# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

04/23/2025

### OPDIV:

IHS

### Name:

Identity Access Management

**PIA Unique Identifier:**

P-8222400-919287

**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?**

No

**Identify the operator.**

Agency

**Is this a new or existing system?**

Existing

**Does the system have Security Authorization (SA)?**

No

**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.**

Review and update of data connector for AMS SCMS which includes the same identity attribute data as previously approved.

**Describe the purpose of the system.**

The IHS Identity Access Management system (IAM) is an enterprise system intended to aggregate user identify data and report on who is authorized to be on the IHS network. Specifically, the services support the the management of credentials a user uses to access IHS data and/or information on IHS systems and component networks. The IAM will identify and manage aggregated user identity data and their associated access authorization, authenticated permissions, and resource rights into a Master User Record (MUR) for each user identity. The capabilities collectively cover the verification and validation of allowed user privileges, user owned credentials, user security behavior training, and appropriately granted resource access rights to users. Additionally, it is to provide an automated means for qualified Indian Health Service personnel for access certifications,

policy management, and identity intelligence. This includes the ability to review, approve, and certify user access to computer and network resources to include Active Directory. In addition to cataloging all personnel with access to IHS information resources, the system will facilitate access reviews, automate and provide a complete history of access provisioning/de-provisioning, track required training compliance, and maintain real-time visibility of access and request status. Employee supervisors from all IHS Facilities will utilize the system to review access to enterprise services as well as local systems within the facility.

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

The Sailpoint IAM system is an IHS-wide consolidated user identity system that will contain the following Personally Identifiable Information (PII) about each user identity, their authorization level, credentials and security related behavior management. This applies to employees, contractors and other affiliated users information in order to provide access to supported Active Directory systems. This data includes:

Full name, employment type affiliation (direct contractor, federal employee), job title, phone number, location, email, contract name, Social Security Number (SSN), Date of Birth, mailing address, and employment status, Role Based Training completion status, supervisor, HHS ID, Completion date and status of mandatory trainings required prior to access approvals (Information Systems Security Training status-completed/not completed), Service contract number and expiration (for contractors), system name and justification for access and any specific permission levels required (view only, full access or other limited access).

This information is used to manage the identity of each Active Directory user and the associated network and application access entitlements to specific systems being requested.

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

In order to configure a Master User Record (MUR) for each user identity, the IAM collects attributes from a number of authoritative data sources. This includes:

The IHS Active Directory for user attributes

The AMS Smart Card Management system for Trust and Credential attributes

The Information System Security Awareness Training for Behave attributes

The Security Management System, Enterprise Virtual Directory for Trust attributes along with the Business Intelligence Information System (BIIS) for Trust attributes

The information from these data sources is filtered through the IAM (SailPoint IIQ) System where the MUR, a consolidated user record is maintained.

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

Yes

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

Social Security Number
Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Education Records
Employment Status

Additional elements also include the employment type affiliation (direct contractor, federal employee), job title, location, supervisor, and HHS ID.

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Business Partners/Contacts/Vendors/Suppliers and other Direct Contractors are any user who is sponsored by an authorized federal supervisor/contracting officer representative for access to an IHS Federal IT system will be required to provide the same information as Federal employees/users in order to obtain access. This information would be included and collected as part of each Federal contract our memorandum of agreement.

**How many individuals' PII is in the system?**

50,000-99,999

**For what primary purpose is the PII used?**

IHS will use the information when individuals request for access to federal information systems, computers, applications, or data to prove the individual's identity and right of access. Additionally, the data will be used for validation and certification of user identity and their authorization to access Federal Information Systems.

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

Yearly compliance auditing and reporting

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

Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), and Health Insurance Portability and Accountability Act (HIPAA) require Indian Health Service to track federal information system users, their associated access to Federal IT systems as well as their training compliance. Privacy Act of 1974 governs use and disclosure specific to use of the system.

**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.**

GSA/GOVT-7 HSPD-12 US Access

**Identify the sources of PII in the system.**

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Other HHS OPDIV

State/Local/Tribal

Non-Governmental Sources

Private Sector

**Identify the OMB information collection approval number and expiration date**

Not Applicable

**Is the PII shared with other organizations?**

No

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

Individuals will be aware of what information is collected when they provide their information directly as part of the on boarding process. They will provide the information via a standard form (SF), SF 745. Individuals will be aware of the purpose of submitting the information, which will be to request assignment of an access badge. Opportunities to further understand the use of their PII will occur during the completion of the eQIP profile, including the provision of background information.

**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.**

The information provided as part of each user identity is included as part of the pre-clearance process and identity investigation as a federal government job requirement. Those who refuse to provide personal information will not meet the requirements of the job and will therefore not be considered further. Data collected is from outside data sources and authorized as part of separate agreements.

Current employees who do not meet these requirements will be terminated.

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

Disclosures from this system are unlikely to be made, except as part of the general use of the application where authorizations are already on file. If any nonstandard disclosures were to be made for any unanticipated reason, such that the disclosure was not a routine use, the system owner would maintain a record in a designated file to document who made the request; exactly what each individual was provided and the date of the disclosure. The IHS, with respect to each system of records under its direct control (i.e., Privacy Act System of Record 09-17- 0001) must keep a record of the date, nature, and purpose of each disclosure of a record to any person or Agency under subsection (b) of the Privacy Act (5 U.S.C. § 552a) and the name and address of the person or Agency to whom the disclosure is made. This record must be kept for 5 years or the life of the record; whichever is longer, after the disclosure for which the accounting has been made. An individual (beneficiary) is entitled, upon request, to get access to this disclosure record of his or her own personal records with the exception for disclosures made under subsection (b) (7) of the Privacy Act (as a result of civil or criminal law enforcement activity). The IHS must inform any person or other Agency about any correction or notation of dispute made by the IHS in accordance with subsection (d)(4) of the Privacy Act (Access of Records) of any record that has been disclosed to the person or Agency if an accounting of the disclosure was made. This is a mandatory reporting requirement and may be recorded utilizing the IHS-505, "Disclosure Accounting Record" form. In cases involving individuals or small groups of users, notifications of major changes will be delivered via individual e-mails as part of each associated data system. In cases involving a large amount of users a mass email will be sent via distribution lists informing users of what has occurred, and their options, if there are any resulting procedural or privacy changes. Incidents will also be reported to the associated application Service Desk and resolved in a timely fashion.

**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.**

The IAM system is not intended to collect non-business-related personal information. The system will have a standard Privacy Act Notice. If required, the individuals should contact their Chief Information Security Officers (CISOs) or Incident Response Team (IRT) if they believe their PII has been inappropriately obtained, is incomplete or inaccurate, or is being misused. Individuals are informed of the proper procedures to follow in these circumstances during security and privacy training, which they are required to complete annually.

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

The IAM system and associated IHS user security policies requires yearly reviews of user information and authorized access by each users supervisor or contract representative. Additionally, IHS Human Resources will periodically require individuals to update and verify the background information provided as a condition of re-issuing individual PIV cards.

**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.**

Indian Health Service will adhere to the National Institute of Standards and Technology (NIST) 800-53 system polices which define user provisioning and support for the application management. The IAM system makes extensive use of secure role based access rights, and privileges to enforce access to PII.

**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.**

Access to PII is based on authorization provided as part of the Authority to Operate as part of defined access roles and privileges. Standard users will not be provided access to the IAM system.

**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.**

All authorized IAM support personnel must attend all applicable federal security and privacy training (part of the ISSA), Privacy Act and IT Rules of Behavior prior to system use.

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

Internal IAM system training is available via role-based training presentations posted on the Intranet and on-the-job application training. Both review PII concepts and security procedures to ensure personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

**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 in accordance with General Records Schedule (GRS) 18, Item 17. Unless retained for specific ongoing security investigations, records of access are maintained for seven years and then destroyed. All other records relating to individuals are retained and disposed of in accordance with GRS 18, Item 22a.

In accordance with IHS Indian Health Manual, Active Directory user accounts are deactivated within 24 hours of user separation. The information within the IAM is maintained in accordance the National Archives and Records Administration (NARA) General Records Schedule 2 (GRS 2).

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

The IAM database and individual identity servers are managed by authorized Active Directory admins. These systems are located within secured buildings and data centers. High degrees of security have been implemented at both locations, with some including PIV authorized access and closed circuit TV monitoring. Technical controls which minimize the possibility of unauthorized access, use, or dissemination of
the data in the system are also in place. These include: user identification, firewalls, Virtual Private Network (VPN) remote access, encryption, Intrusion Detection System and PIV Cards to further ensure PII will be secure. Additionally, the following administrative, technical and controls are in place for the IAM system:

Contingency Plans
System Security Plans
Scheduled and validated Data Backups stored off-site
Least Privilege Access
Role based Security Awareness Training
Firewalls
Data Encryption
Intrusion Detection System (IDS)