Indian Health Service

Identity Access Management: Onboarding and Off Boarding Team Members

KATHRYN LEWIS, IHS HEADQUARTERS
OFFICE OF INFORMATION TECHNOLOGY
SAILPOINT IDENTITY ACCESS MANAGEMENT
08/15/2024

Agenda

- What is Identity Access Management (IAM)?
- Challenges for Onboarding New Team Members
- SailPoint IAM and ServiceNow: Benefits, Improvements and Challenges
- IAM Roles and Responsibilities for Identity Management in IHS
- Onboarding new users
- Yearly Access Certification Review and Security Training Compliance
- Off boarding Team Members
- Reinstating Identities and Access
- References, Questions, Recommendations

What is “Identity Access Management”?

- Definition: “*Identity and Access Management (IAM) is a security and business discipline that includes multiple technologies and business processes to help the right people (and associated digital identities) to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay.”* Gartner

- Policy references:
  - Indian Health Manual (IHM), Part 8, Chapter 21 – Access Control; IHM, Part 8, Chapter 19 – Least Privilege; IHM, Part 10, Chapter 1 and 7 – Access Control and Identification and Authentication (pending final approvals)
  - IHM, Part 5, Chapter 30, “Homeland Security Presidential Directive – 12,” February 28, 2024

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Digital Identity Guidelines, OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management and OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.

- Dear Tribal Leader Letter (DTLL) dated February 29, 2024, The IHS Director writes to Tribal Leaders to provide updates on Agency procedures for access by Tribal staff and contractors to IHS facilities and computer networks.

- DTLL dated March 4, 2024, The IHS Director writes to Tribal Leaders to provide an update on the Agency-wide consolidation of human resources (HR) offices, an initiative that references a "One HR.“

Identity First Security

Identity-First Security refers to a security approach that emphasizes the use of identity as a central component for securing systems and resources. It focuses on the notion that strong and reliable identification of users, devices, and other entities is crucial for effective security measures. 61% of all breaches involve stolen credentials (Verizon Data Breach Investigation Report 2021)

Identity-First Security involves a shift towards a more granular and context-aware security model that revolves around identities and their associated attributes. It involves the use of technologies and practices such as multi-factor authentication (MFA), identity and access management (IAM), privileged access management (PAM), and Customer IAM. This involves improving identity verification practices, implementing mandatory phishing resistant two factor authentication, integrating and automating access based on identity validation and authorization and improving the customer experience and employee productivity seamlessly with automation and AI, By placing identity at the center of the security model, organizations can establish a stronger level of trust and control over their systems and resources.

With Identity-First Security, the implementation of policies and controls that are tailored to specific identities allow organizations to enforce the principle of least privilege where users are granted only the necessary permissions to perform their tasks.

Furthermore, Identity-First Security enables organizations to monitor and track user activities more effectively. By associating actions with specific identities, organizations can detect anomalous behavior, detect potential insider threats, and respond to security incidents more promptly.

Identity First Security Benefits

Stronger authentication

By implementing multi-factor authentication (MFA) along with complementary technologies such as adaptive authentication, the reduced risk of unauthorized access protects sensitive information.

Granular access control

Identity-First Security enables organizations to implement fine-grained access controls based on user identities and their associated attributes. This principle of least privilege ensures that users have only the necessary access privileges to reduce the risk of privilege misuse and unauthorized access.

Context-aware security

Identity-First Security considers contextual information such as the user's location, device, and behavior patterns to assess the security risk and apply appropriate security measures. This adaptive approach enhances security while minimizing disruptions for legitimate users.

Improved visibility

By associating actions with specific identities, Identity-First Security provides enhanced visibility into user activities. This allows organizations to track and audit user actions more effectively, detect suspicious behavior, and hold users accountable for their actions to discourage insider threats.

Improvement Opportunities for Onboarding New Team Members

- Overview: IHS has more than 23,000 active identities being managed using SailPoint IAM. Each user is unique, requiring specific access for specific support. Opportunities for improvement involve the following areas:

  - IHS Area and Facility Roles and Responsibilities
  - IHS onboarding processes, communications and actions required
  - Improving the understanding of IHS Policies relating to Identity and Access Management
  - Improving the understanding of the timelines required in preparation for Day 1
  - Improving training availability on the processes
  - Technical challenges on the use of SailPoint IAM or identity issues that require escalated support
  - Availability of Local and Area contacts for information and support
  - Others?

SailPoint IAM and Service Now Overview

- SailPoint IdentityIQ is an Identity and Access Management Governance product that will provide automated provisioning of IT access requests for connected applications as submitted from ServiceNow.
- SailPoint IAM will also be used as the Identity governance and compliance platform for which managers and ISSOs carry out their roles and responsibilities through various business-related user lifecycle management workflows for all IT Access requests and certifications.
- SailPoint IAM leverages the data that is collected from other authoritative identity data sources (Smart Card Management System (SCMS), IHS Human Resource Systems, ISSA, Active Directory etc.), in order to facilitate the provisioning of access to target IT systems and validating access through automated processes.
- SailPoint IAM retains all user identities with an HHSID for auditing, reporting and future reinstatement actions

SailPoint IAM and ServiceNow Benefits

- Automation and workflows
  - Identity validation and pre-creation based on authoritative source
  - Access requests are integrated from ServiceNow to SailPoint IAM (standard request process for all Catalog items)
- Improved Security policy enforcement for all Digital Identities
  - Enforcement of mandatory Security training
  - Automated Dormant account management
- Authorization, Yearly Certification and Mandatory Reporting
  - Area Information System Security Officer (ISSO) Oversight, approvals and monitoring
  - Yearly certification compliance has improved more than 20% in the last year

