# US Department of Health and Human Services
# Indian Health Service
# Privacy Impact Assessment

**Date Signed:**

5/8/15

**OPDIV:**

IHS

**Name:** IHS Infrastructure, Office Automation and & Telecommunications (IOAT)

**PIA Unique Identifier:**

P-5455720-482091

**The subject of this PIA is which of the following?**

Major Application

**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.**

New Interagency Uses

**Describe the purpose of the system.**

IHS Infrastructure, Office Automation & Telecommunications - 10/5/2005

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

1. Records containing general information on the person's residence, status of work, phone numbers and also the amount of monies awarded to the individuals using scholarships. These records are maintained and tracked from the

beginning of the scholarship process until the person enters employment within the Indian Health.

2. To provide a description of an applicant's interest in applying for jobs advertised within the Indian Health Service.
3. To provide IHS program officials with statistical data upon which the jobs and scholarships can be tracked and accounted for.
4. To serve as a means of communication among members of the personnel team who contribute to fillings and tracking jobs within the Indian Health Service.
5. To serve as the official documentation of jobs begin applied for and scholarships be paid to individual students.
6. To contribute to continuing education of IHS staff to improve their competency to deliver health care services and filling jobs within those health care disciplines.
7. To improve the IHS health care provides entering the Indian Health Service.
8. Yes, contains IIF. Mandatory submission of personal information.

**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
- Education Records
- Military Status, Mailing Address
- Employment Status

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

Public Citizens

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

One million or more

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

State/Local Health Agencies.

A. Records may be disclosed to individuals within the Indian Health Service in the

areas of personnel and finance.

B. Records may be disclosed to authorized organizations, such as the United States Office of Technology Assessment, or individuals for conduct of analytical and evaluation studies sponsored by the IHS.

C. Records may be disclosed to a congressional office in response to an inquiry from that office made at the request of the subject individual.

D. A record may be disclosed for a research purpose, when the Department:

1. Has determined that the use or disclosure does not violate legal or policy limitations under which the record was provided, collected, or obtained;
2. Has determined that the research purpose
    a. cannot be reasonably accomplished unless the record is provided in individually identifiable form, and
    b. warrants the risk to the privacy of the individual that additional exposure of the record might bring;
    c. Has required the recipient to
        i. establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record, and
        ii. remove or destroy the information that identifies the individual at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the research project, unless the recipient has presented adequate justification of a research or health nature for retaining such information, and
    d. make no further use or disclosure of the record except
        i. in emergency circumstances affecting the health or safety of any individual,
        ii. for use in another research project, under these same conditions, and with written authorization of the Department,
        iii. for disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the
        iv.

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

Yes

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

Yes

**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 data is collected via web-based applications from scholarship applicants and job candidates. Subjects are notified by various messages displayed on the web page. A privacy statement is posted on the site to notify subjects about how their information is handled.

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

The data is collected via web-based applications from scholarship applicants and job candidates. Subjects are notified by various messages displayed on the web page. A privacy statement is posted on the site to notify subjects about how their information is handled.

**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.** Both the SORN and Privacy SORN have a notification and contesting record procedures. See SORNS for details

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

Yes

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

- Users: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties. Authorized personnel include: job administrators and site contacts.
- Administrators: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties. Authorized personnel include: job administrators and site contacts.
- Developers: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties. Authorized personnel include: job administrators and site contacts.

- Contractors: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties. Authorized personnel include: job administrators and site contacts.

**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.** Policies and procedures are in place to ensure stored and transmitted / transported data are protected commensurate with their sensitivity. Policies and procedures are in place to ensure data are properly destroyed according to their sensitivity. Disposal methods include burning or shredding of hard copy and shredding or erasing of electronic media.

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

- Policies and procedures are in place to ensure access, to include physical access, to data and equipment is controlled according to operational requirements, personal clearances, and data sensitivity.
- Policies provide for periodic evaluation of threats and vulnerabilities to ensure risks are known and appropriate safeguards are implemented.
- Policies also delineate data backup, contingency operations, incident handling, information storage, sharing, and transmission/ transportation, malicious software protection, logging and audit, training, sanctions, disclosure, and personnel security requirements to ensure the confidentiality, integrity, and availability of the web servers and associated data.
- Each facility is responsible for conducting risk management processes and applying policies and procedures accordingly.
- Electronic and other personal data storage media, and associated computer equipment are stored in areas where fire and life safety codes are strictly enforced.
- Telecommunication equipment (computer terminal, modems and disks) are maintained in access controlled rooms during nonworking hours, Combinations on door locks are changed periodically and whenever an employee resigns, retires or is reassigned.
- Within each facility a list of personnel or categories of personnel having a

demonstrable need for the records in the performance of their duties has been developed and is maintained.

- Procedures have been developed and implemented to review one-time requests for disclosure to personnel who may not be on the authorized user list. Proper charge-out procedures are followed for the removal of all records from the area in which they are maintained. Persons who have a need to know are entrusted with records from this system of records and are instructed to safeguard the confidentiality of these records. They are to make no further disclosure of the records except as authorized by the system manager and permitted by the Privacy Act, and to destroy all copies or to return such records when the need to know has expired.
- Procedural instructions include the statutory penalties for noncompliance. A profile of automated systems security is maintained.
- Security clearance procedures for screening individuals, both Government and contractor personnel, prior to their participation in the design, operation, use or maintenance of IHS automated information systems are implemented.
- The use of current passwords and log-on codes are required to protect sensitive automated data from unauthorized access. Such passwords and codes are changed periodically. An automated audit trail is maintained.
- Privacy Act requirements and specified Automated Information System security provisions are specifically included in contracts and agreements and the system manager or his/her designee oversee compliance with these contract requirements.

**Does the website have a posted privacy notice?**

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.**

Session Cookies

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

No

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

**HHS?**

No