U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: NPS Human Resources (HR) Portal
Bureau/Office: National Park Service, Office of Human Resources
Date: November 13, 2023
Point of Contact:
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: 202-354-6925
Address: 12201 Sunrise Valley Drive, Reston VA 20192

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No

B. What is the purpose of the system?

The National Park Service (NPS) Human Resources (HR) Portal is a complete, end-to-end flow tracking system for HR activities, harassing conduct cases and workflow tracking. The system employs a common off the shelf software product to collect work requests from HR field offices and NPS employees for HR related questions. The Portal provides functions and menus to process work requests ranging from gathering information about personnel actions for current

NPS employees, position description changes, HR system access requests, NPS employees benefits and retirement requests, and harassing conduct cases. This Portal is assigned to the NPS General Support System (One GSS).

C. What is the legal authority?

5 U.S.C. 5101, et seq., Government Organization and Employees; 31 U.S.C. 3512, et seq., Executive Agency Accounting and Other Financial Management Reports and Plans; 31 U.S.C. 1101, et seq., the Budget and Fiscal, Budget, and Program Information; 5 CFR part 293, subpart B, Personnel Records Subject to the Privacy Act; 5 CFR part 297, Privacy Procedures for Personnel Records; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers; and Public Law 101-576 (Nov. 15, 1990), Chief Financial Officers (CFO) Act of 1990.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in the Governance, Risk, and Compliance platform?

☒ Yes
UII: 010-000001980
NPS Human Resources (HR) Portal Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If yes, provide a description.*
None			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes

Employee personnel records are covered under:

a. OPM/GOVT-1, General Personnel Records, 77 FR 79694 (December 11, 2012); modification published 80 FR 74815 (November 30, 2015)

b. INTERIOR/DOI-85 Payroll, Attendance, Retirement, and Leave Records, 83 FR 34156 (July 19, 2018)

Department of the Interior (DOI Active Directory credentials are covered under: INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/ EACS), 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021).

These SORNs may be viewed at the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes

☒ No
The system does not collect information from the public. Information is collected only from NPS employees using forms authorized by the Office of Personnel Management (OPM). OPM forms are published at https://www.opm.gov/forms/.

Section 2. Summary of System Data

A. **What PII will be collected? Indicate all that apply.**

☒ Name
☒ Gender
☒ Birth Date
☒ Marital Status
☒ Other Names Used
☒ Truncated SSN
☒ Place of Birth

☒ Security Clearance
☒ Spouse Information
☒ Emergency Contact
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other:

The system collects requests for HR service from employees. Users are provided free form text fields for entering the description of the request, actions taken, or communication between the employee and the HR office. Users upload associated OPM forms which may include the selected PII elements.

NPS users includes the HR staff and employees submitting the request who use their government issued Personal Identity Verification (PIV) card authenticated through the Enterprise Active Directory (AD) to access the Portal. The system collects the User Principal Name (UPN , user's name, official email address, government phone number, date of last login, and role or access level for authorized users.

B. **What is the source for the PII collected? Indicate all that apply.**

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other

C. **How will the information be collected? Indicate all that apply.**

☐ Paper Format
☐ Email
☐ Face-to-Face Contact

☒ Web site
☐ Fax
☒ Telephone Interview
☒ Information Shared Between Systems: Information from FPPS may be manually collected and entered into the Portal.
☒ Other:
Employees may call into a help desk for assistance and notes of the help desk interaction may be collected in the Portal.

D. **What is the intended use of the PII collected?**

The PII is required for processing personnel requests and to track program management activities.

E. **With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.**

☒ Within the Bureau/Office:
Information is shared within the NPS HR offices among authorized users to process personnel requests.

☒ Other Bureaus/Offices:
If a harassing conduct case moves to an official investigation, there is potential that data from the HR Portal would be manually entered into the DOI IMart system as determined by an Employee Relations Specialist. Personnel information may be shared with the DOI HR office.

☐ Other Federal Agencies

☐ Tribal, State or Local Agencies

☐ Contractor

☐ Other Third-Party Sources.

F. **Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?**

☒ Yes

NPS employees may decline to provide information when requesting HR services; however, this may result in inability of HR to provide the services or complete the request. PII is collected from NPS employees who must use the system to perform the duties of their employee position.

☐ No.

G. **What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

☒ Privacy Act Statement

A Privacy Act Statement is provided to individuals on all government forms that are potentially uploaded into the system.

☒ Privacy Notice

Privacy notice is provided through the publication of this privacy impact assessment, the Privacy Act Statement provided on government forms, and the published systems of records notices, INTERIOR/DOI-85: Payroll, Attendance, Retirement and Leave Records, INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and OPM/GOVT-1, General Personnel Records, which may be viewed at https://www.doi.gov/privacy/sorn.

