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: Human Resources Directorate Service Management (HRD SM)
Bureau/Office: Interior Business Center
Date: November 4, 2021
Point of Contact:
Name: Danna Mingo
Title: Associate Privacy Officer
Email: danna_mingo@ios.doi.gov
Phone: 202-208-3368
Address: 1849 C Street, NW Washington DC, 20240

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?

Human Resources Directorate Service Management (HRD SM) system is an IT Service Management (ITSM) commercial product with multiple modules and is a Cloud Software-as-a-Service solution hosted by the vendor ServiceNow, Inc. The Department of the Interior (DOI), Interior Business Center (IBC), Personnel and Payroll System Division (PPSD) will use ServiceNow (branded HRD SM) to input, track and manage change management documentation throughout the life cycle, including all Enhancement Requests (ENHC), Defects (DFCT) and Service Request (REQ), for the DOI Federal Personnel and Payroll System (FPPS), WebFPPS, WebTA

and Quicktime systems. The IBC is a Federal shared service provider and will process change requests for Federal employees on behalf of Federal agency customers.

PPSD is currently utilizing the Change Management module which has an automated workflow for the employees to document time worked, to attach analysis and test documentation, and to electronically record notes and other information. The HRD SM system will provide reports of the real-time status of the change for the DOI employees and managers to track the progress from the initial change request to the closeout of the documentation, and enable extensive editing to assure that tasks are accomplished timely and in the proper work sequence for meeting all change management requirements.

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), the 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 CSAM?

☒ Yes:

UII Code: 010999991141
Human Resources Directorate Service Management System 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	**None**	No	**N/A**

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

☒ Yes:

This system supports change management processes for DOI systems covered by the DOI-85, Payroll, Attendance, Retirement, and Leave Records, system of records notice, 83 FR 34156, July 19, 2018.

Federal agency customers retain ownership and control over their own records and are responsible for meeting requirements under the Privacy Act for the collection, maintenance and sharing of their agency records. Federal agency customers have their own system of records notices for their records hosted or processed by IBC. Individuals seeking information on their own records owned and maintained by external Federal agency customers should review the applicable system of records notice published by that Federal agency customer.

☐ No

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

☐ Yes:
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Social Security Number (SSN)
☒ Other: *Specify the PII collected.*

The system collects organization and Person Number which is a system generated number used to uniquely identify an individual in FPPS. This Person Number is used in lieu of the SSN

where possible to reduce privacy risk. Under certain circumstance, Federal employee SSN and name might be provided by employees who report issues with the relevant systems that HRD SM supports. Together with the system generated Person Number, PII might be used for the purpose of properly documenting changes made for the FPPS, WebTA, and Quicktime systems and enabling proper processing of personnel and payroll information for the affected individuals.

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
☒ Other:

PII is entered in HRD SM by an authorized IBC employee who may receive the information directly from a Federal employee via telephone call, email or fax to the Help Desk, or from the agency/bureau representative when they act on behalf of the employee to report a problem that affects a specific employee, or when a system changes or system problem occurs which may affect numerous individuals.

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

The PII collected and maintained in HRD SM is used to input, track, and document the system enhancements, service requests and defect changes that are requested by DOI personnel and are subsequently made to FPPS, WebTA, and Quicktime applications. PII is used to identify the individual record and initiate and manage the appropriate changes throughout the life cycle, including all ENHC, DFCTs, and REQs, through an automated workflow for employees to

document time worked, attach analysis and test documentation, and to electronically record notes and other information.

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

☒ Within the Bureau/Office:

PPSD uses HRD SM to input, track and manage change and change management documentation throughout the life cycles of the FPPS, WebFPPS, WebTA and Quicktime systems.

☒ Other Bureaus/Offices:

Authorized IBC employees have access to the PII and may enter PII and recorded issues into the system for a supported bureau or office. The information can be provided directly by a Federal employee who reports a problem or by the representatives of a DOI bureau/office on behalf of the employee reporting the problem.

☒ Other Federal Agencies:

DOI information in this system may be shared with other Federal agencies as authorized by law or the routine uses outlined in the DOI-85: Payroll, Attendance, Retirement, and Leave Records system of records notice. Representatives of Federal agency customers may act on behalf of the employees to report problems to the IBC. Reports may be shared, however, sensitive PII is scrubbed from the reports. Federal agency customers have access to the data for their own employees that is hosted or processed by IBC.

