US Department of Health and Human Services

Indian Health Service

Privacy Impact Assessment

Date Signed:

January 2, 2018

OPDIV:

IHS

Name:

Information Technology Access Control

PIA Unique Identifier:

P-1209405-914897

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Test

Is this a FISMA-Reportable system?

No

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

No

Identify the operator.

Agency

Point of Contact (POC):

POC Title: Director, IT Operations

POC Name: Paul Kundtz

POC Organization: Indian Health Service

POC Email: **paul.kundtz@ihs.gov**

POC Phone: 301-443-2768

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Planned date of Security Authorization

2/28/2018

Describe the purpose of the system.

The Information Technology Access Control (ITAC) system is a consolidated enterprise system intended to provide an automated workflow for qualified Indian Health Service personnel to request, approve, and manage 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 request 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 ITAC system is an IHS-wide request system that will contain the following Personally Identifiable Information (PII) about employees, contractors and other affiliated users information in order to provide access to systems:

Full name, employment type affiliation (direct contractor, federal employee), job title, phone number, location, email, contract name, 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 access 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.

The ITAC system will collect and store information on IHS Active Directory users, as noted above, for the purpose of identifying users and requesting, approving, and documenting and managing their access permissions. User requests will be initiated by each users supervisor or sponsor who will access the system and identify what system access is required for each employee. The request will then be processed/routed through the system level approvers and grantors. Once completed, the information will be active and immediately available to system operators while the user is engaged with IHS. The same process for deactivation and removal of access will be followed through the deactivation of the users network account and all other access. All user information will be archived permanently upon the user’s departure and will be accessible to ITAC system administrators. Information will not be shared outside of IHS.

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

Yes

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

- Name
- Email Address
- Phone Numbers
- Mailing Address
- Employment Status

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

- Employees
- Business Partners/Contacts (Federal, state, local agencies)
- Vendors/Supplies/Contractors
- Other (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?

10,000-49,999

For what primary purpose is the PII used?

PII is used as part of the IHS ITAC system in order to clearly identify a specific user and manage what level of systems access is being requested for what specific systems for each IHS Area Office and local facility. It is used for management of all Active Directory users to include the approvals and management of access.

Describe the secondary uses for which the PII will be used (e.g. testing, training or research)

The ITAC system will also provide verification and reporting of the completion and status of the computer security training for each user as required per IHS policy.

Describe the function of the SSN

Not applicable.

Cite the legal authority to use the SSN

Not applicable.

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

Federal Information Processing Standard Publication 201-2, Personal Identity Verification (PIV) and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors and alignment with the Federal Identity, Credential, and Access management (FICAM) guidance. The 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 used to cover the system or identify if a SORN is being developed.

In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
    In Person
    Other
Government Sources
    Within the OPDIV
    State/Local/Tribal

Identify the OMB information collection approval number and expiration date.

OMB Expiration Date: 2/29/2020
OMB Approval No. 0917-0009

Is the PII shared with other organizations?

Yes

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

Within HHS (PII is only made available to those authorized to have access to such information. Those persons are allowed to access PII for staff at their organization level and below and within their Operating Division. Authorized personnel at the

Department level can access PII for employees throughout the Department as determined by role based access and least privilege policies.)

Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).

Interconnection Security Agreements (ISAs) and/or Memorandums of Understanding (MOUs) exist for all ITAC data records that are based on the security role and authorization outlined for each entity identified above.

Describe the procedures for accounting for disclosures

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.

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

The ITAC system is not intended to collect non-business-related personal information. The system will have a standard Privacy Act Notice.

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.

Users will be provided the option to opt-out with the understanding that access to Federal IT Systems will not be provided without the level of user identification required to be in compliance with Federal Identity Management mandates. There is no method to opt-out and still be approved for access to the IHS Federal Network. The collection of this information is needed for provisioning of access to federal information systems. Access cannot be provided in the event the individual decides to opt-out. ITAC uses PII in the process of creating user accounts. Access to the ITAC system must submit an official request and be approved prior to gaining access to the system.

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

During the employment process the user is provided with the IHS Privacy Act Statement which includes the collection of Personal Identifiable Information is necessary for the identity proofing requirements for employment. The users consent to these terms and conditions is documented into their employee records. If a user chooses not to consent to the terms and conditions they will not be able to access the MD-Staff Application or be provided access. The individual would need to complete an IHS 810 Form.

