**PRIVACY IMPACT ASSESSMENT**
**For the**
**OFFICE OF NAVAJO-HOPI INDIAN RELOCATION**

**Publication Date: December 2012,**
**Revised and Reissued: October 2017**
**Reviewed: 09/2018, 09/2019, 03/04/20**

**Contact Point**

Diane Pratte, CIO
Office of Navajo & Hopi Indian Relocation
P.O. Box KK, Flagstaff, AZ 86002
(928) 779-2721

**Reviewing Official**

Christopher J. Bavasi
Executive Director
Office of Navajo and Hopi Indian Relocation
P.O. Box KK, Flagstaff, AZ 86002
(928) 779-2721

**Approving Official**

Christopher J. Bavasi
Executive Director
Office of Navajo and Hopi Indian Relocation
P.O. Box KK, Flagstaff, AZ 86002
(928) 779-2721

**System Manager for System or Application**

Diane Pratte, CIO
Office of Navajo and Hopi Indian Relocation
P.O. Box KK, Flagstaff, AZ 86002
(928) 779-2721

**IT Security Manager/ Received this Document**

Diane Pratte, CIO
Office of Navajo and Hopi Indian Relocation
P.O. Box KK, Flagstaff, AZ 86002
(928) 779-2721

**Office Privacy Act Officer**

Larry A Ruzow
Office of Navajo and Hopi Indian Relocation
P.O. Box KK, Flagstaff, AZ 86002
(928) 779-2721

## INTRODUCTION

## 1.0 SYSTEM APPLICATION/GENERAL INFORMATION - The System, the Information Collected and Stored Within the System.

### 1.1 What information is to be collected?

- The information to be collected is Navajo and Hopi client information relating to the eligibility process including name, address, social security number, tribal census number or other identifying number, symbol assigned to the individual.
- Information collected and stored within the system is statistical data and information for programmatic use.
- Information collected and stored within the system is program information on individual status, action, and activities.

### 1.2 Does this system contain any information about individuals?

- Yes, the system contains information about Navajo or Hopi clients who are impacted by Public Law 93-531 and subsequent amendments.
- The system also contains information on all employees of the Office of Navajo and Hopi Indian Relocation, including those who are Navajo and Hopi clients impacted by Public Law 93-531 and subsequent amendments.

### 1.3 From whom (what are the sources) is the information collected?

- The sources of information in the system on clients and family members are derived directly from the Navajo and Hopi clients impacted by Public Law 93-531.
- Other sources of information for clients and their family members are external sources, including federal, tribal or local agencies.
- Sources of information maintained on ONHIR employees are derived directly from the employee.

## 2.0 PURPOSE OF THE SYSTEM AND THE INFORMATION COLLECTED AND STORED WITHIN THE SYSTEM

### 2.1 Why is the information being collected?

The client information in identifiable form is being collected for the following purposes:

- The eligibility process for Navajo and Hopi clients impacted by Public Law 93-531 and subsequent amendments.
- Statistical reports
- Demographic data
- Agency program status and activities
- Homesite lease process
- Appeals process
- Budget preparation.
- Congressional or government reports

**2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information**?

- The legal authority that authorizes the collection of information is Public Law 93-531 and subsequent amendments.
- 25 C.F.R. Section, 700.257 (d) authorizes the collection of information for collection, maintenance, use or dissemination.

**2.3 Privacy Impact Analysis: Given the amount and type of information collected as well as the purpose, discuss what privacy risks were identified and how they were mitigated.**

Privacy risks involve creation, recording, filing, maintenance, and storage, of electronic and manual records containing information. The risks were mitigated in the following manner:

- Development and implementation of the Automated Casefile Checkout System (ACCS) for access to physical records containing PII .
- Utilization and compliance of NARA standards for all record keeping and information systems to ensure authenticity and reliability.
- Establishment of agency directives, policies, priorities, or procedures that govern and provide guidance on electronic and physical records containing PII data to ensure proper authorization and prevent loss or destruction.
- Standards for maintenance of record keeping and information systems are subject to the Privacy Act and Freedom of Information Act in accordance with 25 C.F.R., Section 700.261 (a), (b), (c).
- Implementation of annual staff training to ensure compliance with Privacy Act requirements on electronic and manual records that contain PII or other data.
- Internal maintenance procedures that require a semi-annual inventory of physical records that contain client PII.
- Creation and implementation of strategies, responsibilities and requirements to support maintenance and use requirements of record keeping and information systems to ensure integrity and security of the information and data contained within the systems.