IAM Roles and Responsibilities

- Area Human Resource Office
  - They are to coordinate with the Hiring Manager on the identification and approvals to hire a new employee.
  - They are to update the Enterprise Human Capital Management (EHCM) system with required new employee information
  - They are to coordinate the new employees start date and communicate with the Hiring Manager
- Personnel Security Representative
  - They are to schedule each new IHS employee, contractors and volunteers for fingerprinting and identity proofing. This includes the required forms, information and location for the appointment.
  - They are to validate the users pre-clearance authorization and communicate the status to the Hiring Manager
  - They are to issue and then later terminate the users PIV card upon user leaving IHS
- Hiring Manager/COR
  - They are to confirm the level of physical or IT access needed for each new team member as part of onboarding the new user using SailPoint. This includes the needed roles and entitlements.
  - They are to submit all IT access requests via the ServiceNow portal for approval and fulfillment.
  - They are to review a user's IT access based on the Annual IT certification review and to submit for any changes

IAM Roles and Responsibilities (cont.)

- Hiring Manager/COR (cont.)
  - They are to terminate a users identity and all associated access first using SailPoint IAM and then submitting application access terminations using ServiceNow
  - They are to confirm authorized access by accepting or revoking a user's access privileges when they leave IHS or access is no longer required. NOTE: Contractors are NOT to be sponsors, only Federal or Tribal staff.

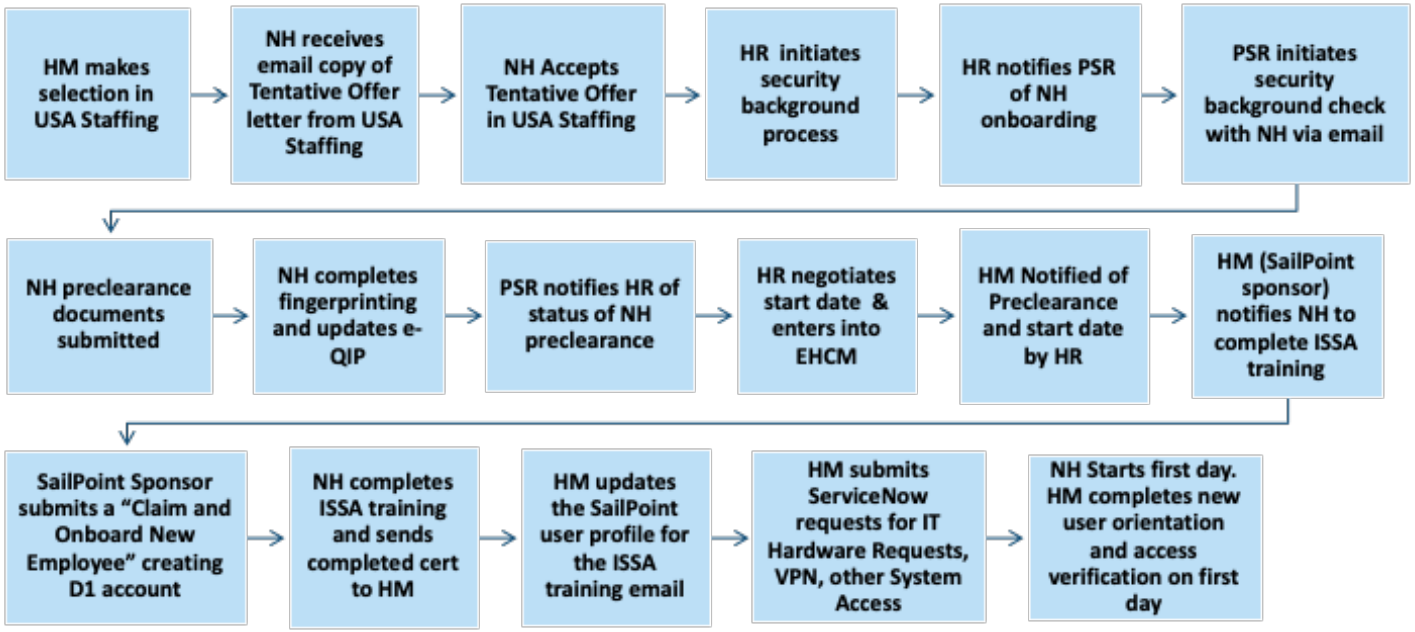
- ISSO Role and Responsibility for Certification
  - They provide the needed process support for escalations, forwarding and reassignments and approving of some access requests
  - They are to confirm mandatory pre-requisites have been completed for access to IT systems and services within IHS.
  - They are to certify the completion of access reviews by all Area SailPoint managers and to monitor using specific Area Reporting

- Local IT Fulfiller Role and Responsibility for Certifications
  - They are to validate current access authorization, roles and functionality requested and approved.
  - They are to provision a user's local IT access based on requests submitted through ServiceNow
  - They support the IAM process with information on training availability, Knowledge Base Article documentation, email notifications, etc.

Onboarding New IHS users (Team Members)

