempts, may use strong passwords with as few as six (6) characters having at least one uppercase, lowercase, and numeric; and a minimum password age of 1 day and a maximum of 90 days. Mobile devices include Portable Electronic Devices and Personal Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices, but does not include portable laptop computers.

2. The information system, for PKI-based authentication:
 - a. Validates certificates by constructing a certification path with status information to an accepted trust anchor;
 - b. Enforces authorized access to the corresponding private key; and
 - c. Maps the authenticated identity to the user account.

Enhancement Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

3. The organization requires that the registration process to receive HSPD12 smart cards shall be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).
6. The organization protects authenticators commensurate with the classification or sensitivity of the information accessed.
7. The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Enhancement Supplemental Guidance: Organizations exercise caution in determining whether an embedded or stored authenticator is in encrypted or unencrypted form. If the authenticator in its stored representation, is used in the manner stored, then that representation is considered an unencrypted authenticator. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

References: OMB Memorandums 04-04, 06-16, 07-16; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; NIST Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB).

Priority and Baseline Allocation:

| | | | |
|-----------|---------------------|--|---|
| P1 | LOW IA-5 (1) | MOD IA-5 (1) (2) (3) (6) (7) | HIGH IA-5 (1) (2) (3) (6) (7) |
|-----------|---------------------|--|---|

IA-6 AUTHENTICATOR FEEDBACK

Applicability: All Information Systems

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

Control Enhancements: None.

References: None

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P1 | LOW IA-6 | MOD IA-6 | HIGH IA-6 |
|-----------|-----------------|-----------------|------------------|

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Applicability: All Information Systems

Control: The information system uses 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.

Supplemental Guidance: None.

Control Enhancements: None.

References: FIPS Publication 140-2; Web: CSRC.NIST.GOV/CRYPTVAL.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P1 | LOW IA-7 | MOD IA-7 | HIGH IA-7 |
|-----------|-----------------|-----------------|------------------|

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Applicability: All Information Systems

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include all information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. 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). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are 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 organizational operations, organizational assets, individuals, other organizations, and the Nation. Identification and authentication requirements for information system access by organizational users are described in IA-2. Related controls: AC-14, AC-17, AC-18, MA-4.

Control Enhancements: None.

References: OMB Memorandum 04-04; Web: WWW.CIO.GOV/EAUTHENTICATION; NIST Special Publication 800-63.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P1 | LOW IA-8 | MOD IA-8 | HIGH IA-8 |
|-----------|-----------------|-----------------|------------------|