## 3.0 USES OF THE SYSTEM AND THE INFORMATION

**3.1 Describe all uses of the information**

- The eligibility process for Navajo and Hopi clients impacted by Public Law 93-531 and subsequent amendments.
- Economic impact and development studies.
- Community impact and development studies
- Budget preparation

**3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern**?

Yes, programs have been written and special queries can be requested to identify a group of clients (data elements). Data may be analyzed for the following purposes:

- Identify clients affected by amendments, court decisions, and other Federal and management directive changes.

- To provide statistics to management or other parties such as the media or Congress.
- To review and determine necessary changes to eligibility levels.
- To help management in the review of the Agency departmental performance and determine areas needing assistance.
- To assist management in determining techniques or methods to improve the operation of the agency and service to the clients.

**3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?**

- Accuracy is determined through standards for record series and system requirements that are designated by the National Archives and Records Administration.
- Information collected and derived from the system is verified for accuracy through public records, employment records, court records, tribal records, school records, or other records for development of eligibility criteria (Public Law 93-531 and 25 C.F.R., Section 700.147).
- Information will be checked for accuracy of type, valid coding (when practical), and existence of cross-referenced data when applicable via entry program controls (System Security Plan, Section 3.9.10).

**3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?**

- The retention period of the data in the system is determined by the type of data, the information collected and the format of the data, either electronic or physical.
- Standards for record series and retention are established, authorized and approved and by NARA authorities, 36 C.F.R. 1228.20 - 1228.32, Subpart B, and authorize the agency to:
  - Request records/data retention disposition authority
  - Formulate, develop record/data retention and disposition schedules
  - Maintain, schedule and transfer temporary or permanent record/data (physical and electronic).

- Require an authorized individual to validate records destruction and transfer, review or correct, assign and change records and provide an audit trail of record/data retention and dispositions.
- Compliance with specifications is identified by NARA (36 C.F.R.1228.188**)**

**3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.**

- Archival functions are planned, determined and incorporated in an integrated manner for managing information throughout the lifecycle of the information and data contained in the system in accordance with NARA requirements.
- Records management and archival functions are designed, developed and implemented into the information systems to record, preserve and make accessible sufficient information to ensure the management and accountability of agency programs in accordance with NARA requirements.
- The information systems used by the agency are designed to protect the legal and financial rights of the federal government in accordance with federal statutes and issuances that govern records management. Those authorities are derived from Federal Records Act, 36 C.F.R. and OMB Circular A-130.

## 4.0 INTERNAL SHARING AND DISCLOSURE OF INFORMATION WITHIN THE SYSTEM

**4.1 With which internal components of the agency is the information shared?**

Information is shared with all internal departments within the agency that require use of the information for programmatic purposes.

**4.2 For each recipient, component or office, what information is shared and for what purpose?**

Information is available to be shared with each department within the agency and for specific purposes listed below:

- Executive - budget, program information
- Administration - budget, program information
- Relocation Operations - eligibility, program information
- Personnel - budget, FTE information

**4.3 How is the information transmitted or disclosed?**

Data is transmitted to intra-agency components to include retrieval of information from the following sources:

- Information is retrieved from physical record systems maintained within the agency. The retrieval of the physical records is tracked through the ACCS.
- Information is retrieved from the electronic records system using staff menus

(which control information access) on the AS/400.

- Information is disclosed when requested through an FIOA request that is approved by the agency Privacy Act Officer.
- Information is disclosed as allowed in 25 C.F.R. 700.267 and 25 C.F.R. 700.525 (d).

**4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated**.

The risks identified were ensuring the use of information for programmatic purposes, and maintaining the security and integrity of information maintained within the electronic information system and agency physical records. These risks are mitigated by:

- Creation and implementation of proper controls to protect the information and data, ensure its integrity and prevent unauthorized access through security measures.
- Development of record series, records schedule and record keeping system requirements established and authorized by the National Archives and Records Administration.
- Implementation and compliance with Privacy Act regulations for internal sharing information and data.
- Agency wide prescribed procedures to govern and appropriately manage security and protection of information and data in accordance with 25 C.F.R. Section 700.259 and Section 700.261(a).

## 5.0 EXTERNAL SHARING AND DISCLOSURE

**5.1 With which external recipients is the information shared?**

- Information or data is shared with federal, tribal, local or legal agencies as well as the media and the public.