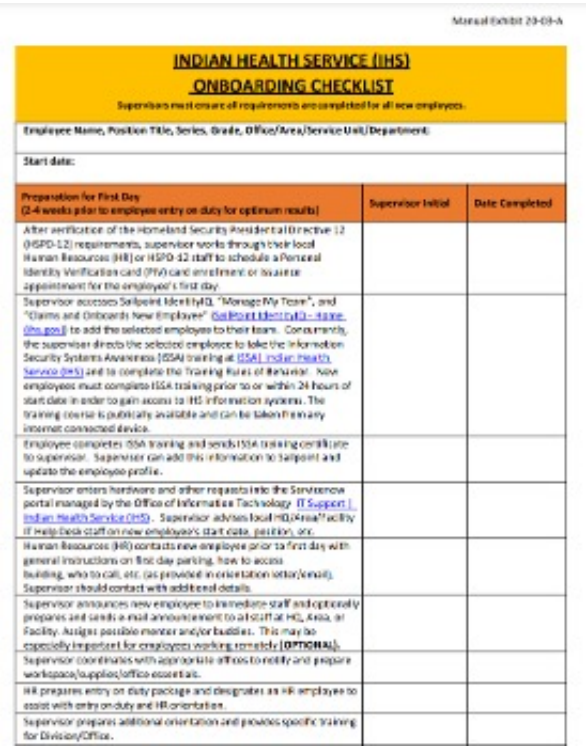
- See IHM Circular, Management Onboarding Policy and Checklist
- Requires coordination with IHS Area Human Resources Offices (HR) and Personnel Security Representatives (PSRs)
- Authorization to “Claim and Onboard” a new Team Member begins with the “Preclearance Authorization” from the local HR office.
- Within two weeks of the users enter on duty/start date (EOD), Managers are to access SailPoint and “Claim and Onboard” their new Team Members. This allows for account creation, access request submission and approvals and equipment readiness well in advance of the users start date.

Claim and Onboard New Team Members



Participants: Hiring Manager (HM) or COR, HR Specialist (HR), Personnel Security Representative (PSR), SailPoint sponsor (SPS), New Hire (NH), e-QIP=Electronic Questionnaires for Investigation Processing

Onboarding Checklist



Manual Exhibit 20-03-A

INDIAN HEALTH SERVICE (IHS)
ONBOARDING CHECKLIST
Supervisors must ensure all requirements are completed for all new employees.

Employee Name, Position Title, Series, Grade, Office/Area/Service Unit/Department:		
Start date:		
Preparation for First Day (2-4 weeks prior to employee entry on duty for optimum results)	**Supervisor Initial**	**Date Completed**
After verification of the Homeland Security Presidential Directive 12 (HSPD-12) requirements, supervisor works through their local Human Resources (HR) or HSPD-12 staff to schedule a Personal Identity Verification card (PIV) card enrollment or issuance appointment for the employee's first day.		
Supervisor accesses Sailpoint IdentityIQ "Manage My Team", and "Claims and Onboards New Employee" (SailPoint IdentityIQ - itsnet.ihs.gov) to add the selected employee to their team. Concurrently, the supervisor directs the selected employee to take the Information Security Systems Awareness (ISSA) training at (ISSA	Indian Health Service (IHS)) and to complete the Training Rules of Behavior. New employees must complete ISSA training prior to or within 24 hours of start date in order to gain access to IHS information systems. The training course is publically available and can be taken from any internet connected device.		
Employee completes ISSA training and sends ISSA training certificate to supervisor. Supervisor can add this information to Sailpoint and update the employee profile.		
Supervisor enters hardware and other requests into the Servicenow portal managed by the Office of Information Technology (IT Support	Indian Health Service (IHS)). Supervisor advises local HQ/Area/Facility IT Help Desk staff on new employee's start date, position, etc.		
Human Resources (HR) contacts new employee prior to first day with general instructions on first day parking, how to access building, who to call, etc. (as provided in orientation letter/email). Supervisor should contact with additional details.		
Supervisor announces new employee to immediate staff and optionally prepares and sends e-mail announcement to all staff at HQ, Area, or Facility. Assigns possible mentor and/or buddies. This may be especially important for employees working remotely **(OPTIONAL)**.		
Supervisor coordinates with appropriate offices to notify and prepare workspace/supplies/office essentials.		
HR prepares entry on duty package and designates an HR employee to assist with entry on duty and HR orientation.		
Supervisor prepares additional orientation and provides specific training for Division/Office.		

Management Onboarding Checklist

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Indian Health Service
Rockville, Maryland 20857

Refer to: OHR

INDIAN HEALTH SERVICE CIRCULAR NO. 20-03

MANAGEMENT ONBOARDING CHECKLIST

Sec.

1. Purpose
2. Policy
3. Background
4. Responsibilities
5. Records Retention
6. Supersedure
7. Effective Date

1. PURPOSE. The purpose of this circular is to establish the Indian Health Service (IHS) procedure for proper and complete onboarding of new employees.

2. POLICY. The Onboarding Checklist (Exhibit 20-03-A) [PDF - 697 KB], is a mandatory tool for supervisors to use when all new employees are hired. This checklist will standardize and document the completion of required actions and tasks for both the employee and supervisor.

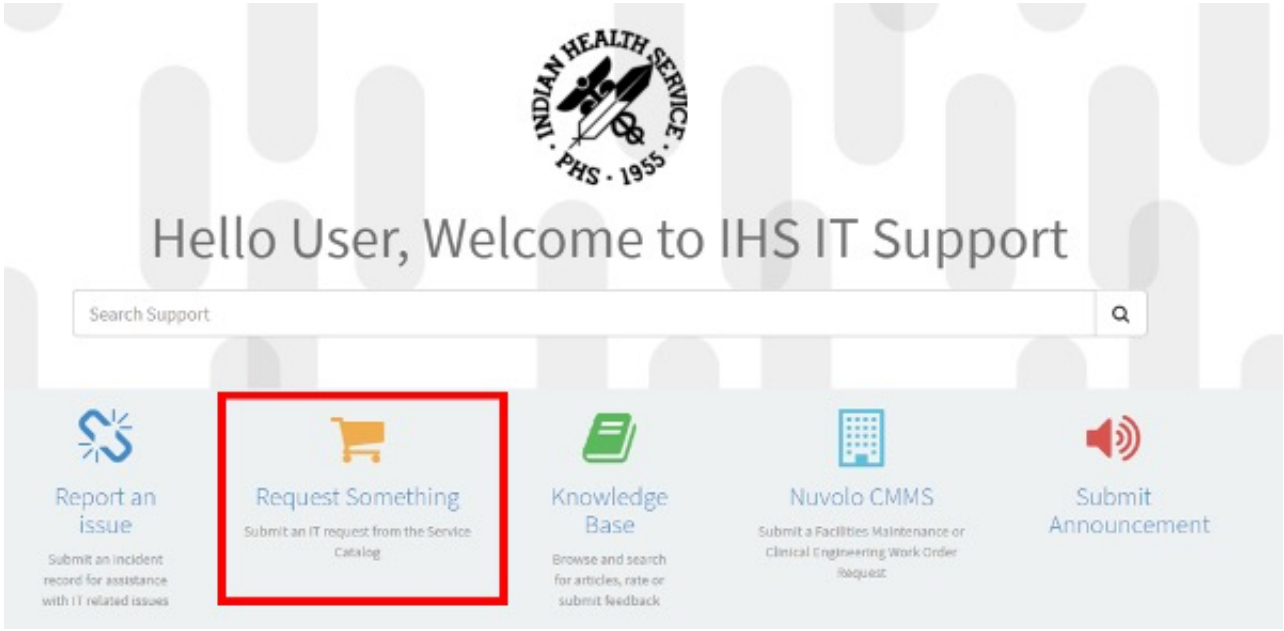
Onboarding new IHS users into SailPoint IAM