The Federal Warning Banner will be displayed during login that will describe that the system is a government operated system and that users can opt out of usage of the ITAC application at any time. Individuals would be notified directly of major system changes that affect their rights or interests, but no such changes are anticipated. Users are notified of information collected as part of the initial processing within the Human

Resources department as well as during collection of information required in order to obtain a Federal Identification card. Consent is obtained by user signature as part of the initial on-boarding process.

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 ITAC system is not intended to collect non-business-related personal information. Information related to the use of PII for each user is obtained during the initial on-boarding with the Human Resource office as well as signed consent to obtain a PIV card. ITAC contains data for federal civilian, Commissioned Corps and contract employees. All formal and informal requests and concerns and assistance are available from supervisors, human resource offices, the IHS IT Service Desk or Information Security Officers, all of which would ultimately lead to correction or mitigation. Note: Complaints may also be filed directly with the Secretary, DHHS for breaches of PHI.

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 ITAC system and associated user security policies requires yearly reviews of user information and access. These reviews will be completed as part of the validation of access to Federal IT Systems between the Federal Supervisor and employee/user. Additionally, the Indian Health Service Privacy Official (s) will conduct periodic reviews to ensure data integrity, availability, accuracy, and relevancy, and will conduct continuous monitoring, at a minimum, monthly reviews.

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

- Administrators: ITAC System Administrators (Direct Contractors) will require access to administer the Federal IT System on behalf of the Government. Modifications include security assessments, database health, and general system maintenance.
- Developers: ITAC Application Developers (Direct Contractors) will require access to manage the Federal IT System on behalf of the Government. This includes

design testing, configuration management and reporting of system health and maintenance.

- Contractors: Technical direct contract support staff will require access to the ITAC system in order to manage the Federal IT System on behalf of the Government.

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. Most IHS standard users do not have access to ITAC and the associated PII. For those that do have access to PII they fit into the following categories where access is limited to specific groups based on each functional security role: Supervisors, Approvers, Grantors, Administrators and general support staff.

Supervisors manage system access for the users they supervise by submitting access requests that are routed to approvers and grantors. They also annually review their users' access, track the progress of the submitted access requests, edit team members' profile and access information, and submit remove access requests when users leave the organization.

Approvers review access requests for completeness and correctness. The access request is approved if the approver determines that the user requires the access to perform job duties.

Grantors create accounts on information systems and ensure that users have access.

Administrators and support staff monitor the ITAC system to keep it fully operational and assist ITAC users with technical support requests.

All access is restricted using an authorization process and based on role definitions.

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 rights are determined based on position role and responsibility and as requested by Federal Sponsor. System users without administrator roles will see only the profiles of personnel who are on their team or are requesting access to their respective asset. Annual access reviews are performed to make sure user roles have not changed.

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

ITAC system operators are required to attend yearly Information System Security training sessions, Privacy Act and IT Rules of Behavior training to learn appropriate system use. In addition, user manuals are available along with other on-demand user resources.

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

PII restrictions are covered as part of the ITAC training documentation and annual security awareness training and available to all users regarding permissible disclosure. Users who do not complete training will not will have access to the system. In person, webinar based training is available as needed. Application management training for Administrators and user support training will be provided by the vendor engaged in the implementation.

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. Cite specific records retention schedules.

Records are retained and disposed of in accordance with National Archives and Records Administration's (NARA) General Records Schedule 2 (GRS 2). All record retention requirements are defined as statements in statutes, regulations, and agency directives or authoritative issuances, that provide general and specific requirements for Federal agency personnel on particular records to be created and maintained by the agency (36 CFR 1220.14).

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

Active Directory management for access to and management of user specific Personally

Identifiable Information data is dependent on delegation policies, roles and responsibilities and will prevent unauthorized access. All changes are tracked and logged to support any audit requirements. Active Directory technical controls will prevent non-network users from gaining access. The following administrative, technical and physical controls are in place for the ITAC system:

Contingency Plans

System Security Plans

Scheduled and validated Data Backups stored off-site

Least Privilege Access

Role based Security Awareness Training

Two factor Authentication (PIV)

Firewalls

Data Encryption

Intrusion Detection System (IDS)

Physically Secure Data Center with Key cards and locked server racks