**5.2 What information is shared and for what purpose?**

- Disclosures of information are usually in response to Freedom of Information or Privacy Act Requests from varied external sources including clients, the public, legal entities, government agencies and the media.
- Disclosures of information are generally provided for litigation, legal issues, programmatic or policy issues, agency activities or status and statistical information purposes.
- Disclosures are also provided in response to public or private entities who request information of a programmatic or statistical nature.

**5.3 How is the information transmitted or disclosed?**

- Information is transmitted in various formats including written correspondence, computer reports, or other documents.
- Information is transmitted via electronic mail. Subsequent attachments to the e-mail containing personally identifiable information (PII) will be encrypted according to policy. Other Agency information is transmitted via Virtual Private Networks, i.e. IBC.

**5.4 Are there any agreements concerning the security and privacy of the data once it is shared?**

Yes, agreements concerning the security and privacy of the data are made in advance of the sharing the data.

**5.5 What type of training is required for users from agencies outside ONHIR prior to receiving access to the information**?

- Notice is provided to all external sources requesting information, in accordance with 25 C.F.R. Section 700.263 (b), stating that a warning will be issued that summarizes that the Privacy Act carries a criminal penalty for the unauthorized disclosure of records for which it applies.
- 25 C.F.R., Section 700.267 provides for written assurance that the record will be used for purposes intended, and the record is not transferred in an individually identifiable form.

**5.6 Are there any provisions in place for auditing the recipients' use of the information?**

No provisions are in place for auditing the recipient's use of the information.

**5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated:**

An identified risk is the unauthorized release of information and privacy concerns that would allow for exposure of information. Mitigation of this risk is as follows:

- Compliance with administrative controls and procedural standards for handling, protection, security and maintaining the integrity of electronic and physical records in accordance with 25 C.F. R., Section 700.265.
- Compliance with Privacy Act requirements to protect against unauthorized release of information to external sources.
- Compliance with the statutory requirement of 25 C.F.R., Section 700.263 that ensure the security and confidentiality of records and how they are to be maintained in manual (physical) form and electronic form within the agency.

## 6.0 NOTICE

**6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, privacy act notice on forms or a system of records published in the Federal Register Notice). If notice was not provided, why not?**

- Notification is provided to the individual prior to collection of information as part of the eligibility process as required by Public Law 93-531, and subsequent amendments.
- A Privacy Act notice appears on the ONHIR *Request and Authorization for Disclosure of Information and Certification of Identity* form. The form is signed by individuals who request information prior to the collection of information and release of information. (See Attached copy in Appendix.)*
- In accordance with 25 C.F.R. Section 700.261 (d), (2), (I) (ii) (iii), (iv), (3)(i)(ii), (iii), provides that requirements be issued for advice to individuals concerning uses of information. The requirements state that at a minimum, the notice to the individual must state, the authority, the purpose, the routine uses, the effects as well as the standards for collection of information.

**6.2 Do individuals have an opportunity and/or right to decline to provide information?**

- Yes, individuals do have an opportunity and/or right to decline to provide information.

**6.3 Do individuals have an opportunity to consent to particular uses of information, and if so what is the procedure by which an individual would provide such consent?**

- In accordance with 25 C.F.R., Section 700.261(d)(2)(iv), authorizes the solicitation of information, the uses of information, the purposes, and provides that a notice be granted to individuals as to the basis for consenting to supply information and consequences, if any, of not supplying information.
- Procedures for consent for solicitation of information is provided in 25 C.F.R., Section 700.261 (3)(i)(ii) and (iii). This section covers using forms for collection of information and providing notice to individuals, and in some cases, written acknowledgment by the individual for collection of information.

**6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.**

The privacy risk identified was the unauthorized access to or release of information or data to external sources. This risk has been mitigated by:

- Standards for record series and system requirements that are built into

information systems including electronic record keeping system (ACCS), an automated process of managing electronic records that ensure authenticity and reliability.

- Development of agency policies and procedures to protect and secure information through data management systems that evaluate, organize and determine use and value of information as established in the 25 C.F.R. Chapter IV, Subpart K Sections 700.259 through 700.295 and ONHIR Management Manual, Sections 6310.1, 6310.2, 6080.2.
- Development of records maintenance procedures in accordance with NARA regulations.
- Training to ensure the accurate execution of policy and procedures.

## 7.0. INDIVIDUAL ACCESS AND REDRESS

### 7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

- The procedures which specifically address the opportunity for individuals to seek access to their own information is detailed in 25 C.F.R., Sections 700.235 Subpart J, through 700.283. The policies outlined in these sections provide detailed instructions on how individuals can access information maintained in the system.
- The procedures which specifically address the opportunity for individuals who seek redress or amendment of their own information is outlined in 25 C.F.R., Sections 700.285 thru 700.295. The requirements outlined in these sections provide detailed instructions on how individuals can seek to amend or redress information from the agency.