- When to claim and onboard
- Validation of Mandatory Security Training (ISSA) compliance
- Local IT notifications
- ServiceNow access requests
- Ready for Day 1?

1.Open web browser (e.g., Google Chrome or Microsoft Edge).

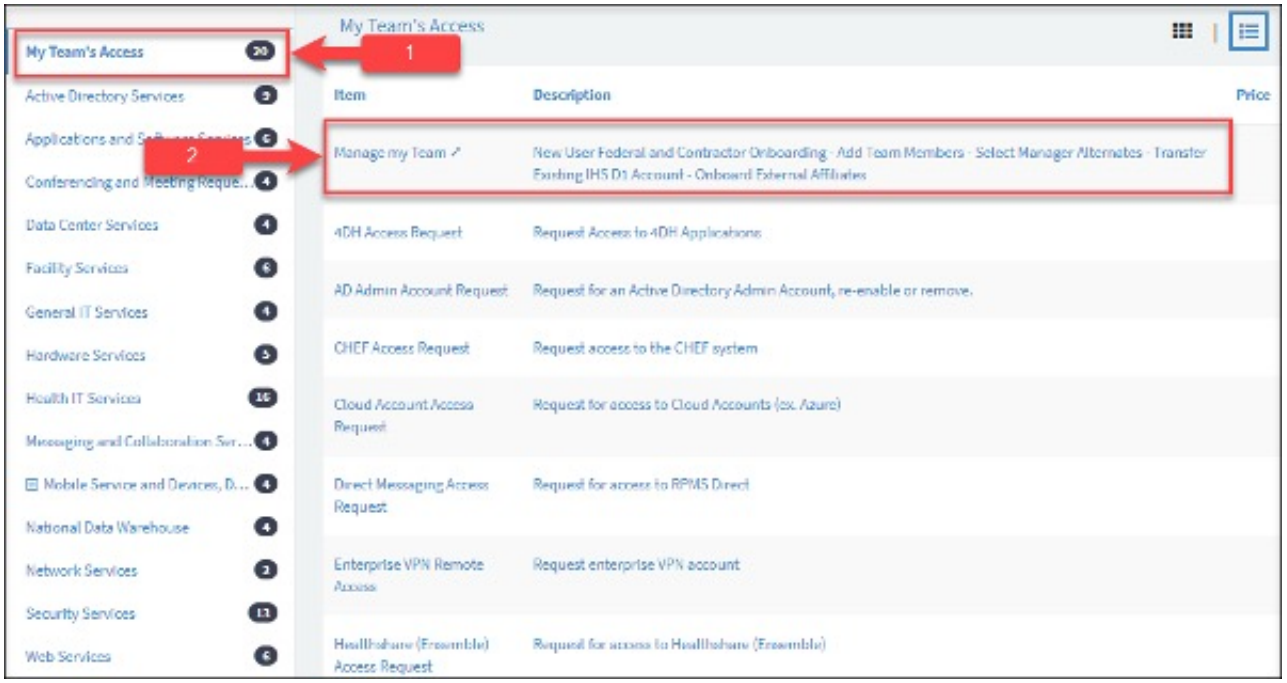
2.Navigate to the **IHS ServiceNow Self Service Portal** main page **IHS IT Support (https://www.ihs.gov/itsupport).**

