



IT Security Handbook

Identification and Authentication

ITS Handbook (ITS-HBK-2810.17-01)
Identification and Authentication

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

May 6, 201

Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

Change History	3 -
1 Introduction and Background	5 -
2 Organizational Users (IA-2)	6 -
3 Device Identification and Authentication (IA-3)	6 -
4 Identifier Management (IA-4)	6 -
5 Authenticator Management (IA-5)	7 -
6 Authenticator Feedback (IA-6)	7 -
7 Cryptographic Module Authentication (IA-7)	7 -
8 Non-Organizational Users (IA-8)	7 -
9 Organizationally Defined Values	8 -

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.1 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Identification and Authentication (IA) information security controls.
- 1.2 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.3 - The Identification and Authentication control family relates to the activities and provisions which ensure the identity of a given entity requesting access to NASA resources (e.g., a person logging in to a computer, or a laptop computer connecting to a wireless network). The controls address the creation, management, usage, and protection of identities (e.g., usernames) and authenticators (e.g., smart cards and tokens).
- 1.4 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NPR 1600.1, NASA Security Program Procedural Requirements*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *NM 1600-52, Office of Security and Program Protection Personal Identity Validation Policy and Procedures*
 - *EA-STD-0001, Standard for Integrating Applications into the NASA Access Management, Authentication, and EA-SOP-0004, Procedures for Submitting an Application Integration Deviation Request and Transition Plan*
 - *Homeland Security Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Federal Employees and Contractors*
 - *OMB M-04-04, E-Authentication Guidance for Federal Agencies*
 - *OMB M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors*
 - *Authorization Infrastructure*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *NIST SP 800-63, Electronic Authentication Guideline*

2 Organizational Users (IA-2)

2.1 - Roles and Responsibilities

2.1.1 *The NASA Chief Information Officer (CIO) shall:*

2.1.1.1 - Provision for Agency-wide compliance with *Homeland Security Presidential Directive 12 (HSPD-12)*.

2.1.1.1.1 - *HSPD-12*, Policy for a Common Identification Standard for Federal Employees and Contractors, and its supporting documents require identifying all persons who require access to NASA non-public information systems and networks. *HSPD-12* requires the use of a mandatory, government-wide standard for secure and reliable forms of identification for Federal Employees and contractors. Although some authentication credentials may be restricted for certain types of data, authentication credentials currently accepted for general use with NASA systems are:

2.1.1.1.2 - User Identification (User ID) and password;

2.1.1.1.3 - PIV Authorization Certificate and Personal Identification Number (PIN); and

2.1.1.1.4 - User ID, PIN, and RSA® SecurID token code.

2.1.1.2 - Provision for Agency-wide compliance with *OMB M-04-04*, and *OMB M-05-24*.

2.1.1.2.1 - *OMB Memorandum M-05-24* requires that PIV II-compliant smartcards be used for access to all on-site systems by all permanent on-site employees.

2.1.1.2.2 - The IdMAX system manages identities for use throughout NASA and establishes the Agency Unique ID (AUID) which is unique across NASA.

2.1.1.2.3 - IdMAX contains the NASA Account Management System (NAMS) tool which supports the creation, modification, and deletion of accounts for all NASA systems. The NASA Agency Forest (NAF) and E-Authentication provide central authentication and authorization services that support the NASA-accepted credentials.

2.1.2 *The Information System Owner (ISO) shall:*

2.1.2.1 - Ensure that, except for public websites, information system users are uniquely identified and authenticated for access to NASA information systems.

2.1.2.2 - Ensure that, except for public websites, the minimum authentication for NASA information systems are at least *NIST SP 800-63* Level 2 compliant. (Note: A more stringent authentication may be specified/required by these information system security requirements or by the ISO).

2.1.2.3 - Ensure that for NASA information systems, 2-factor identification using the PIV card or RSA SecurID, is required for network access to privileged accounts. (Note: "Privileged Accounts" are also referred to as "Elevated Privileges").

2.1.2.4 - When employing multifactor authentication for local and remote access to information systems, ensure that it is *NIST SP 800-63* Level 4 compliant using the PIV card, or RSA SecurID.

2.1.2.4.1 - 2-factor identification using the PIV card or RSA SecurID shall be required for local access to non-privileged accounts.

2.1.2.5 - Ensure that for local system access, information systems employ a *NIST SP 800-63* Level 3 compliant (Entrust) or a *NIST SP 800-63* Level 4 compliant (RSA SecurID or PIV card).

2.1.3 *The NASA Account Management System (NAMS) Project Manager shall:*

2.1.3.1 - Ensure NAMS and IdMAX systems provide the NASA common infrastructure required to support the federal E-Authentication and HSPD-12 requirements.