### 7.2 How are the individuals notified of the procedures for seeking access to or amendment of their information?

- As specified in 25 C.F.R, Section 700.269, an individual desiring access to information or disclosures of a record pertaining to themselves shall follow procedures outlined in 25 C.F.R. Section 700.277. The instructions and procedures in this section are available upon request to individuals who seek access to information.
- As specified in 25 C.F.R., Section 700.285, the Privacy Act permits an individual to request amendment of a record pertaining to themselves based on specific reasons in accordance with 5 U.S.C. 552a(d)(2). The instructions and procedures in this section are available upon request to individuals who seek to amend information.

**7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individuals?**

- 25 C.F.R., Section 700.293, (a)(b)(2)(c)(2)(3) provides procedures for to seek redress or amendment to information when a petition for amendment which has been rejected. These procedures are available upon request to individuals who seek recourse as other alternatives to amend information.

**7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system taken as a result of agency reliance on information in the system.**

- 25 C.F.R., Section 700.287 details procedures on how an individual can make request for amendment of a record.
- 25 C.F.R, Section 700.293 details procedures for an individual to appeal when a petition for amendment is rejected in whole or in part, for information contained in the system as a result of agency reliance on information.

## 8.0 TECHNICAL ACCESS AND SECURITY

**8.1 Which user group(s) will have access to the system?**

The user groups who will have access to the information system are those who are authorized to have access to information for programmatic or information technology use, to include:

- Executive
- Administrative
- Relocation Operations
- Legal Counsel

**8.2 Will contractors to the Agency have access to the system? If so, submit a copy of the contract/PO describing their role with this PIA.**

***Copies of contracts/PO will be held on file.***

**8.3 Does the system use "roles" to assign privileges to users of the system?**

ONHIR Management Manual Section 7020.1 lists in sequence the titles or roles of various staff who are involved in the process of granting authorization for changes and access to users of the system.

**8.4 What procedures are in place to determine which users may access the system and are they documented?**

Agency procedures for accessing the computer system are documented in Section 7020.1 of the agency Management Manual. These procedures outline the process of granting authorization for changes or access to users of the system.

**8.5 How are the actual assignments of roles and rules verified according to established security?**

The security level and type of access is documented in Section 7020.1 procedures of the agency Management Manual details the process and assignment of roles for authorization to secure automated data against unauthorized access.

**8.6 What auditing measures and technical safeguard are in place to prevent misuse of data?**

- Auditing measures and technical safeguard procedures are detailed in Section 7020.1 and 7020.2 of the ONHIR Management Manual.
- The Management Manual sections referenced above provide technical instructions and authorization roles for securing automated data and changes to computer access.

**8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?**

- Privacy Act requirements for records maintained in computerized form are detailed in accordance with 25 C.F.R Section 700.263(c).
- Section 7020 of the agency Management Manual procedures identifies requirements for training for users of the system that is relevant to the functionality of the program or system.
- The ONHIR Information Security Handbook provides for annual training of staff in relation to the protection, use restrictions, and maintaining functionality of the system.
- The ONHIR System Security Plan, Section 3.1 outlines further protection requirements.
- The ONHIR Privacy Rules of Conduct document provides guidance to ONHIR staff and contractors on the handling of this information.

**8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?**

Yes, data is secured in accordance with FISMA requirements. The execution of a full Certification and Accreditation (C&A) is currently being developed. The Director has issued an interim authority to operate.

**8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.**

The privacy risks identified are the probability of human error and/or the accidental deletion or modification of data. These risks have been mitigated by:

- Periodic checks of staff information entry and handling.
- Electronic cross checks of information stored.
- Reporting of modifications and deletion of data.
- Controlled access to delete information with cross checks of the process.

## SECTION 9.0 TECHNOLOGY

**9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?**

System goals and mission have not changed since the inception of the system. There have been new technologies developed over the life of the system and their use has been incorporated when practical and within budget.

**9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.**

As enhancements are considered for the system, current processes are evaluated for the effect the enhancements may have on the integrity, security, and privacy of the data. A through systems analysis of the new hardware, information, or software being considered and how it will interact with current technology is completed before implementation of same.

