US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/09/2025

OPDIV:

NIH

Name:

CIT Identity, Credential and Access Management Services (IAM) General Support System (GSS)

PIA Unique Identifier:

P-8673434-707591

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

References to Sebastian Technical Solutions were removed, as NIH IAM Services no longer share PII with Sebastian Technical Solutions.

Updated the list of agreements authorizing information sharing or disclosure (e.g., Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).

Describe the purpose of the system.

The NIH Identity, Credential and Access Management (IAM) Services General Support System (GSS) is an enterprise-level system that gives NIH the ability to: leverage trusted identities and authoritative credentials to ensure only permitted individuals are granted access to protected resources;
associate a digital identity with authoritative proof of that claimed identity; construct a trusted digital

identity based on a individual's defining attributes; accept external credentials for access to NIH systems and applications; and provide secure access to external systems using NIH credentials.

The following systems are integral in providing IAM Services:
Identity Management Services (IMS) allows for the creation, maintenance, resolution, and deactivation of identities (usernames). Credential Management Services (CMS) to processes sponsored requests for credential registration, create, issue, maintain, and store this information within the credential database. Access Management Services (AMS) provides NIH with the capability to authenticate access to
NIH networks and systems users and to subsequently and automatically authenticate those users to other target systems users need to access. AMS also handles password change requests from target systems and may support post-sign-on automation for additional tasks.

Federation Services (FS) provides a gateway for NIH staff and registered and authorized external collaborators to access internal and external resources. Management Tools (MT) provides the capability to complete audit and logging functions; conduct Cloud security monitoring activities; develop, deploy and maintain scripts for automated
security control and compliance actions; monitor key user and administrator changes; and scan NIH systems and applications to ensure security policy compliance.

NIH IAM Services encompasses the following login services: NIH Login and Research Auth (orization) Services (RAS).

During the on-boarding process, NIH employees (federal and direct contractors, as well as fellows and post doctorates (docs) are provisioned into the NIH Enterprise Directory (NED), which is the authoritative source for accurate, locator and organization information for individuals using NIH services or facilities and provides the basis for physical and information security systems. NED is also used to authorize NIH services such as identification (ID) badges, NIH Library access, listing in the NIH Telephone and Services Directory. NED maintains its own unique privacy impact assessment (PIA) with all legal authorities documented.

The Division of Personnel Security and Access Control (DPSAC), within the NIH Office of Research Services (ORS), is responsible for verifying personal identity, validating suitability, conducting background checks, authorizing facility access and issuing Personal Identity Verification (PIV) cards and personal identification number (PIN) for NIH federal and direct contract personnel.

The Center for Information Technology (CIT), NIH is responsible for the development, implementation and management of NIH IAM Services.

Describe the type of information the system will collect, maintain (store), or share.

The systems within the IAM Services GSS systems may independently and/or collectively collect, maintain and/or share the following personally identifiable information (PII) pulled from NED, the authoritative source:

HHS Identification (ID) number
Employee/Contractor Name
NIH Phone Numbers
NIH E-Mail Address
NIH Mailing Address
Personal Mailing Address
Personal E-Mail Address
NIH Username (login) and Password

Group/access Membership(s)
HHS Operating Division (OPDIV)
NIH Organizational Department
Personal identity verification (PIV) card status
Employee Status

Fingerprint verification through the ORS Background Investigation Tracking System (BITS)
Validation of mandatory training records for all NIH employees through the Learning Management System (LMS) and Security Awareness Training System (SATS).

In addition, the following IAM GSS components specifically collect and/or store the following PII:

Credential Management Services (CMS): eRA Commons username and password
Access Management Services (AMS): Authentication information and Single Sign-On (SSO) information
Authentication and single-sign-on information consist of: User's first name, last name, HHS ID number, NIH password, and phone number from NED.

Federation Services (FS) collects the following from NIH and non- NIH users:
NIH users: first name, last name, email address, and HHS identification number (HHS ID); and Non-NIH users: first name, last name, email address, and persistent identifier from the external identity provider (the owner of the account you used to log in).

