OFFICE OF NAVAJO AND HOPI INDIAN RELOCATION (ONHIR) GENERAL SUPPORT SYSTEM (GSS)

Version:	**1.1**
System Acronym:	**ONHIR GSS**
Document Title:	**Privacy Impact Assessment (PIA)**
Date Created:	**04/07/2021**

Document Change/Review History

Table 1: ***Document Change/Review History,*** below, details changes and reviews to the ONHIR GSS Privacy Impact Assessment (PIA) document.

Document Version	Change Description	Change POC	Change Date
1.0	Initial Document	Kareem Adham Softthink Solutions, Inc.	04/07/2021
1.1	Added ONHIR contacts, Added signature for Executive Director, Changed C.3.2.5 and C.3.3.4 to have words that apply to the Agency	Diane Pratte, ONHIR	5/14/2021
1.1	Review	Diane Pratte	1/11/2022

Table 1: Document Change/Review History

Document Approval Page

This document must be signed by the ONHIR CIO or other ONHIR personnel with written authority to act as the Authorizing Official (AO) to be considered authoritative. This document can be signed either physically (wet signature) or digitally using a PKI-enabled digital signature (non-repudiation).

X Diane Pratte, CIO 2/7/2023

Diane Pratte
ONHIR Designated Authorizing Official

X

Christopher J Bavasi
Executive Director

Approved based on STSI's involvement and analysis

X 2-12-2023

Lawrence A. Ruzow
Privacy Officer

References

The following reference material was used in the development of this document:

a) **NIST SP 800-30 Revision 1**, "*Risk Management Guide for Information Technology Systems*"
b) **NIST SP 800-37 Revision 2**, "*Risk Management Framework for Information Systems and Organizations*"
c) **NIST SP 800-53 Revision 4**, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
d) **NIST SP 800-60 Volume I Revision 1**, "*Guide for Mapping Types of Information and Information Systems to Security Categories*"
e) **NIST SP 800-60 Volume II Revision 1**, "*Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*"
f) **NIST SP 800-122**, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
g) **NIST SP 800-144**, "*Guidelines on Security and Privacy in Public Cloud Computing*"
h) **NISTIR 8062**, "*An Introduction to Privacy Engineering and Risk Management in Federal Systems*"
i) **5 U.S.C. § 552a**, **Freedom of Information Act of 1996**, As Amended by *Public Law No. 104-231, 110 Stat. 3048*
j) **5 U.S.C. § 552a, Privacy Act of 1974**, As Amended
k) **Public Law 100-503, Computer Matching and Privacy Act of 1988**
l) **E-Government Act of 2002 § 208**
m) **Federal Trade Commission Act § 5**
n) **44 U.S.C. Federal Records Act**, *Chapters 21, 29, 31, 33*
o) **Title 35, Code of Federal Regulations**, *Chapter XII, Subchapter B*
p) **OMB Circular A-130,** "*Management of Federal Information Resources*", 1996
q) **OMB Memo M-10-23**, "*Guidance for Agency Use of Third-Party Websites*"
r) **OMB Memo M-99-18**, "*Privacy Policies on Federal Web Sites*"
s) **OMB Memo M-03-22**, "*OMB Guidance for Implementing the Privacy Provisions*"
t) **OMB Memo M-07-16**, "*Safeguarding Against and Responding to the Breach of PII*"
u) **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
v) **NIST SP 800-70 Revision 4**, "*National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*"

Table of Contents

List of Tables

OFFICE OF NAVAJO AND HOPI INDIAN RELOCATION

1. Introduction

The Office of Navajo and Hopi Indian Relocation (ONHIR) is completing this Privacy Impact Assessment (PIA) for the ONHIR General Support System (ONHIR GSS). The ONHIR GSS information system (IS) provides critical Information Technology (IT) infrastructure/capabilities to the organization. The Privacy Threshold Assessment (PTA) indicated that the ONHIR GSS (IS) is a "Privacy Sensitive System".

2. Overview

This PIA is designed to demonstrate ONHIR's structured processes for identifying and mitigating privacy risks to the ONHIR GSS (IS). Special consideration was given to the confidentiality of the information and information system in the development of the PIA (***ref f***). The ONHIR GSS PIA is designed to ensure the (IS) will meet the following objectives throughout the system's lifecycle:

a. Ensure the (IS) handling of PII information conforms to all applicable legal, regulatory, and policy requirements (***ref f***)
b. Determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic (IS) (***ref f***)
c. Identify and evaluate protections and alternative processes for handling information to mitigate potential privacy risks (***ref f***)

2.1 ONHIR Organizational Background

The ONHIR was established by Congress to implement the settlement of a land conflict between the Navajo and Hopi Indian Tribes. The Office was established under Public Law 93-531 (as amended) and operates under this law as amended. The primary mission of ONHIR is to provide quality services to eligible households and others impacted by the relocation act, in such a way that ONHIR clients have the opportunity to re-establish their lives in a positive and productive manner.

2.1.1 ONHIR Organizational Structure

The ONHIR organizational structure has three sections: **ONHIR Executive Director, ONHIR Mission Area Personnel**, and **ONHIR Mission Support Areas**.

- **ONHIR Executive Director:** Is directly responsible for the strategic, operational, and managerial oversight of the Designated Agency Ethics Official (DAEO), and Designated EEO Official (DEEOO). The ONHIR Mission and Mission Support Areas report to the ONHIR Executive Director. The ONHIR Executive Director is not typically involved in the day-to-day business activities and is not given administrator access to ONHIR Mission and Mission Support files, work products, or IT assets (primarily the Waldo server).
- **ONHIR Mission Area Personnel:** Are directly responsible for the strategic, operational, and managerial oversight of the Finance department, Contracting department, Information Systems department, Relocation Operations department, New Lands Development

department, Legal department, and the Human Resources department. The ONHIR Mission Area personnel are not typically given administrator access to ONHIR Executive Director's office or Mission Support files, work products, or IT assets.

- **ONHIR Mission Support Areas:** Are directly responsible for strategic, operational, and managerial oversight of the Finance department, Contracting department, Information Systems department, Relocation Operations department, New Lands Development department, Legal department, and the Human Resources department. The ONHIR Mission Support Area personnel are not typically given administrator access to ONHIR Executive Director's office or Members or Mission Area files, work products, or IT assets, with exception of Information System personnel. The Information System personnel that are assigned as administrators are typically given rights to access IT assets from the ONHIR Executive Director's office, and the Mission Area, and Mission Support Areas.

2.2 ONHIR GSS System Description

ONHIR GSS (IS) provides personnel with the IT infrastructure/capabilities to perform their assigned tasks. The ONHIR GSS (IS) is comprised of one subsystem: **ONHIR General Support System (GSS)**. The subsystem acts in concert to provide ONHIR personnel with the following IT capabilities:

- Data storage and retrieval
- Data receiving and transfer
- File repository
- Local Network and Internet access
- Inter Office Telephony communication
- E-mail services
- Document creation, modification, and deletion (MS Office, etc.)
- Printer services

2.3 ONHIR GSS PII Collection and Uses

ONHIR GSS (IS) typically collects and utilizes Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (S-PII) during the execution of mission related tasks utilizing information types that fall under the C.3.2.5 Financial Management: Payments, C.3.3.4 Human Resource Management: Compensation Management, C.3.5.6 Information & Technology Management: Record Retention, which are described in NIST SP 800-60 Volume II Revision 1 "*Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*",

2.3.1 C.3.2.5 Financial Management: Payments

"Payments include disbursements of Federal funds, via a variety of mechanisms, to Federal and private individuals, Federal agencies, state, local, and the private sector, to effect payment for goods and services, or distribute entitlements, benefits, grants, or claims. Payment management provides appropriate control over all payments made by or on behalf of an organization, including but not limited to payments made to: vendors in accordance with contracts, purchase orders and other obligating documents; state governments under a variety of programs; employees for salaries and expense reimbursements; other Federal agencies for reimbursable work performed; individual citizens receiving Federal benefits: managing time, attendance, leave and pay; and managing payroll."

2.3.2 C.3.3.4 Human Resource Management: Compensation Management

"*Compensation Management designs, develops, and implements compensation programs that attract, retain and fairly compensate agency employees. In addition, designs, develops, and implements pay for performance compensation programs to recognize and reward high performance, with both base pay increases and performance bonus payments. This sub-function includes developing and implementing compensation programs; administering bonus and monetary awards programs; administering pay changes;"*

2.3.3 C.3.5.6 Information & Technology Management: Record Retention

"Records Retention involves the operations surrounding the management of the official documents and records for an agency."

2.4 ONHIR Organizational Usage of PII

The following table highlights the typical organization usage of PII for each subsystem in the ONHIR GSS information system.

ONHIR GSS Subsystem	Information Categories Utilized	Typical PII Usage
Microsoft Office 365	C.3.3.4 Human Resource Management: Compensation Management	PII is typically utilized to process client housing and land relocation applications, case files, contracts, ONHIR employee HR actions, and employee compensation.
ONHIR servers (IBM i System AS400 Waldo server, ONHIR-DC1 server	C.3.2.5 Financial Management: Payments, and C.3.3.4 Human Resource Management: Compensation Management	PII is typically utilized to process client housing and land relocation applications, case files, contracts, ONHIR employee HR actions, and employee compensation.
ONHIR Endpoints (Desktops, laptops, Verizon cell phones)	C.3.3.4 Human Resource Management: Compensation Management	PII is typically utilized to process client applications and contracts, and HR actions. PII can be transferred verbally utilizing the telephony communication system. PII data is transmitted but not saved on agency endpoints as a policy.
Network (Flagstaff computer network, New Lands Chambers network, New Lands Sanders network) using CenturyLink (Lumen)	C.3.2.5 Financial Management: Payments, and C.3.3.4 Human Resource Management: Compensation Management	PII is transferred and received utilizing the network infrastructure.
Interior Business Center (IBC)	C.3.2.5 Financial Management: Payments and C.3.3.4 Human Resource Management: Compensation Management,	PII is transferred and received utilizing the third-party financial system.