3 Device Identification and Authentication (IA-3)

3.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

4 Identifier Management (IA-4)

4.1 - Roles and Responsibilities

4.1.1 *The ISO shall:*

ITS Handbook (ITS-HBK-2810.17-01) -
Identification and Authentication -

- 4.1.1.1 - Ensure that their information system uses the AUID for NASA User accounts within their applications residing on general purpose computers connected to NASA administrative IP networks. -
 - 4.1.1.1.1 - The NASA IdMAX System manages identities for use throughout NASA and establishes the AUID which is unique across NASA. -
- 4.1.2 *The IdMAX Project Manager shall:* -
 - 4.1.2.1 - Ensure IdMAX manages identities for use throughout NASA and establishes AUIDs which are unique across NASA. -
 - 4.1.2.2 - Ensure all NASA users are entered into the IdMAX system. -
 - 4.1.2.3 - Ensure AUIDs are not reused in a manner consistent with organizationally defined values. -
 - 4.1.2.4 - Ensure that IdMAX includes an archive of previously used identifiers precluded from reuse following archival in a manner consistent with organizationally defined values. -
 - 4.1.2.5 - Ensure user identifiers are disabled in a manner consistent with organizationally defined values. -
- 4.1.3 *The Information Technology Security Enterprise Data Warehouse (ITSEC-EDW) project manager shall:* -
 - 4.1.3.1 - Ensure that ITSEC-EDW establishes and centrally manages identifiers for IT devices which are unique across NASA. -

5 Authenticator Management (IA-5)

5.1 - Roles and Responsibilities

- 5.1.1 *The ISO shall:* -
 - 5.1.1.1 - Ensure PIV card enabled applications are implemented in accordance with the *NPR 1600.1*. -
 - 5.1.1.2 - Ensure the initial authenticator for devices (e.g. initial password and factory default settings) is changed upon installation. -
 - 5.1.1.3 - Ensure password-based authenticators are implemented in a manner consistent with organizationally defined values. -
- 5.1.2 *The NAMS Project Manager shall:* -
 - 5.1.2.1 - Ensure centralized authentication is provided by NAMS for information systems registered in NAMS. -

6 Authenticator Feedback (IA-6)

- 6.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system. -

7 Cryptographic Module Authentication (IA-7)

- 7.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system. -

8 Non-Organizational Users (IA-8)

8.1 - Roles and Responsibilities

- 8.1.1 *The ISO shall:* -
 - 8.1.1.1 - Ensure information systems uniquely identify and authenticate non-organizational users for access to NASA non-public information systems. -
 - 8.1.1.2 - Ensure a risk assessment is performed prior to implementing any authentication system for non-NASA Users in a manner consistent with *OMB M-04-04*. -
 - 8.1.1.3 - Ensure that identifiers assigned to non-organizational users do not conflict with identifiers assigned to organizational users if the information system will accept authentication for either. -
 - 8.1.1.4 - In cases of a conflict, the organizational user identity has priority. -

9 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control’s enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
IA	01	Identification and Authentication Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
IA	02	Identification and Authentication (Organizational Users)	E 8	[1]	Reference	List of replay-resistant authentication mechanisms used for network access to privileged accounts.		2-factor identification using the PIV card or RSA SecurID	2-factor identification using the PIV card or RSA SecurID
IA	02	Identification and Authentication (Organizational Users)	E 9	[1]	Reference	List of replay-resistant authentication mechanisms used for network access to non-privileged accounts.			2-factor identification using the PIV card or RSA SecurID
IA	04	Identifier Management	Main	[1]	Time Period	Prevention of the reuse of device identifiers.	10 Years	10 Years	10 Years
IA	04	Identifier Management	Main	[2]	Time Period	Disabling user identifiers.	60 Days	60 Days	60 Days

ITS Handbook (ITS-HBK-2810.17-01) -
Identification and Authentication -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
IA	05	Authenticator Management	Main	[1]	Time Period	Changing/refreshing authenticators.	PIV (Personal Identity Verification) authenticator change/refresh in accordance with OPS (Office of Protective Services) PIV card management and control	PIV authenticator change/refresh in accordance with OPS PIV card management and control	PIV authenticator change/refresh in accordance with OPS PIV card management and control
IA	05	Authenticator Management	E 1	[1]	Reference	Password complexity.	Use at least 3 of the 4 in the password of upper-case letters, lower-case letters, numbers, and special characters.	Use at least 3 of the 4 in the password of upper-case letters, lower-case letters, numbers, and special characters.	Use at least 3 of the 4 in the password of upper-case letters, lower-case letters, numbers, and special characters.
IA	05	Authenticator Management	E 1	[2]	Reference	Minimum number of characters when new passwords are created.	12	12	12
IA	05	Authenticator Management	E 1	[3]	Reference	Password lifetime restrictions.	1 Day - 60 Days	1 Day - 60 Days	1 Day - 60 Days
IA	05	Authenticator Management	E 1	[4]	Number	Prohibited password reuse period.	24 Uses	24 Uses	24 Uses
IA	05	Authenticator Management	E 3	[1]	Reference	Defined types and/or specific authenticators required for registration processes.		Authenticators for information system access	Authenticators for information system access