NED, BITS, LMS, SATS and eRA Commons maintain their own unique PIA, with all legal authorities documented.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The NIH IAM Services GSS is an enterprise-level system that gives NIH the ability to: leverage trusted identities and authoritative credentials to ensure only permitted individuals are granted access to protected resources; associate a digital identity with authoritative proof of that claimed identity;
construct a trusted digital identity based on a individual's defining attributes; accept external credentials for access to NIH systems and applications; and provide secure access to external systems using NIH credentials.

The following systems are integral in providing IAM Services:

IMS allows for the creation, maintenance, resolution, and deactivation of identities (usernames).
CMS to processes sponsored requests for credential registration, create, issue, maintain, and store this information within the credential database.
AMS provides NIH with the capability to authenticate access to NIH networks and systems users and to subsequently and automatically authenticate those users to other target systems users need to access. AMS also handles password change requests from target systems and may support post-sign-on automation for additional tasks.
FS provides a gateway for NIH staff and registered and authorized external collaborators to access internal and external resources.
MT provides the capability to complete audit and logging functions; conduct Cloud security monitoring activities; develop, deploy and maintain scripts for automated security control and compliance actions; monitor key user and administrator changes; and scan NIH systems and applications to ensure security policy compliance.

During the on-boarding process, NIH employees (federal and direct contractors, as well as fellows and post docs) are provisioned into NED, which is the authoritative source. NED is also used to authorize NIH services such as ID badges, NIH Library access, listing in the NIH Telephone and Services Directory. Personal mailing addresses collected from NED is used to send security keys to NIH users who do not reside close to a NIH badging office. NED maintains its own unique PIA with all legal authorities documented.

DPSAC is responsible for verifying personal identity, validating suitability, conducting background checks, authorizing facility access and issuing PIV cards and PIN for NIH federal and direct contract personnel.

The systems within the NIH IAM Services GSS systems may independently and/or collectively collect, maintain and/or share the following PII pulled from NED, the authoritative source:

HHS ID number
Employee/Contractor Name
NIH Phone Numbers
NIH E-Mail Address
NIH Mailing Address
Personal Mailing Address
Personal E-Mail Address
NIH Username (login) and Password
Group/access Membership(s)
HHS OPDIV
NIH Organizational Department
PIV card status
Employee Status
Fingerprint verification through the ORS BITS Validation of mandatory training records for all NIH employees through the LMS and SATS

In addition, the following IAM GSS components specifically collect and/or store the following PII:

CMS: eRA Commons username and password
AMS: Authentication information and SSO information
Authentication and single-sign-on information consist of: User's first name, last name, HHS ID number, NIH password, and phone number from NED.

FS collects the following from NIH and non- NIH users:
NIH users: first name, last name, email address, and HHS ID; and Non-NIH users: first name, last name, email address, and persistent identifier from the external identity provider (the owner of the account you used to log in).

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
Biometric Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Employment Status

HHS Identification ID number, NIH Username (login) and Password, Group/access Membership(s), personal email address
HHS OPDIV, NIH Organizational Department, PIV card status, Fingerprint verification, Mandatory training validation

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The PII collected from NIH users and external collaborators enables streamlined access to NIH applications, data and websites and provides standardized methods of logging and auditing.

Personal email addresses collected from NIH users is used to send NIH users required training and password expiration notifications.

Personal mailing addresses collected from NED are used to send security keys to NIH users who do not reside close to an NIH badging office. NIH users are required to complete a consent form to acknowledge that NIH will share their home address with a third party vendor for the shipment of the security key. These keys allow secure access to NIH applications, data and websites.

Describe the secondary uses for which the PII will be used.

Not Applicable

Identify legal authorities governing information use and disclosure specific to the system and program.

44 U.S.C 3101 and 3102, and HSPD-12

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-90-0777, Facility and Resource Access Control Records, HHS

09-25-0216, Administration: NIH Enterprise Directory

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Online
Government Sources
Within OpDiv
Other HHS OpDiv
Other Federal Entities
Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Due to character limitations, please find the response in the General Comments section.

Describe the procedures for accounting for disclosures.

The information displayed in the GAL and NED are publicly available through a Public NED search application, which maintains its own PIA.

Federation Services and eRA maintain disclaimers on their respective sites, informing users that their PII is collected and what it will be used for.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

NIH Users

The NIH on-boarding process includes notification to individuals that their personal information will be collected, maintained, and shared. All collected information is maintained via NED, which provides notice and collects, maintains, and shares data as part of the NIH Division of Personnel Security and Access Control (DPSAC) enrollment, suitability determination, and badging process. NED is the authoritative source for personnel information at the NIH and maintains its own PIA.

