



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.17-02 v2024-02

Published: 2024-02-23

**Identification and Authentication
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	3
Document History Log	3
Approval	3
1. Introduction	4
1.1. Purpose	4
1.2. Scope	4
1.3. Point of Contact(s)	4
1.4. Applicability	5
1.5. Applicable Documents	5
1.5.1. Executive Orders (EOs)	5
1.5.2. Office of Management and Budget (OMB)	5
1.5.3. Federal Information Processing Standards (FIPS)	5
1.5.4. National Institute of Standards and Technology (NIST)	5
1.5.5. National Aeronautics and Space Administration (NASA)	5
1.5.6. Cancellations, Updates, Consolidations	5
2. Security Controls and Corresponding Roles and Responsibilities	6
2.1. Identification and Authentication (Organizational Users) (IA-2)	6
2.1.1. NASA Chief Information Officer (CIO)	6
2.1.2. Information System Owner (ISO)	6
2.1.3. NAMS Project Manager	7
2.2. Device Identification and Authentication (IA-3)	7
2.2.1. Information System Owner (ISO)	7
2.3. Identifier Management (IA-4)	7
2.3.1. Information System Owner (ISO)	7
2.3.2. IdMAX Project Manager	7
2.4. Authenticator Management (IA-5)	8
2.4.1. Information System Owner (ISO)	8
2.4.2. NAMS Project Manager	8
2.5. Authenticator Feedback (IA-6)	8
2.5.1. Information System Owner (ISO)	8
2.6. Cryptographic Module Authentication (IA-7)	8
2.6.1. Information System Owner (ISO)	8
2.7. Identification and Authentication (Non-Organizational Users) (IA-8)	8
2.7.1. Information System Owner (ISO)	8
Appendix A: Acronyms	9

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-02	Initial Draft
1.1	2013-04-30	Extended for 1 year.
1.2	2014-04-24	Extended while revision 4 updates are rolled into the Handbook.
1.3	2015-03-03	Revised for Rev 4 controls & ODVs, updated TOC
1.4	2017-02-14	Extended due to updates
1.5	2017-04-14	Updated to reflect new tools and maintain consistency with referenced documents/standards
1.6	2018-08-03	Reformatted, minor updates
1.7	2021-09-30	Minor updates for SP 800-53r5
1.8	2023-01-31	Annual update.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update

Approval



Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

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 ([FIPS 199, *Standards for Security Categorization of 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*](#)), in a manner consistent with the Risk Management Framework ([NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)). [NPD 2810.1, *NASA Information Security Policy*](#), [NPR 2810.1, *Security of Information and Information Systems*](#), and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of [SP 800-53](#).

[NPR 2810.1](#) designates this handbook as a guide of NASA's Identification and Authentication (IA) information security controls, and the content of this document, in conjunction with [NPD/R 2810.1](#), defines NASA policy and procedures to address [IA-1](#).

This handbook supports implementation of requirements in [NPR 2810.1](#) and [NPD 2810.1](#). It also augments NIST guidance with NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within RSAARCHER in the Risk Information Security Compliance System (RISCS).

1.1. Purpose

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).

1.2. Scope

This Handbook applies to authentication on all NASA systems by both organizational and non-organizational users.

Although NASA handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. However, pursuant to [NPR 1400.1](#), portions of NASA handbooks containing procedural or process guidance may be cited in contract, program, and other Agency documents, and may become requirements when a NASA directive specifies their use by citing the document title, revision letter/number, and date; or, when a NASA manager with authority over a NASA program, project, or other activity, identifies it as a requirement.

This Handbook and the procedural guidance contained within remains in full force and effect until such time that the Handbook is formally cancelled, rescinded, or superseded by an updated document.

A documented rationale and/or justification will accompany any non-concurrence, disapproval, denial, or request for deviation from the procedural guidance set forth in this Handbook to support such decision. The documented rationale/justification is provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Chief Information Security Officers (CISO), to review and validate for the record.

1.3. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- hq-dl-cspd-policy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular Handbook to address and resolve.

1.4. Applicability

This handbook is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

1.5. Applicable Documents

1.5.1. Executive Orders (EOs)

- [Homeland Security Presidential Directive 12 \(HSPD-12\), *Policy for a Common Identification Standard for Federal Employees and Contractors*](#)

1.5.2. Office of Management and Budget (OMB)

- [OMB M-04-04, *E-Authentication Guidance*](#)
- [OMB M-05-24, *Implementation of Homeland Security Presidential Directive \(HSPD\) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*](#)

1.5.3. Federal Information Processing Standards (FIPS)

- [FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*](#)
- [FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*](#)
- [FIPS 201-3, *Personal Identity Verification \(PIV\) of Federal Employees and Contractors*](#)

1.5.4. National Institute of Standards and Technology (NIST)

- [NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)
- [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#)
- [NIST SP 800-63-3, *Digital Identity Guidelines*](#)

1.5.5. National Aeronautics and Space Administration (NASA)

- [NPD 2810.1, *NASA Information Security Policy*](#)
- [NPR 1600.1, *NASA Security Program Procedural Requirements*](#)
- [NPR 2810.1, *Security of Information and Information Systems*](#)
- [IT-HBK-2841-03A, *Identity, Credential, and Access Management \(ICAM\) Services*](#)

1.5.6. Cancellations, Updates, Consolidations

- ITS-HBK-2810.17-01, Identification and Authentication

2. SECURITY CONTROLS AND CORRESPONDING ROLES AND RESPONSIBILITIES

2.1. Identification and Authentication (Organizational Users) (IA-2)

2.1.1. NASA Chief Information Officer (CIO)

The NASA CIO shall:

- Provision for Agency-wide compliance with [HSPD-12](#).
 - [Homeland Security Presidential Directive 12 \(HSPD-12\), 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](#) mandates the use of a 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:
 - Personal Identity Verification (PIV) smart card certificate and Personal Identification Number (PIN);
 - Agency Smart Badge (ASB) smart card certificate and PIN;
 - User ID, PIN, and RSA® SecurID token code (with limited approval);
 - User Identification (User ID) and password (with limited approval).
- Provision for Agency-wide compliance with [OMB M-04-04, E-Authentication Guidance](#) and [OMB M-05-24, Implementation of Homeland Security Presidential Directive \(HSPD\) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors](#).
 - [OMB M-05-24, Implementation of Homeland Security Presidential Directive \(HSPD\) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors](#) requires that PIV II-compliant smart-cards be used for access to all on-site systems by all permanent on-site employees. This requirement is met by the PIV Card and the Agency Smart Badge (ASB).
 - The IdMAX system manages identities for use throughout NASA and establishes the Agency Unique ID (AUID) which is unique across NASA.
 - IdMAX contains the NASA Account Management System (NAMS) which supports the creation, modification, and deletion of accounts for all NASA systems. The NASA Consolidated Active Directory (NCAD) and Access Launchpad services provide central authentication and authorization to support the NASA-accepted credentials.

2.1.2. Information System Owner (ISO)

The ISO shall:

- Ensure that, on non-public websites, information system users are uniquely identified and authenticated for access to NASA information systems.
- Ensure that, on non-public websites and select applications, the minimum authentication for NASA information systems are at least [NIST SP 800-63-3, Digital Identity Guidelines](#) Authentication Assurance Level (AAL) 2 compliant.

- A more stringent form of authentication may be specified/required by these information system security requirements or by the ISO.
- Ensure that 2-factor identification using the PIV card is required for network access to privileged accounts on NASA information systems.
 - “Privileged Accounts” are also referred to as “Elevated Privileges”
 - Ongoing effort to minimize the number of privileged accounts;
 - Limit the duration that privilege users can be logged in;
 - Limit the privileged functions that can be performed using remote access;
 - Ensure that privileged user activities are logged and such logs are reviewed regularly.
- When employing multifactor authentication for local and remote access to information systems, ensure that the authentication mechanism is [SP 800-63-3](#) Authentication Assurance Level (AAL) 3 compliant using the PIV card.
 - 2-factor authentication using the PIV card shall be required for local access to non-privileged accounts.
- Ensure that for local system access, information systems employ a [SP 800-63-3](#) Authentication Assurance Level (AAL) 2 compliant (e.g., RSA token) or a [SP 800-63-3](#) Authentication Assurance Level 3 compliant (e.g., PIV card, ASB card) authentication mechanism.

2.1.3. NAMS Project Manager

The NAMS Project Manager shall:

- Ensure NAMS and IdMAX systems provide the NASA common infrastructure required to support the Federal E-Authentication and [HSPD-12](#) requirements.

2.2. Device Identification and Authentication ([IA-3](#))

2.2.1. Information System Owner (ISO)

The ISO shall:

- Ensure that their information system uniquely identifies and authenticates routers, wireless access points, hubs, or network attached storage devices before establishing a local or network connection.

2.3. Identifier Management ([IA-4](#))

2.3.1. Information System Owner (ISO)

The ISO shall:

- 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.
 - The NASA IdMAX System manages identities for use throughout NASA and establishes the AUID which is unique across NASA.

2.3.2. IdMAX Project Manager

The IdMAX Project Manager shall:

- Ensure IdMAX manages identities for use throughout NASA and establishes AUIDs which are unique across

NASA.

- Ensure all NASA users are entered into the IdMAX system.
- Ensure that IdMAX includes an archive of previously used AUIDs to support preventing reuse of those AUIDs, in a manner consistent with organizationally defined values.
- Ensure user identifiers are disabled in a manner consistent with organizationally defined values.

2.4. Authenticator Management (IA-5)

2.4.1. Information System Owner (ISO)

The ISO shall:

- Ensure PIV card-enabled applications are implemented in accordance with NPR 1600.1A.
- Ensure password-based authenticators are implemented in a manner consistent with organizationally defined values.

2.4.2. NAMS Project Manager

The NAMS Project Manager shall:

- Ensure that NAMS provides centralized authentication services for information systems registered in NAMS.

2.5. Authenticator Feedback (IA-6)

2.5.1. Information System Owner (ISO)

The ISO shall:

- Ensure that their information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

2.6. Cryptographic Module Authentication (IA-7)

2.6.1. Information System Owner (ISO)

The ISO shall:

- Ensure that the information system implements 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.

2.7. Identification and Authentication (Non-Organizational Users) (IA-8)

2.7.1. Information System Owner (ISO)

The ISO shall:

- Ensure information systems uniquely identify and authenticate non-organizational users for access to NASA non-public information systems.
- 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, E-Authentication Guidance](#).
- 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.
- In cases of a conflict between organizational and non-organizational users, the organizational user identity has priority.

APPENDIX A: ACRONYMS

AAL	Authentication Assurance Level
ASB	Agency Smart Badge
AUID	Agency Unique ID
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CSPD	Cybersecurity and Privacy Division
FIPS	Federal Information Processing Standards
HBK	Handbook
HSPD	Homeland Security Presidential Directive
IdMAX	Identity Management and Account eXchange
ISO	Information System Owner
IT	Information Technology
ITS	Information Technology Security
NAMS	NASA Account Management System
NASA	National Aeronautics and Space Administration
NCAD	NASA Consolidated Active Directory
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
PIN	Personal Identification Number
PIV	Personal Identity Verification

SP Special Publication

User ID User Identification