Table 2: Typical ONHIR Organizational ONHIR GSS Usage of PII

2.5 ONHIR GSS PII Protections

The ONHIR GSS (IS) has been developed with an emphasis placed on the protection of PII and S-PII information. The (IS) System Security Plan (SSP) incorporates the guidelines for the implementation of the Risk Management Framework (RMF) Assessment and Authorization (A&A) process as outlined in NIST SP 800-37 Revision 2 "*Risk Management Framework for Information Systems and Organizations*". ONHIR GSS (IS) incorporates the appropriate baseline security controls to protect the confidentiality, integrity, and availability (CIA) of the system. ONHIR GSS utilizes "Low" level baseline security controls, as outlined in the NIST SP 800- 53 Revision 5, "*Security and Privacy Controls for Federal Information Systems and Organizations*". ONHIR is committed to protecting the PII information contained in the ONHIR GSS (IS) by emphasizing the following security controls listed in ***Table 4: Critical PII Protection Controls***.

Control Number: Description	Control Description	Reference
AC-3: Access Enforcement	Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists). This can be done in many ways.	**Ref (c) (f)**
AC-5: Separation of Duties	Organizations can enforce separation of duties for duties involving access to PII.	**Ref (c) (f)**
AC-6: Least Privilege	Concerning PII, the organization can ensure that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.	**Ref (c) (f)**
AC-17: Remote Access	Organizations can choose to prohibit or strictly limit remote access to PII. If remote access is permitted, the organization should ensure that the communications are encrypted.	**Ref (c) (f)**
AC-19: Access Control for Mobile Devices	Organizations can choose to prohibit or strictly limit access to PII from	**Ref (c) (f)**
AC-20: Use of External Information Systems	Organizations can establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, (e.g., the agency accounting system) allowing authorized individuals to: a) access the information system from external information systems; and (b) process, store, or transmit organization-controlled information using external information systems.	**Ref (c) (f)**
AC-21: User-Based Collaboration and	Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually based restrictions, for PII.	**Ref (c) (f)**

Information Sharing		
AU-2: Auditable Events	Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.	**Ref (c) (f)**
AU-6: Audit Review Analysis, and Reporting	Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate ONHIR officials, and take necessary remedial actions to safeguard agency PII/S-PII from possible malicious security activities.	**Ref (c) (f)**
IA-2: Identification and Authentication (Organizational Users)	Users can be uniquely identified and authenticated before accessing PII. The strength requirement for the authentication mechanism depends on the impact level of the PII and the system as a whole. OMB M-07-16 specifies that Federal agencies must—allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access, and also must—use a _'time-out' function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity.	**Ref (c) (f)**
MP-2: Media Access	Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability.	**Ref (c) (f)**
MP-3: Media Marking	Organizations can label information system media and output containing PII to indicate how it should be distributed and handled. The organization could exempt specific types of media or output from labeling so long as it remains within a secure environment.	**Ref (c) (f)**
MP-4: Media Storage	Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures. One example is the use of storage encryption technologies to protect PII stored on removable media.	**Ref (c) (f)**
MP-5: Media Transport	Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas. Examples of protective safeguards are encrypting stored information and locking the media in a container	**Ref (c) (f)**
MP-6: Media Sanitization	Organizations can sanitize digital and non-digital media containing PII before it is disposed of or released for reuse. An example is degaussing a hard drive—applying a magnetic field to the drive to render it unusable.	**Ref (c) (f)**
PE-3: Physical Access Control	Organizations can enforce physical access authorizations at crucial organization-defined entry/exit points to the facility where the information system resides. Individual access is authorized before granting access to the facility and physical access audit logs and inventories are maintained. Documents containing PII are kept secure in locked steel cabinets in a locked room, and the agency secures keys, combinations, and other physical access devices.	**Ref (c) (f)**
SC-9: Transmission Confidentiality	Organizations can protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted.	**Ref (c) (f)**
SC-13: Cryptographic Protection	Organizations can implement organization-defined cryptographic protection of critical information system assets using encryption for their PII/S-PII data that are held in agency servers and IT components/endpoints as identified in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	**Ref (c) (f)**

