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 templateto assess third-party websites or applications.

Name of Project: Human Resources Management Suite (HRMS)
Bureau/Office: Interior Business Center
Date: September 29, 2021
Point of Contact
Name: Danna Mingo
Title: OS Departmental Offices Associate Privacy Officer
Email: danna_mingo@ios.doi.gov
Phone: (202) 441-5504
Address: 1849 C Street NW, Room 7112, 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?

The Department of the Interior (DOI) Human Resource Management Suite (HRMS) is a human resource management system that consists of a suite of HRMS Modules, a System Integration Framework (HRMS SIF), and a set of standardized integration connectors that provide functionality for the life cycle management of human resource functions. HRMS is operated and maintained by the DOI Interior Business Center (IBC) and provides single-point data capture, with real-time sharing of data with other systems needing the data.

HRMS significantly improves the Federal Government's business processes for management of human resources functions through seamless, end-to-end, real-time integration between HR and other systems. The standardized integration connections provide integration between the HRMS modules and the IBC Federal Personnel and Payroll System (FPPS) and eRecruitment solutions allow HRMS to integrate with solutions from a variety of vendors and Federal human resources Shared Service Centers (SSCs).

HRMS contains several modules:

- HRMS Module: Affiliate Workforce Transformation Tracking System (AWTS). The AWTS module provides the functionality to allow Contracting Officer's Representatives (CORs) the ability to record and track information about contractors.

- HRMS Module: Workforce Transformation Tracking System (WTTS). The WTTS module has been acquired by IBC as Government Off-the-Shelf (GOTS) software from the National Aeronautics and Space Administration (NASA). IBC "federalized" WTTS to make it generic for use by any Federal agency. The WTTS module allows managers and personnel specialists to project gains, transfers, and losses of federal staff. It also allows personnel specialists to develop checklists for entrance on duty. This information is used for planning purposes by executives, security, and facilities staff. When actual gains, transfers, or losses are occurring, the planning information previously entered into WTTS is sent real-time to FPPS to initiate personnel actions.

- HRMS Module: Entrance on Duty System (EODS). EODS has been acquired by IBC as GOTS software from NASA. IBC "federalized" EODS to make it generic for use by any Federal agency. EODS provides online forms for new employees to complete information required on entrance to duty. These forms are pre-populated with information captured by upstream business processes and can be fed to electronic Official Personnel Folder (eOPF).

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 Pub. L. No. 101-576 (Nov. 15, 1990), the Chief Financial Officers (CFO) Act of 1990; 40 U.S.C. 1401 et seq, Clinger-Cohen Act of 1996; E-Government Act of 2002; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service", April 27, 2011; Office of Management and Budget (OMB) and the United States Office of Personnel Management (OPM) Human Resources Line-Of-Business initiative to migrate United States Government agencies to Federal Human Resources (HR) Shared Service Centers (SSC).

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:

E. Is this information system registered in CSAM?

☒ Yes:

010-999991217; Human Resources Management Suite 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:

Records maintained in this system are covered under DOI-85, Payroll, Attendance, Retirement, and Leave Records. Personnel records are also maintained under government-wide system of records notices OPM/GOVT-1, General Personnel Records, and OPM/GOVT-5, Recruiting, Examining, and Placement Records. These notices may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

Federal agency customers retain ownership and control over their own records and are responsible for meeting the requirements under the Privacy Act for the collection, maintenance and sharing of their agency records. Federal agency customers have published their own system of records notices for their records hosted or processed by IBC. Individuals seeking information on their 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: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Other Names Used
☒ Disability Information
☒ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Other:

☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Personal Email Address
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Personal Cell Telephone Number

Employee drug test information, employee employment information, Employee Common Identifier, Home Address, Age, Employee Benefit Information (Health/Life Insurance, Thrift Savings Plan), Personal Contact information (Next of Kin, Beneficiaries), Payroll and Tax Information, and other information related to process personnel actions.

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 *Describe*

HRMS receives information from two subscribing e-Systems, as a way of integration with eRecruitment solutions: OPM's USA Staffing System and Monster Hiring Management Enterprise System. The information collected consists of information from job applicants, which is used by IBC and Federal customer agencies to manage new employees recruiting process. HRMS receives information via FIPS 140-2 compliant, encrypted point-to-point data transmission. Data is also obtained from DataMart (DM), an FPPS subsystem that loads the most current Employee data using mainframe flat files created by FPPS.

☐ Other:

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

Personally Identifiable Information (PII) is used to process personnel actions and support the full life cycle management of human resource functions and the normal operation activities for Federal Human Resources Management for Federal employees, and Federal Acquisitions activities for management of Federal contracts.

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

☒ Within the Bureau/Office:

IBC personnel process the data in the HRMS system for human resources, payroll, and employee benefits.

☒ Other Bureaus/Offices:

Some DOI Bureau/Office data is shared with the DOI Bureaus/Offices for their own human resources activities.

☒ Other Federal Agencies:

Federal agency customers will have access to the data for their own employees and contractors. Information may be shared with other Federal agencies as authorized as a routine use outlined in the DOI-85, Payroll, Attendance, Retirement, and Leave Records SORN, which may be viewed at: https://www.doi.gov/privacy/doi-notices, and OPM government-wide notices, which may be viewed at https://www.doi.gov/privacy/sorn.

☐ Tribal, State or Local Agencies:

☒ Contractor:

Data will be shared with DOI contractors who are involved in the design and development of the HRMS system, or will be involved with maintenance of the system, and who support the human resources functions and processes managed by the HRMS.

☒ Other Third Party Sources:

Information processed through the HRMS may be shared with third parties as authorized as a routine use outlined in the DOI-85, Payroll, Attendance, Retirement, and Leave Records SORN, which may be viewed at: https://www.doi.gov/privacy/doi-notices, and OPM government-wide notices, which may be viewed at https://www.doi.gov/privacy/sorn.

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

☒ Yes:

Information is collected as a condition of employment, and the provision of personal information is provided voluntarily. Individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII during the application and onboarding process. Various official forms contain Privacy Act Statements that inform individuals of the uses of their PII and the consequences of not providing requested information.

☐ No:

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

☒ Privacy Act Statement:

Information is collected during the application and onboarding process as a condition of employment. Various Federal human resources standard forms contain Privacy Act Statements that inform individuals of the uses of their PII and the consequences of not providing requested information. For example, Optional Form 306 Declaration of Federal Employment contains a Privacy Act Statement: https://www.opm.gov/forms/pdf_fill/of0306.pdf.

On-boarding employees who submit information via the Entrance on Duty System (EODS), the only system that is accessed directly by the individuals, are provided with two warning screens.

The first screen is entitled "Security Caution – Protecting Personal Identifiable Information (PII)". The screen provides information on the responsibility of the user to take appropriate caution in protecting their PII.

The second screen is entitled Privacy Policy. The Privacy Policy screen notifies the On-boarding Employee that "Access to this information is limited to only those who have a need for the information in the performance of their official duties".

☒ Privacy Notice:

Privacy notice is also provided through the publication of this privacy impact assessment and the published DOI-85, and OPM government-wide SORNs that cover these records.

☒ Other:

Users are provided with a privacy and security warning banner when accessing the WTTS and EODS. HRMS modules contain a Privacy Policy that warns users of the privacy requirements, their consent to monitoring, and references the DOI Privacy Act regulations and applicable Privacy Act penalties.

☐ None

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

Records may be retrieved by employee name, WTTS ID, FPPS Transaction Number, Employee Common Identifier, Organization Code, EOD Date, Position Title, Announcement Type, Appointment Type, Pay Plan, Occ Series 1 Code, Grade, Selected Series, Supervisor/Hiring Official ID, Employee Type, Announcement Number, Certificate Number 1, Last Modified Date, Fiscal Year, Declination Type, Organization Code, Declination Date.

A variety of reports are available through WTTS and are based upon types of activities which occur in a given interval of time.

I. Will reports be produced on individuals?

☒ Yes:

Reports will be produced on individuals for the purpose of completing standard Human Resource Management activities such as On-boarding, Benefits, and other functions.

☐ No

Section 3. Attributes of System Data

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

The source data is validated for accuracy before it is imported into HRMS. HRMS maintains the data accuracy via custom rules that perform data validation routines prior to accepting information from external systems. The HRMS system also utilizes application-level input validation with multiple data checks that inspects user input for expected results prior to accepting the information provided by the end user.

B. How will data be checked for completeness?

The source data is validated for completeness before it is imported into HRMS. HRMS maintains the data accuracy and completeness via custom rules that perform data validation routines prior to accepting information from external systems. The HRMS system also utilizes application-level input validation with multiple data checks that inspects user input for expected results prior to accepting the information provided by the end user.

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

The FPPS Daily Update file is imported from FPPS on a daily basis, and this keeps the data current. Employee data is also daily updated by DataMart using files created by FPPS.

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 will be maintained under the DOI Departmental Record Schedule (DRS) 1.1 Short Term Administrative Records, which was approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0001-0001). The records disposition is temporary, and the records will be cut off at the end of the fiscal year in which the record is created. The contractor data will be cut off when the contractor separates or is no longer employed by the agency.

Other HRMS records are covered by DRS 2.1, Short Term Human Resources Records (DAA-0048-2013-0001-0004). The records disposition is temporary, the records will be cut off at the end of the fiscal year in which the record is created. The contractor data will be cut off when the contractor separates or is no longer employed by the agency. Records must be retained 3 years after cut-off.

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?

Records are disposed of in accordance with the applicable records retention schedules for each bureau or office, Departmental policy and NARA guidelines. Paper records are shredded and records contained on electronic media are degaussed or erased in accordance with Departmental Policy. Contractor data will be purged via use of an automated script which will drop records whose date is greater than three years past the Contractor Record Termination Date.

Federal agency customers are the owners of their own records and are responsible for the disposition of their records in accordance with the Federal Records Act.

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.

Within HRMS, the EOD collects PII directly from the individuals. The other data are imported from the two e-recruitment solution systems. There is a privacy risk from the PII collected and processed by HRMS, which is mitigated through administrative, physical and technical controls that have been put into place to protect the confidentiality, integrity and availability of HRMS data. Individuals are notified of the privacy practices through published government-wide and DOI SORNs, Privacy Act Statements, Privacy Policy and Notices, and the user banners posted on the client facing website and applications.

HRMS is rated as a FISMA moderate system that requires management, operational, and technical controls established by National Institute of Standards and Technology (NIST) SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information. PII from HRMS users is collected via encrypted internet connections. All internet connections with subscribing systems are NIST FIPS 140-2 compliant. Information is used, retained, and processed by authorized personnel based on need-to-know and least privilege principles. HRMS user account creation and authorization requires supervisor's signature and the user's signed acceptance of the HRMS System Rules of Behavior. The record retention schedule and disposal procedures are clearly defined and followed, which further mitigates the relevant privacy risks from the maintenance and potential mishandling of the PII data.

DOI mandates that all Federal employees and contractors complete initial and annual information security and privacy training; tailored role-based privacy and security training is also required for personnel with privacy or security responsibilities. The resulting high awareness provides an enhanced level of assurance on the life cycle management of the PII data.

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:

HRMS is a human resources management system, and the use of personal data is both relevant and necessary to the use of the system.

☐ 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. No new data is being created.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated.

Data is being consolidated from several existing systems. Controls are in place to protect the data from unauthorized access or use in accordance with NIST SP 800-53. Access to the data is authenticated and controlled. Access is granted pursuant to a role-based access model that only allows user access to specific information, functions or reports within the system.

☐ 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

EODS Users can input and view their own personal information, but cannot access the information of others. EODS Users update information associated with their hiring and employee benefits. WTTS Users are HR professionals and use WTTS data in the hiring process. WTTS User will access the personal information of job applicants in keeping with their professional duties.

AWTS users are contractors who can input and view their own personal information but cannot access the information of others. Contracting Officers and Contracting Officer Representatives may access information concerning contracts for which they are responsible, to include the information of contractors furnished under those same contracts.

☒ Contractors

Contractors may be involved in the design and development of the HRMS system, or with maintenance of the system, and may support the human resources functions and processes managed by the HRMS.

☒ Developers

Developers can access Development and Test environments, but do not have access to Production environments.

☒ System Administrator

System Administrators have wide-ranging access to the System in keeping with their duties. The activities of System Administrators are logged and audited.

☐ Other:

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

Access to the data is determined by the requirements associated with their professional responsibilities on need-to-know basis. Access to the data is based upon the concept of Least Privilege and is allowed only in keeping with professional responsibilities. Specific criteria, procedures, controls, and responsibilities regarding access are documented in the HRMS System Security and Privacy Plan.

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.

Contractors participate in the design and development of the system and are involved with maintenance of the system. Privacy Act contract clauses are included in the contract.

☐ 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.

HRMS System Audit Logs are produced to identify and monitor the actions of system users.

☐ No

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

Information such as username, logon date and time, number of failed logon attempts, and changes to records is captured in the HRMS System Audit Logs.

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

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include 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. 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.

(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.

(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 Associate Director, Human Resources Directorate, Interior Business Center serves as the HRMS Information System Owner and the official responsible for oversight and management of the HRMS security controls and the protection of customer agency information processed and stored by the HRMS system. The Information System Owner and 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. The Privacy Act system manager is responsible for ensuring the requirements of the Privacy Act are met, including the publication of a notice, and making decisions on Privacy Act requests for notification, access, and amendments, 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 the 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 HRMS Information System Owner and Information System Security Officer are responsible for oversight and management of the HRMS security and privacy controls, and for ensuring to the greatest possible extent that HRMS data is properly managed and that all access to customer agency and agency data has been granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of HRMS data or customer agency is reported to DOI-CIRC, and the customer agency, within 1-hour of discovery in accordance with Federal policy and established DOI procedures.