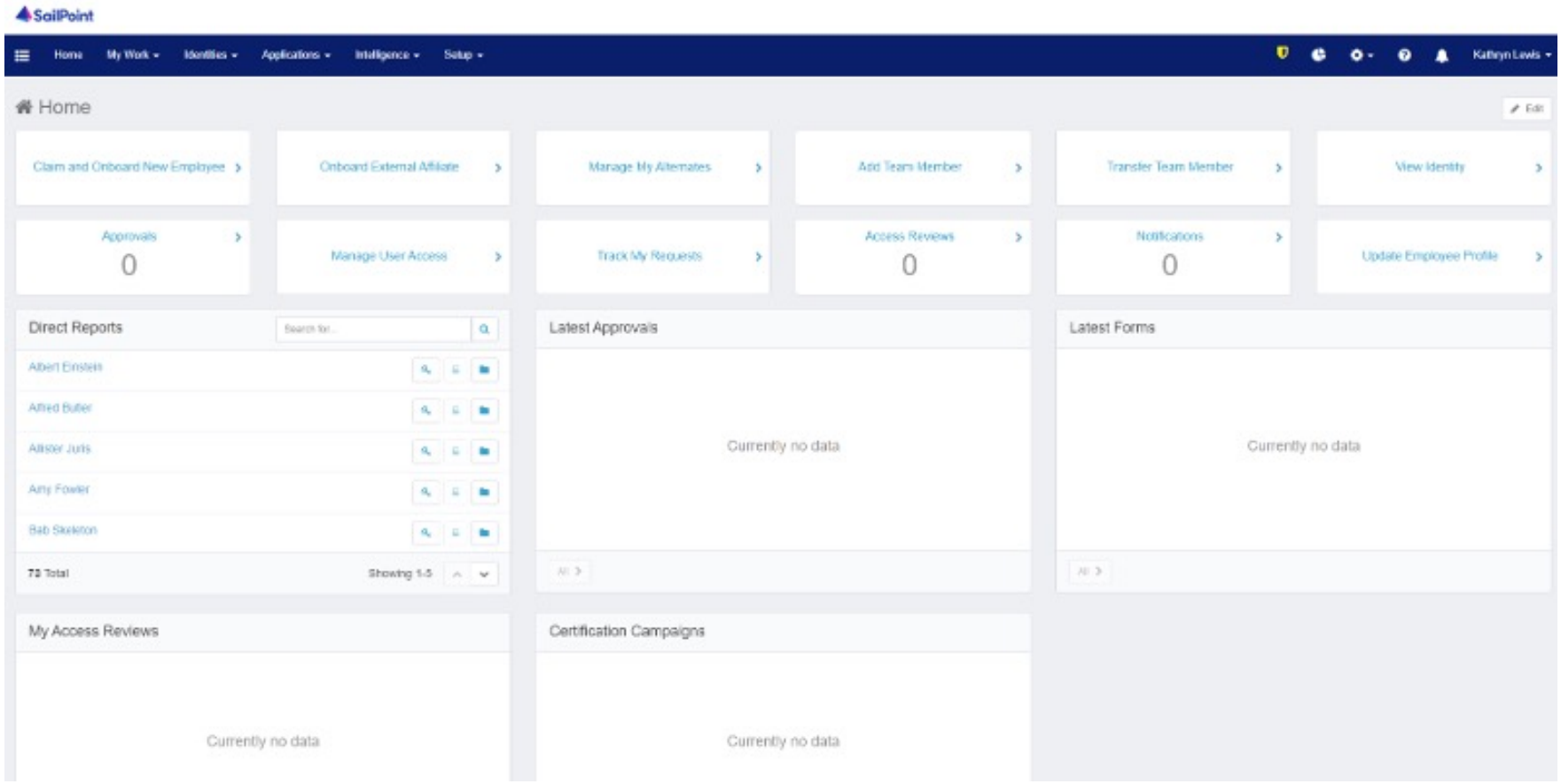
3.Click **Request Something** (highlighted) from **Self Service Portal** main page to navigate to **Service Catalog**.

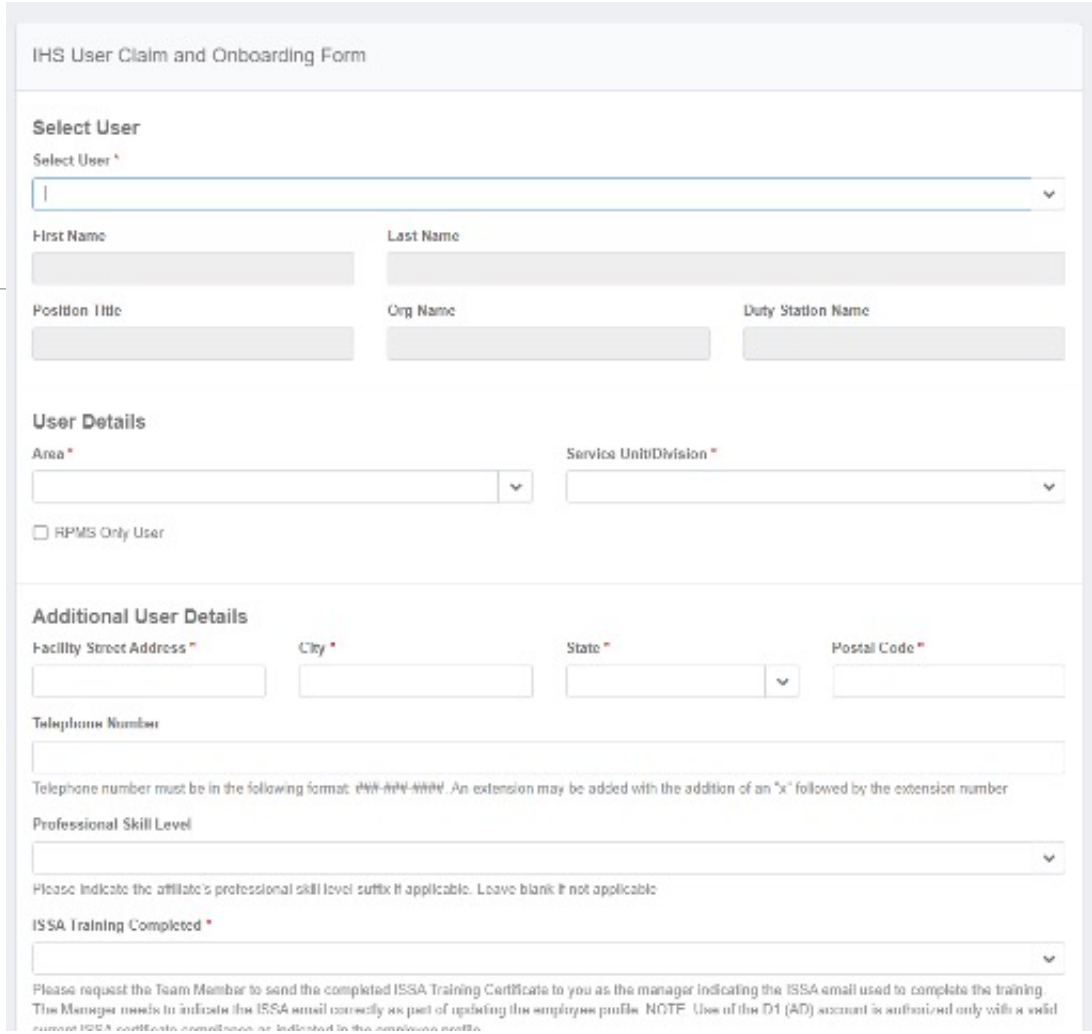


Select My Team's Access (1 - highlighted), to display My Team's Access Service Catalog items list.