SC-28: Protection of Information at Rest	Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information.	**Ref (c) (f)**
SI-4: Information System Monitoring	Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events. An example is the use of data loss prevention technologies.	**Ref (c) (f)**

Table 3: Critical PII Protection Controls

3. Legal Authority to Process PII

ONHIR is authorized to collect PII based on the following statute:

- **Privacy Act of 1974**: Allows for the collection of information about a U.S. Citizen that aligns with the mission objectives of federal agencies. ONHIR collects information about personnel relevant to client housing applications, land relocations, housing contracts, employment, payroll, vendor payments and other mission related tasks. *(ref j)*

4. ONHIR GSS System of Record Notice (SORN) Requirement

Disclosures outside the Office of Navajo and Hopi Indian Relocation may be made to (1) the

5 ONHIR GSS System Security Plan (SSP)

The ONHIR GSS SSP has been developed and is updated in accordance with (IAW) the RMF process.

6 ONHIR GSS Characterization of Information

The ONHIR GSS (IS) collects, uses, disseminates, or maintains PII information from two categories: prospective employees, current employees, terminated employees and Navajo and Hopi tribe's information which is submitted by the applicants.

Category of Individual	Type of PII Collected	Collection Source	PII ONHIR GSS Storage Locations

ONHIR	Financial account numbers, Employment		IBM i System AS400 Waldo server
Navajo and Hopi Applicants	Financial account numbers, Employment information, Social Security numbers, Truncated SSN (such as last four digits), Education information	Individual	IBM i System AS400 Waldo server
Vendors	Financial account numbers, Employment	Individual	IBM i System AS400 Waldo server

Table 4: ONHIR GSS Collected PII Information

7 Privacy Impact Analysis of Characterization of Information

Primary risks for the ONHIR GSS (IS) as it relates to the characterization of information are a data breach of the ONHIR GSS subsystem, loss of an ONHIR Endpoints (printers, laptops, workstations, mobile phone, etc.), and malicious (intentional or unintentional) activity from ONHIR personnel.

(a) Employment at ONHIR requires the collection of PII/S-PII to determine the prospective employee's eligibility for employment, performance monitoring of current employees, and completion of various work tasks.

(b) Acquiring housing and resolving land relocations through ONHIR requires the collection of PII/S-PII to determine the prospective client's eligibility to submit applications, appraisals, approvals and/or denial of applications, client data retention, client contracts, and completion of various related client-fulfillment tasks.

The collected PII and S-PII is stored on the agency server which is encrypted and is located on the IBM I System AS400 Waldo system. Some PII/S-PII may also be found on Microsoft Office 365 emails on ONHIR endpoints (workstations, laptops, cell phones), though the agency policy is to not store any data on endpoints. Subsequently, ONHIR GSS (IS) relies on the performance of the Executech team to properly implement the appropriate information security controls and disclose breaches to ONHIR management and affected teams.

PII and S-PII information that is stored on an ONHIR Endpoints (workstations, laptops, mobile phones, network printers, printers etc.) could become compromised if the asset is lost.

Malicious (intentional or unintentional) activity from ONHIR personnel could compromise PII information. Proper implementation of data encryption, least privilege principles, separation of duties, proper account management practices, user training and physical security are used to reduce the risk of PII/S-PII being compromised through this threat vector.

8 Individual Opportunities to Consent to Use or Decline Use of PII

Individuals have the right to decline usage of their PII in ONHIR operations, but it will restrict their ability to –

(a) gain or maintain employment at ONHIR

(b) apply for housing, sign contracts and participate in the government mandated housing program at ONHIR.

(c) Construction Contractors to build homes on the Navajo Indian Reservation. Required to be in good standing, pass Agency housing inspection in good standing, required to bring substandard work up-to passing inspection.

Individuals are notified that the information they are providing is subject to applicable statutes regarding PII and how the information will be used. ONHIR documentation that uses PII is marked and/or labeled with the appropriate statute (i.e., Privacy Act statement).

9 Retention of Collected PII

Formally requested and/or provided PII from individuals are retained according to the ONHIR's records management program.

10 ONHIR GSS ISSO PII Program Recommendations

- Utilize enhanced privacy controls as outlined in NIST SP 800-53 Revision 5, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- Conduct annual privacy control reviews to help ensure effectiveness of implemented privacy controls
- Continue to conduct annual privacy trainers for standard users and administrators
- Monitor the cloud provider's implementation of privacy controls
- Continue to make improvements to ONHIR GSS access controls processes.

11 Agency Contacts

Contact Point

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

Reviewing Official and Approving Official

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

System Manager for System or Application and IT Security Manager/Received this Document

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

Office Privacy Act Officer

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

C:\Users\Diane\Office of Navajo and Hopi Indian Relocation\Audit - Documents\IT Program\Tier III Program Management\General Support System\Privacy Documentation\Privacy