NIH users eligible for a security key provide consent to allow NIH to collect and share their home address with a third-party vendor for the shipment of the security key.

Non-NIH Users

The login screen has a Warning Notice to individuals that their personal information will be collected, and actions monitored.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Individuals cannot opt out of the collection or use of their PII.

If an individual opts out, they won't have access to NIH resources to perform their job.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Users would be notified via email or alert if there were major changes to the system.

Users of FS would be notified, via a message posted on the FS login screen, if there were major changes to the system.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

NIH Users

The process to contest a record is specified in the published NIH System of Record Notice (SORN)

09-25-0216. The petition for amendment must be addressed in writing to the System Manager. The individual must identify himself/herself, specify the system of records from which the records are retrieved, the particular records to be corrected or amended, whether seeking an addition to or a deletion or substitution for the records, and the reason for requesting correction or amendment of the record.

All NIH personnel (users) may update their PII via the NED web interface. Individuals may contact the NIH Service Desk if they have further concerns.

Non-NIH Users
There is no process in place for non-NIH users because they supply their PII information directly to FS whenever they log into the system.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

NIH Users
PII is not periodically reviewed for accuracy because the data is either internal, system generated data (e.g., unique identifiers) or pulled from NED. A web-based interface allows users to maintain their PII within NED.

Non-NIH Users
There is no process in place for periodic reviews of PII because PII is collected and retained temporarily for the duration of a user's log in session in FS. PII will be reviewed by users' respective authoritative sources. FS uses IMS as the authoritative source for login credentials. Automated mechanisms, internal and external to IMS, enforce established policies for password security and account life cycle management. These policies prescribe the conditions for allowing, denying, and terminating access in a timely fashion.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

NIH employs the principle of least privilege and need to know, allowing only authorized accesses for users which are necessary to perform primary job responsibilities in accordance with organizational missions and business functions.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

NIH employs the principle of least privilege and need to know, allowing only authorized accesses for users which are necessary to perform primary job responsibilities in accordance with organizational missions and business functions.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy awareness training. Training is completed on the http: //irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Administrators and privileged users are required to take additional training specific to their roles and responsibilities, e.g. role-based training.

NIH users with contingency planning, incident response planning; and configuration management responsibilities are required to take contingency planning (CP), incident response (IR) planning, and configuration management trainings, respectively.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

Item 07-204 - System access records. Systems requiring special accountability for access.
System access records.
These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Includes records such as:
user profiles
log-in files
password files
audit trail files and extracts
system usage files
cost-back files used to assess charges for system use
Exclusion 1. Excludes records relating to electronic signatures.
Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.
Systems requiring special accountability for access.
These are user identification records associated with systems which are highly sensitive and potentially vulnerable.

Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

Item10-101 - Administrative records maintained in any agency office.

Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, excluding records scheduled elsewhere in the general records schedule (GRS) such as timekeeping and procurement.
Disposition: Destroy when business use ceases. In accordance with DAA-GRS-2016-0016-0001

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative:
Permissions to perform specific operations are assigned to specific roles in order to complete various job functions. Authorized users are assigned particular roles, and through those role assignments acquire the system permissions to perform particular system functions. Users are assigned permissions based on their role (or roles). Management of individual user rights requires

assigning appropriate roles to the user's account. This simplifies common operations, such as adding a user, or changing a user's department. Users' access and corresponding permissions are reviewed once a year to assess and confirm need for continued authorized access.

Technical:
IT hardware and software are segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentications must be used for access. File integrity and auditing software are employed on hardware.

Physical:
Access is limited by controlled access to NIH servers located in a secured facility. Security personnel are stationed at the main entrance of the complex, 24 hours a day, seven days a week. Anyone entering the building must display a valid government ID showing a current identification photo or register with the security guard to acquire a temporary visitors' badge. All entrance doors to the complex, including machine rooms are controlled by card-activated locks that restrict access 24 hours a day seven days a week. Access to the specific Data Center requires biometric (eye scan) validation.

Identify the publicly-available URL:

https://auth.nih.gov/docs/RAS/index.html
https://auth.nih.gov/docs/RAS/serviceofferings.html
Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes