

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2841.1

Effective Date: January 06,
2011

Expiration Date: June 06,
2016

[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: Identity, Credential, and Access Management

Responsible Office: Office of the Chief Information Officer

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [ALL](#) |

Chapter 3. ICAM Requirements

3.1 Identity, Credential, and Access Management (ICAM) Service Managers shall:

- a. Implement ICAM services in compliance with all Federal and NASA regulations.
- b. Implement ICAM services in alignment with NASA's ICAM Enterprise Architecture segment.
- c. Implement enhancements to ICAM services to meet customer requirements and requirements for integration with other NASA enterprise services as approved by the Agency CIO and the Agency AA for Protective Services.
- d. Be the sole provider of authoritative identity management and directory services.
- e. Be the primary provider of credential management and access management services.
- f. Accept trusted identities and/or credentials provided and managed by Federated Identity Providers (IdPs) and Credential Service Providers (CSPs), as needed, to support NASA's mission.

3.2 Center Security Office Personnel shall:

- a. Verify identities of persons who require access to NASA's physical and IT assets to meet the requirements of this NPR.
- b. Issue Agency credentials that are used for access to both physical and IT assets. The ICAM Services Handbook describes NASA-accepted credentials that can be used for both physical and logical access.
- c. Revoke Agency credentials when a person's affiliation with NASA has been terminated.
- d. Revoke Agency credentials as needed to address security threats.
- e. Accept trusted identities and/or credentials provided and managed by Federated IdPs or CSPs as needed to support NASA's mission.

3.3 Registration Authorities (RAs) shall:

- a. Issue credentials and certificates that are used solely for access to IT assets. The ICAM Services Handbook describes NASA-accepted credentials that can be used for logical access.
- b. Revoke credentials and certificates when a worker's affiliation with NASA has been terminated.
- c. Revoke credentials and certificates as needed to address IT security threats.

3.4 Identity Sponsors shall:

- a. Use the ICAM infrastructure for the creation and maintenance of identity information for all persons accessing NASA assets.
- b. Request identity disablement for persons who no longer have an active relationship with NASA.

c. Request the acceptance of federated identities and/or credentials in accordance with the Identity Providers and Credential Service Providers SOP.

3.5 Access Sponsors shall:

- a. Validate an End User's need for access whenever a request for access is made.
- b. Request removal of access when an End User no longer requires access to perform his/her duties.
- c. Perform disposition of records as needed when an End User's access is terminated.

3.6 Information System Owners shall:

a. Register their IT assets in the authoritative system of record for IT assets defined in the ICAM Services Handbook ensuring that:

(1) New assets are registered at the first stage of their construction or system development life cycle, generally prior to Preliminary Design Review.

(2) Existing assets are registered and maintained throughout their life cycle, culminating with asset retirement and decommissioning.

b. Collaborate with the Information Owner(s) to ensure that an LoR is assigned to each type of access and/or access role for each IT asset under their System Security Plan(s).

c. Collaborate with the Information Owner(s) to implement the appropriate provisioning method for managing access to their assets using the NASA access management service. One of the following methods may be used:

(1) An approval-based method for granting access to their IT asset(s).

(2) A BLE related to a community designation or other attributes maintained authoritatively in enterprise directory services.

d. Ensure that all persons accessing their IT assets have a NASA-accepted identity.

e. Ensure that persons granted access to their IT assets meet the appropriate LoC for the associated LoR of the access to the IT asset.

f. Ensure that credentials allowed to access their IT assets meet the appropriate LoA for the associated LoR of the access to the IT asset.

g. Reconcile all accounts recorded in the access management service with the accounts on the IT asset, ensuring that:

(1) Discrepancies between the account list in the access management service and the account list in the IT asset are analyzed and reconciled so that the access management service accurately reflects approved access to the asset.

(2) Reconciliation is conducted on an annual basis at a minimum.

h. Request a deviation using the process described in the ICAM Services Deviation SOP to allow continued use of a legacy or special purpose ICAM service provider provided that:

(1) There is a technological constraint that does not allow the use of the NASA enterprise ICAM services.

(2) The legacy or special purpose ICAM service provider has met the requirements in Section 3.11 of this NPR.

(3) A transition plan is provided that details when the asset will be retired or integrated with the enterprise ICAM service.

i. Delegate requirements in this NPR as appropriate to persons responsible for managing, operating, and/or maintaining IT assets governed by their IT System Security Plan(s).

3.7 Information Owners shall:

a. Assign an LoR to each type of access and/or access role (e.g., generation, collection, processing, dissemination, and disposal) for information under their authority.

b. Collaborate with the Information System Owner to ensure that the credentials allowed to access information under their authority meets the appropriate LoA for the associated LoR of the access to the information.

c. Determine the appropriate provisioning method to manage access to information under their authority, utilizing the NASA access management service using one of the following methods:

(1) An approval-based method for granting access to their IT asset(s).

(2) A BLE related to a community designation or other attributes maintained authoritatively in enterprise directory services.

3.8 Physical Asset Owners shall:

a. Ensure that their physical assets have been properly registered in the authoritative system of record for physical assets defined in the ICAM Services Handbook.

b. Assign a LoR to each type of access for each physical asset.

c. Manage access to their physical assets using the NASA access management service using one of the following methods:

(1) An approval-based method for granting access to their asset.

(2) A BLE related to a community designation or other attributes maintained authoritatively in enterprise directory services.

d. Ensure that all persons accessing their physical assets have a NASA-accepted identity.

e. Ensure that persons have been verified to the appropriate LoC to meet the associated LoR of their access to the physical asset.

f. Ensure that credentials allowed to access their physical assets meet the appropriate LoA for the associated LoR of the access to the physical asset.

3.9 Community Managers shall:

a. Manage membership in their communities within the access management service using one of the following methods:

(1) An approval-based method.

(2) A logical combination of other communities or attributes maintained authoritatively by identity management services.

(3) Self-registry by the membership.

(4) A combination of self-registry, approval-based, and attribute-based methods.

b. Approve BLE access of their communities to assets.

c. Notify all asset owners who grant access to their community of any change to the membership requirements of their community.

3.10 Systems and Applications shall be designed to:

a. Utilize enterprise directory services for person lookup services provided by their systems.

b. Utilize enterprise authentication and authorization services for end user authentication and authorization.

(1) Systems and applications may utilize internal authorization mechanisms for fine-grained, role-based authorization.

c. Use Agency-accepted credentials for access to all NASA IT assets.

d. Utilize NASA-accepted certificates for person and NPE authentication, encryption, and signing.

3.11 Legacy and special purpose ICAM service providers may continue to operate their services provided that:

a. The legacy or special purpose service relies on identities maintained in the ICAM identity management service.

b. There is a technological constraint that does not allow applications or systems utilizing the service to transition to the NASA enterprise ICAM services.

c. A deviation request is submitted and approved in accordance with the ICAM Services Deviation SOP.

d. Federal and NASA requirements for ICAM services are met.

e. A transition plan is provided that details when the service will be retired or integrated with enterprise ICAM services.

3.12 Federated Identity Providers (IdPs) and Credential Service Providers (CSPs) shall:

a. Apply for acceptance of their identities and/or credentials using ICAM Identity Providers and Credential Service Providers SOP.

- b. Conform to Federal interoperability standards.
- c. Conform to NASA interoperability standards.
- d. Be sponsored by a NASA civil servant in order for the request to be considered.

3.13 End Users shall:

- a. Notify their Identity Sponsor of any changes in identity information, such as legal name or citizenship status. For civil servants, the Identity Sponsor is the Office of Human Capital Management. For contractors, the Identity Sponsor is the Contracting Officer's Technical Representative (COTR).
- b. Use only the credential(s) issued to them for access to NASA assets.
- c. Not share their credentials and/or secret keys with another person.
- d. Secure their credentials and secret keys in a way that reduces the likelihood that they will be used by others.
- e. Ensure the validity of certificates provided by other parties in PKI encoded transactions and sessions.
- f. Upon notification, review access granted to them through the access management service, and request that access be rescinded for any asset they no longer require to perform assignments.
- g. Upon notification, request that membership be rescinded for any community no longer required to perform assignments.
- h. Sign and encrypt data in accordance with Federal and NASA regulations using only NASA-accepted encryption and signing certificates.
- i. Encrypt data in accordance with Federal and NASA regulations using only NASA-accepted encryption tools.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [AppendixA](#) | [AppendixB](#) |
[AppendixC](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