**9.3 What design choices were made to enhance privacy?**

The system is protected by unique user ID and password security and Multi Factor Authentication. Coding is embedded into programs to assure access to certain processes and information is protected from access. The network has been enhanced to protect from intrusion by unwanted sources. Antivirus and Malware protection are managed by a central system. Various encryption options have been deployed. Manual process is done to continue our removal of social security or EIN numbers when no longer needed by the financial officer.

## CONCLUSION

The Privacy Impact Assessment conducted by the Office of Navajo and Hopi Indian Relocation provides for certain protections to be built into the system for handling and managing information in identifiable form:

- To ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy.
- Determine the risks and effects of collecting, maintaining and disseminating information.
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The Privacy Impact Assessment (PIA) conducted by the Office of Navajo and Hopi Indian Relocation will ensure that system owners and developers have incorporated privacy protections throughout the life cycle of a system by ensuring that certain privacy protections are built into the system from the beginning.

The Privacy Impact Assessment (PIA) has provided that the Program Manager, the FOIA/Privacy Act Officer, address privacy issues to ensure appropriate and timely handling of privacy concerns. The PIA conducted by ONHIR represents a commitment for analyzing and sharing information within the agency, and addresses the need to place protections for privacy of information in identifiable form that is collected, stored, retrieved and shared. The protections in place for information privacy seek three objectives:

- Minimize intrusiveness into individual privacy while executing the mission of the agency
- Maximize fairness in agency decisions made about individuals
- Observe reasonable expectations of individual privacy and safeguard personally identifiable information.

The Office's Privacy Impact Assessment demonstrates that the agency considers privacy from the first stages of system development and throughout its life cycle, and system developers and owners have made technological choices that reflect the incorporation of privacy into the system. The PIA also demonstrates that as the system needs updating, privacy protections have been implemented into the updates. To accomplish this endeavor involves collaboration between program, information technology and security components to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system. It also requires evaluation of protections and alternative processes for handling information to mitigate potential privacy risks.

The Office is committed through comprehensive and meaningful collaboration and commitment of agency senior officials to use technologies that do not erode privacy, but sustain it and these objectives are reflected in the Privacy Act Assessment.

**RESPONSIBLE OFFICIALS**

Christopher J. Bavasi
Executive Director

Larry A Ruzow
Privacy Act Officer

Diane Pratte
Chief Information Officer Reviewed/Signature

**APPROVAL/SIGNATURE**

Christoph Executive Director
Office of Navajo and Hopi Indian Relocation

Date

## APPENDIX

Attachment references in Section 6.1:

REQUEST AND AUTHORIZATION FOR DISCLOSURE OF AND INFORMATI0N
CERTIFICATION OF IDENTITY

FULL NAME OF REQUESTER _____

CLIENT NAME _____ CENSUS # _____ SS#_____

I hereby request and authorize the Office of Navajo and Hopi Indian Relocation to provide copies of documents listed below from ONHIR Client Casefile # _____ .

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I am the person named above, and I understand that any falsification of this statement is p1ift.ishable under the provision of 18 U.S.C. Section 1001 by a fine of not more than $10,000 or.by imprisonment or not more than five years or both, and that requesting or obtaining any record(s) under false pretenses is punishable under the provisions of 5 *V.S.C.* 552a(iX3) by a fine of not more than $5,000.

_____ _____
Signature Date

_____ _____
Address Identity Verification (Drivers License, cm, Social)

_____ _____
City, State, Zip ONHIR Employee Signature Date

**Records Requested**:

_____

_____

**Interpreter's Clause**

I, _____ (Interpreter name) can speak and understand both the Navajo and English languages and swear that I have faithfully translated the above Authorization for Disclosure of Confidential Information to _____ (Client name), to the best of my ability and understanding. That _____ (Client name) did understand the same and swears that the averments contained therein are true and correct to the best of his/her/their knowledge.

_____

Interpreter Signature Date

**Optional: Authorization to Release Information to Another Person**

This section is to be completed by a requester who is authorizing information relating to himself or herself to be released to another person. Further, pursuant to 5 U.S.C. Section 552a(b), I authorize the Office of Navajo & Hopi Indian Relocation to release any and all information relating to me to: _____

_____

**Response Time:**

Under the 1974 Privacy Act statute, all federal agencies including the Office of Navajo and Hopi Indian Relocation are required to respond to a FOIA request within thirty business days. This time period does not begin until the FOIA Privacy Act request is received by this Office. A federal agency is not required to send out the releasable documents by the last business day; it can send you a letter informing you of its decision and then send the documents within a reasonable time.

Rev. 5/08