☐ Other

☐ None

H. **How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).**

HR users may retrieve data by name or ticket number. Employees only have access to their data and are limited to what they have entered into their request or responses from HR on their requests.

I. **Will reports be produced on individuals?**

☐Yes

☒ No

No reports on individuals are produced. Authorized HR users have access to create reports on information collected concerning customer service metrics which do not include PII.

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

To the extent possible, information is collected from the individual and verified for accuracy by HR users.

The system also uses information from AD for account and access management. These records are generated by NPS or DOI (e.g., email address, UPN, first name and last name) during operational activities.

B. How will data be checked for completeness?

Data entered in the system is reviewed for accuracy and completeness by HR professionals to ensure the necessary information is included in order to complete the request. Employees also have access to their information and can request changes through the HR Portal.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Employees also have access to their information and can request changes through the HR Portal. Once the personnel action is completed and the ticket is closed, the data becomes historical data and associated forms are transferred to the electronic official personnel file.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

As supporting information for HR processes, data in the NPS HR Portal is subject to the Department Records Schedule (DRS) 1.2.0004 - Short-Term Human Resources Records (DAA-0048-2013- 0001-0004), which is approved by the National Archives and Records Administration (NARA). Records have a temporary disposition. Records are destroyed 3 years after they are created. Records may also be maintained under other long-term records schedule, such as DRS 1.2C, Retirement and Payroll Records Warranting Extended Preservation (DAA-0048-2013-0001-0008), which is approved by NARA. The system generally maintains temporary records, and retention periods vary based on the type of record under each item and the needs of the agency.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

The approved disposition methods include degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

The HR Portal is categorized as a moderate privacy risk and FISMA moderate system. All information acquisition and collection is done through the portal over encrypted communication channels that comply with the required federal standards and stored to minimize risk of data breaches while in transit. Information access and retrieval is done through electronic web forms over encrypted channels following defined application security roles and permissions to ensure proper distribution and disclosure of information guided by the principle of least privilege to minimize the risk of improper information disclosure. The protection and maintenance of information for recovery and backup purposes is done following NPS data center policy and process for backup and retention of information.

There are privacy risks related to hosting, processing, and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties.

The NPS HR Portal enables access for DOI authorized employees only through use of PIV Credentials and DOI AD using UPN or UserID attributes for authentication and role/permission management. DOI users must complete a background check, are required to sign the DOI's Rules of Behavior, and must complete security and privacy training prior to accessing a DOI computer system or network.

Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Device level encryption have been deployed to encrypt data at rest. Other security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes, or use of data. Federal employees and contractors are required to take annual mandated security, privacy, and records management as well as role-based training where applicable and sign the NPS Rules of Behavior prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that erroneous information may be collected. This risk is mitigated by allowing individuals to access and update only their records in the system. For user accounts, this risk is further mitigated by validating information against DOI AD, authentication results, and activity report and audit log content.

There is a risk that information in the system will be maintained longer than necessary to achieve the agency's mission or may be improperly disposed or destroyed. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Detailed procedures and automated scripts for data disposal/destruction will be developed and secured under change management. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA, SORNs, and Privacy Act Statements within the application.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes
The HR Portal is both relevant and necessary to provide employees and HR professionals access to an electronic means of creating and managing requests for HR services.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☐ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access will be restricted for all users. Each user will be assigned permissions, groups of permissions may be used to define a user's role. The permissions will determine what function the user may execute in the system and define what records the user can create, read, edit or delete.

System management staff may on occasion be required to view PII in the performance of their duties for troubleshooting or system maintenance purposes. Employee staff with privileged accounts will be subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☐ Yes

☒ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smartcards or Caller ID)?

☐ Yes

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes

The system is not intended for monitoring users; however, the system does identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about a user's visit, including UPN, as well as create/update/delete activities performed by users to support user access controls, troubleshooting, and incident response support.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

System logging records all attempted access to the system from users and internal processes, including monitoring, maintenance, and audit processes. Items logged include unique identifiers, timestamp, and event information attempts.

A system administrator may access platform configuration settings, and all platform configuration settings are monitored for changes. All system administrator accounts are monitored and routinely audited.

M. What controls will be used to prevent unauthorized monitoring?

Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring. Procedures are published for granting accounts, and privileged accounts are routinely audited for compliance. All access to the system, including the generation of reports, creates an audit log entry. Periodic audits will be performed by the Information Systems Security Officer (ISSO).

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training

☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Chief of HR Information Systems serves as the HR Portal Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in the system. The Information System Owner and ISSO are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within in the system, in consultation with NPS and DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The Human Resources Footprints Information System Owner and Human Resources Footprints ISSO are responsible for daily operational oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner and ISSO are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and appropriate NPS and DOI officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.