Select Manage my Team (2 - highlighted) from My Team's Access Service Catalog items list.



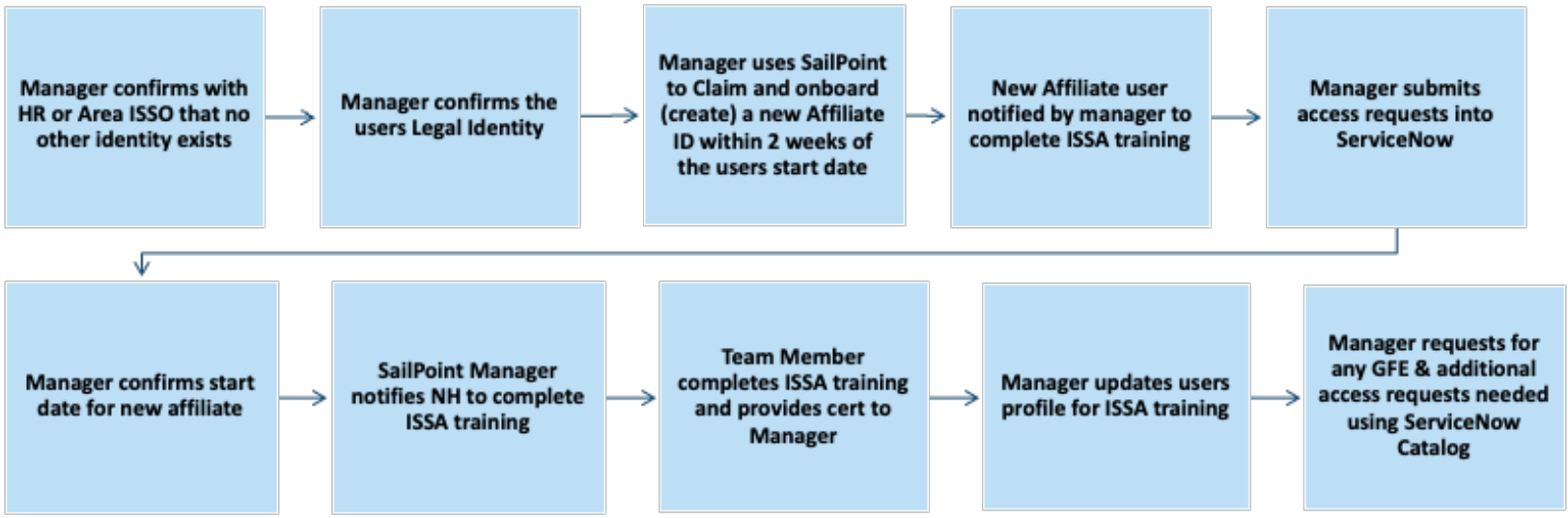

SailPoint
Home
My Work
Identities
Applications
Intelligence
Setup
Kathryn Lewis
Home
Edit
Claim and Onboard New Employee
Onboard External Affiliate
Manage My Alternates
Add Team Member
Transfer Team Member
View Identity
Approvals
0
Manage User Access
Track My Requests
Access Reviews
0
Notifications
0
Update Employee Profile
Direct Reports
Search for...
Albert Einstein
Alfred Butler
Allister Juris
Amy Fowler
Bob Skeleton
73 Total
Showing 1-5
Latest Approvals
Currently no data
All
Latest Forms
Currently no data
All
My Access Reviews
Currently no data
Certification Campaigns
Currently no data


IHS User Claim and Onboarding Form
Select User
Select User *
First Name
Last Name
Position Title
Org Name
Duty Station Name
User Details
Area *
Service Unit/Division *
RPMS Only User
Additional User Details
Facility Street Address *
City *
State *
Postal Code *
Telephone Number
Telephone number must be in the following format: ###-###-####. An extension may be added with the addition of an "x" followed by the extension number
Professional Skill Level
Please indicate the affiliate's professional skill level suffix if applicable. Leave blank if not applicable
ISSA Training Completed *
Please request the Team Member to send the completed ISSA Training Certificate to you as the manager indicating the ISSA email used to complete the training.
The Manager needs to indicate the ISSA email correctly as part of updating the employee profile. NOTE: Use of the D1 (AD) account is authorized only with a valid

Onboarding new IHS users (Team Members)

- PIV card issuance to be scheduled by the Area PSR
- Orientation for the First Day – Visit with HR (Federal Employee Benefits and forms, TSP, etc.), Learning about IHS, Introductions to Co-workers, Review of Organizational Charts, review of duties and performance expectations (PMAP), confirmation of access, etc.
- Providing an Orientation presentation or list of where to find information, training, etc. See https://youtu.be/4ezqKQYR828
- Access to other key systems – Mypay, ITAS, eOPF, Concur, LMS, etc.
- Where to go for Questions and Support (both IT and non-IT items)
- See a list of ServiceNow FAQs in the Portal

Claim and Onboarding for Affiliates



Participants: Contracting Officers Representatives (COR); Personnel Security Representatives (PSR)

Yearly ISSA Compliance

- Per IHS Policy, all IHS users having physical or IT access to Enterprise or local IT systems are required to complete the mandatory ISSA training by the due date provided by the IHS Chief Information Officer (CIO).
- ISSA compliance verification is based on the users HHSID and ISSA email account to verify completion
- By the due date, SailPoint IAM will enforce approved IT access verification based on the completed ISSA training for all current and new user identities.
- Access will be disabled for all non-compliant users until ISSA training has been validated and the users profile updated with the ISSA email.
- The FY24 ISSA compliance reached over 97% compliance by the due date required. Great work everyone!

Yearly Access Certifications

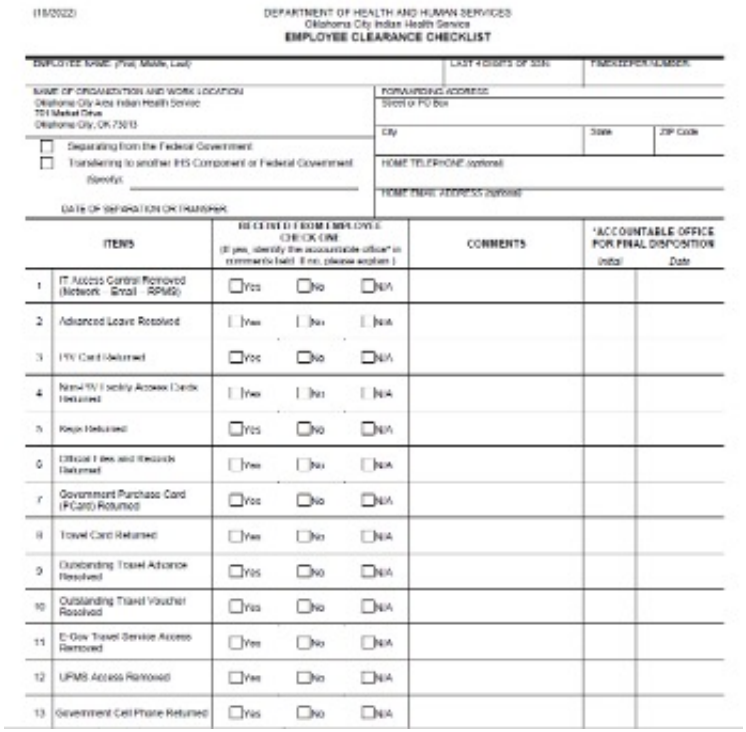
What are Certifications and Why is it required?

- Federal security regulations require all IAM Access Managers to conduct annual team member access reviews and validation for every team member once a year or more often as necessary, and make administrative changes if there are discrepancies. This annual access review is essential to ensure that users maintain only the access needed to do their jobs. This includes the determination for continued need for specific access and privileges in alignment with users role and duties. This process of reviewing and certifying access is known as certifications or an IT access review.
- These requirements apply to ALL identity types (employees, contractors and affiliates).
- As it can be seen, Identity and Access Management and the authorized access to critical IT systems, is a vital component of an organization's security posture. As we move forward into the next generation of business automation and Health IT, both on-premise and in the cloud, solid IAM business practices and associated technologies will help significantly ensure a more efficient and secure computing environment in support of patient care.
- This activity is currently performed once per year only for specific access items (Admin accounts, VPN, PIV Exemptions, Sponsor roles and minor HealthIT applications.
- This year's scheduled certification campaign resulted in a 90% compliance rate!

Off boarding Team Members

- Users/Team Members to be terminated are identified based on the following criteria:
  - Employees who will be leaving IHS
  - Contractors who are no longer supporting IHS
  - Users who may be moving to another IHS Area
- Preparation requires communications with HR and PSRs at least two weeks prior to the users last day (for termination in EHCM and SCMS)
- Managers must submit a Scheduled Termination using SailPoint IAM for the D1 account
- Managers must submit for access terminations for RPMS and other applications using ServiceNow

Off Boarding Checklist



(10/2022)

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Oklahoma City Indian Health Service
EMPLOYEE CLEARANCE CHECKLIST

EMPLOYEE NAME: (First, Middle, Last) | LAST 4 DIGITS OF SSN: | TIMEKEEPER NUMBER:

NAME OF ORGANIZATION AND WORK LOCATION
Oklahoma City Area Indian Health Service
701 Market Drive
Oklahoma City, OK 73013

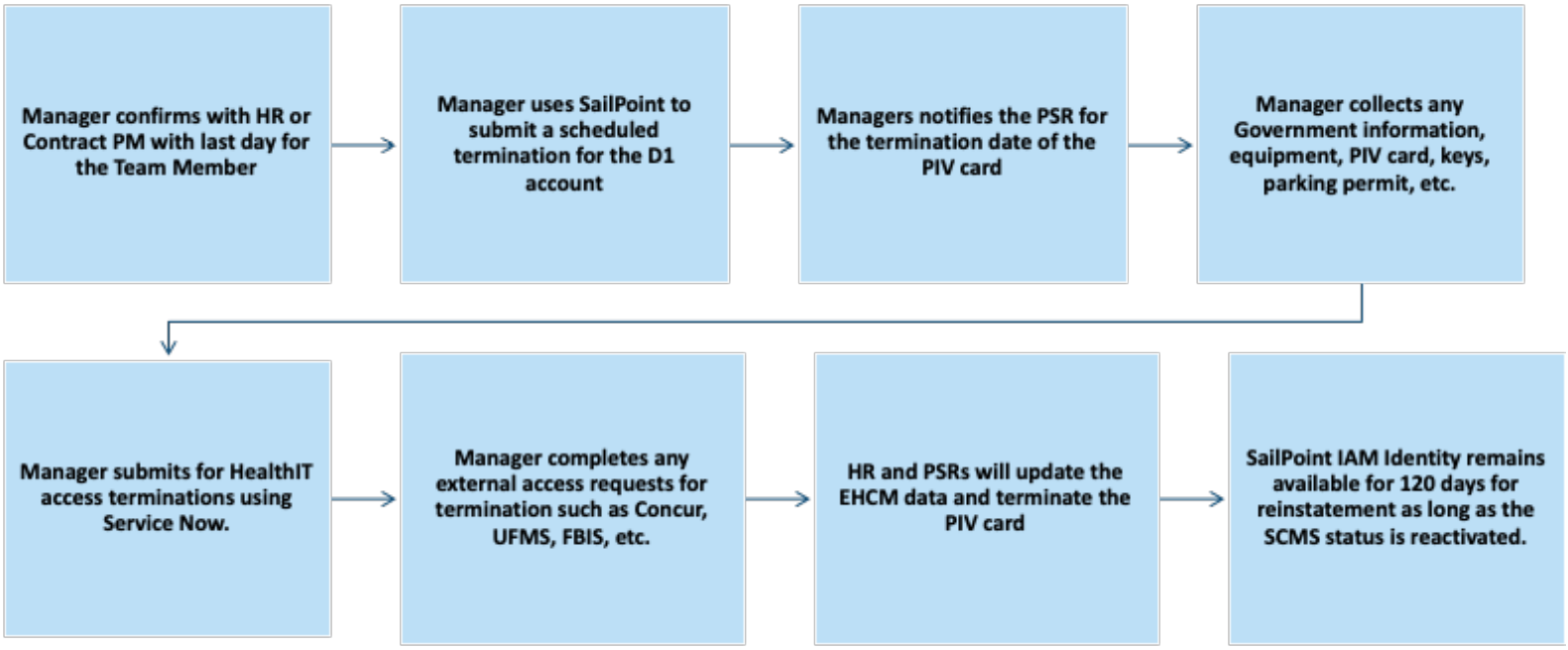
☐ Separating from the Federal Government
☐ Transferring to another IHS Component or Federal Government
Specify: _____

DATE OF SEPARATION OR TRANSFER:

FORWARDING ADDRESS
Street or PO Box
City | State | ZIP Code
HOME TELEPHONE (optional)
HOME EMAIL ADDRESS (optional)

	ITEMS	RECEIVED FROM EMPLOYEE CHECK ONE (If yes, identify the accountable officer* in comments field. If no, please explain.)			COMMENTS	*ACCOUNTABLE OFFICE FOR FINAL DISPOSITION Initial	Date
1	IT Access Control Removed (Network Email RPMS)	☐Yes	☐No	☐N/A			
2	Advanced Leave Resolved	☐Yes	☐No	☐N/A			
3	PIV Card Returned	☐Yes	☐No	☐N/A			
4	Non-PIV Facility Access Cards Returned	☐Yes	☐No	☐N/A			
5	Keys Returned	☐Yes	☐No	☐N/A			
6	Official Files and Records Returned	☐Yes	☐No	☐N/A			
7	Government Purchase Card (P-Card) Returned	☐Yes	☐No	☐N/A			
8	Travel Card Returned	☐Yes	☐No	☐N/A			
9	Outstanding Travel Advance Resolved	☐Yes	☐No	☐N/A			
10	Outstanding Travel Voucher Resolved	☐Yes	☐No	☐N/A			
11	E-Gov Travel Service Access Removed	☐Yes	☐No	☐N/A			
12	UPMS Access Removed	☐Yes	☐No	☐N/A			
13	Government Cell Phone Returned	☐Yes	☐No	☐N/A			

Terminating Identities and Access



Participants: Manager/Contracting Officers Representatives (COR); Personnel Security Representatives (PSR)

Reinstatements for Returning Users (Identities)

- IHS Identities with an HHSID# will continue to be stored from within SailPoint for potential future reinstatements.
- Returning users may be “reinstated” using Identity Operations within SailPoint IAM as long as the SCMS (PIV) card status is still active.
- Managers are to ensure that all team members have an HHSID. New Affiliate Identities will be required to be approved by the Area ISSO.
- Returning users will require new access requests to be submitted using ServiceNow.

References

- KB0013552 IAM: Manager's Quick Reference Guide to Team Management, https://ihsitsupport.servicenowservices.com/kb_view.do?sysparm_article=KB0013552 . This includes:
- KB0013552 IAM: Manager's Quick Reference Guide to Team Management, https://ihsitsupport.servicenowservices.com/kb_view.do?sysparm_article=KB0013552, to include updating a users profile for the Area/Facility and ISSA training compliance
- KB0013068 IAM: How to Reinstate a Disabled or Terminated Team member's AD Profile , D1 Network Access, https://ihsitsupport.servicenowservices.com/kb_view.do?sysparm_article=KB0013068
- KB0012019 IAM: How to View a User's Identity Attributes (Profile), https://ihsitsupport.servicenowservices.com/kb_view.do?sysparm_article=KB0012019
- KB0012036 IAM: How to Update Employee Profile or Initiate a Domain Transfer in IAM https://ihsitsupport.servicenowservices.com/kb_view.do?sysparm_article=KB0012036
- KB0013068 IAM: How to Reinstate a Disabled or Terminated Team member's AD Profile , D1 Network Access https://ihsitsupport.servicenowservices.com/kb_view.do?sysparm_article=KB0013068
- KB0012556 SailPoint/IAM Access Management Support Call Frequently Asked Questions, https://ihsitsupport.servicenowservices.com/kb_view.do?sysparm_article=KB0012556
- IAM SharePoint Training site
- Acronym lists and SharePoint sites may be available within each Area/Program for specific functions/services

Questions?

Kathryn Lewis
Manager, IT Operations
Headquarters, OIT
505-563-5080
Kathryn.Lewis@ihs.gov
Indian Health Service
itsupport@ihs.gov


INDIAN HEALTH SERVICE
PHS · 1955 ·