☐ Tribal, State or Local Agencies:

☒ Contractor:

Contractor personnel may be involved with design, development, testing and implementation as well as maintenance and providing general support.

☐ 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:

Employees voluntarily contact the Help Desk or human resources (HR) personnel to request

assistance and have the option of not providing information when requesting a change. However, failure to provide requested identifying information will result in delay of processing their request. The PII collected is solely used for change management purposes. Some of the data elements used to record requested changes are from FPPS. Federal employees are required to provide certain types of personal information, such as name and SSN, to Federal employers for human resource management purposes. Some of the PII would be entered into HRD SM to initiate change management processes. There are some alternative methods that employees may utilize to make changes to their records, such as accessing and updating their records in Employee Express or contacting their local HR office to make the requested change.

☐ No:

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

☒ Privacy Act Statement:

Privacy Act Statements are provided through various personnel and payroll forms and processes, as well as Employee Express and Quicktime.

☒ Privacy Notice:

Individuals are also provided notice on how their PII is managed during these personnel and payroll activities through the publication of this PIA and the DOI-85 SORN, which may be viewed on the DOI Privacy Program website at https://www.doi.gov/privacy/privacy-program.

☐ 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.).

Data is generally retrieved by ENHC, DFCT or REQ number, bureau, or organization, and not by PII. However, the HRD SM system has the capability to conduct any keyword search. HRD SM also allows task search by project.

I. Will reports be produced on individuals?

☐ Yes:

☒ No

Section 3. Attributes of System Data

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

Mandatory reviews of tasks and documentation are required to ensure all information is accurate. Information within HRD SM pertaining to system changes that do not affect a specific individual are verified through periodic reviews by IBC's HRD SM users by following standardized automated workflows processes. The HRD SM application requires multiple reviews be performed throughout the lifecycle of the change to ensure data accuracy.

B. How will data be checked for completeness?

HRD SM utilizes automated workflows to manage the entire change process. Mandatory reviews of tasks and documentation are required to ensure all information is complete. A final quality assurance review is performed by a HRD SM System Administrator before a change is completed electronically. The HRD SM application requires multiple reviews be performed throughout the lifecycle of the change to ensure the data is complete.

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

HRD SM data is separated into four categories: Current, Disapproved, Future and History. "Current" data contains up-to-date information. "Disapproved" data is updated at the time when the review is completed, and the data becomes disapproved. "Future" data would be updated to reflect its new status when any Change in queue get rechecked and assigned to a current release. "History" data remains unchanged after the closed-out. The HRD SM application requires multiple reviews be performed throughout the lifecycle of the change to ensure data is current.

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

DOI records in HRD SM and its change management documentation are covered under 3112 – Change and Configuration Management (CCM) Files detailed in the OS Records Manual, which has been approved the National Archives and Records Administration (NARA)(DAA-0048-2013-0001-0013). The disposition is temporary. Cut off when type/device or system terminates, is superseded or obsolete. Destroy no later than 3 years after cutoff. Federal agency customers are the owners of their own records and are responsible for identifying associated record retention schedules for their records and ensuring they are properly managed under the Federal Records Act.

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

When the retention period described above has been met, the program office will complete a DI-1941 for the records eligible for disposal. Once approved, the files can be deleted from the system.

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.

There is a moderate risk to individual privacy due to the sensitive PII used by HRD SM. Accordingly, DOI has defined and implemented a series of administrative, technical, and physical mitigation measures to mitigate these risks. There is a risk that individuals do not have notice that their PII will be collected or how it will be used or stored. HRD SM supports Privacy Act systems and is used to input, track, and manage the lifecycle change management documentation for DOI's FPPS, WebFPPS, WebTA and Quicktime systems.

In most cases, employees contact DOI officials to initiate a change request. PII is used by HRD SM to provide service to internal and external customers, and is only used for the relevant purposes, through the notice and consent processes, as stated in the related published SORNs and PIAs covering records in these systems. There is a risk that individuals may gain unauthorized access to the information in the system. This risk is mitigated by ensuring effective access controls are implemented, and only authorized personnel are granted access to the records in the system and agree to adhere to the DOI Rules of Behavior. Access to the DOI network requires two-factor authentication. PII that HRD SM use can only be shared and disclosed internally by DOI personnel to carry out their essential job duties. It can only be accessed by authorized IBC users who are granted access to the system based on need-to-know and least-privilege principles, as defined by the management.

The access right is subjected to the review by the authorities on an ongoing basis. IBC reviews each user account annually to ensure the users are in proper group and have the appropriate assigned roles within HRD SM in compliance with the appropriate DOI use policy. HRD SM also maintains an audit trail of activity that includes the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The users must be authenticated to validate the user authorization before access is granted.

There is a risk that some data may not be appropriate to store in a vendor system or that the vendor may not handle and or store information appropriately according DOI's records policy. The vendor's ServiceNow Federal Risk and Authorization Management Program (FedRAMP) approved environment is physically separated and the ServiceNow platform has received

FedRAMP certification from the U.S. Government. This certifies that the ServiceNow government community cloud has passed the Federal risk management process defining standard security requirements. The ServiceNow cloud offering has logical separation in place, which warrants that DOI provisions its own database instance. The physical controls are in effect to limit access to the protected Data Center. Vendor personnel can access the system administrative data for troubleshooting purposes only through approved Federal roles, and this troubleshooting is monitored and recorded by the system logs. Appropriate Privacy Act clauses were inserted into the vendor contract for this system.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. To enforce the administrative controls and ensure the effectiveness of the security and privacy controls, the DOI requires all the employees and contractors to complete onboarding and annual security and privacy awareness training. The IBC personnel who are authorized to manage, use, or operate the system information are required to take additional role-based training and sign DOI Rules of Behavior. In addition, IBC conducts internal reviews to ensure compliance with the Privacy Act and related policy.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Data collected, used and maintained is limited to the minimal amount needed to support the change management process. Records in HRD SM are retained to support agency personnel and payroll operations in accordance with approved records retention schedules and will be properly disposed in accordance with the standard DOI method and NARA procedure.

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 use of data is relevant and necessary to document changes requested for and made to FPPS,WebFPPS, WebTA, and Quicktime.

☐ 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?

N/A. No new data is derived.

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*

DOI authorized users and contractors can make updates to data for tasks they are assigned to and per their role authorized in the system. The DOI System Administrators can make changes to data when required, as well as changes to the application. Under emergencies or exceptional circumstances, per pre-approval by the program manager according to the Change Control Procedure, the developer within HRD can be the approved personnel authorized to make corrections to certain data per the service requested.

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

The managers of the data owners determine who needs access to the data and the System Administrator assigns access to the individual on a "need-to-know" basis and least privilege principles. Access criteria, procedures, controls, and responsibilities are built into the application.

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.

Yes, contractor personnel may be involved with design, development, testing and implementation as well as maintenance and general support. Appropriate security and privacy clauses are contained in the contracts, such as the Privacy Act Notification (FAR 1452.224-1 and FAR 52.224-01).

☐ 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.

☒ No

The HRD SM does not identity, locate or monitor individuals, however, the system does utilize audit features that track and monitor user activities for security purposes.

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

HRD SM has audit features and additional controls that monitor authorized user activity. The information collected from audit trails contain the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls.

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

IBC fully complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. The use of DOI IT systems, including HRD SM, is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

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 IBC Office of Human Resources, Associate Director, Human Resources Directorate serves as the HRD SM Information System Owner and the official responsible for oversight and management of the HRD SM security and privacy controls and the protection of agency information processed and stored by the HRD SM system. This includes ensuring the hosting vendor and their employees maintain the highest level of standards for protecting the privacy rights of employees. The Information System Owner and the Information System Security Officer, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in HRD SM, as well as protecting the privacy rights of employees for the information they collect, maintain, and use in the system, meeting the requirements of the Privacy Act, and responding to complaints in consultation with DOI privacy officials. Federal agency customer data is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting requirements of the Privacy Act.

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 HRD SM Information System Owner is responsible for oversight and management of the HRD SM security and privacy controls, and for ensuring to the greatest possible extent that

agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII or customer agency data is reported to the customer agency and DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures.