

Department of the Interior
Privacy Impact Assessment

February 19, 2010

Name of Project: Human Resources Management System (HRMS)

Bureau: National Business Center (NBC)

Project's Unique ID: 010-00-01-07-01-1226-24

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- NBC Chief Information Security Officer (CISO)
- NBC Privacy Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

A. CONTACT INFORMATION:

Departmental Privacy Office

Office of the Chief Information Officer

U.S. Department of the Interior

202-208-1605

DOI_Privacy@ios.doi.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. The Human Resources Management System (HRMS) contains the following personal information about individuals:

Note: The information listed below does not constitute an exhaustive list of all information pertaining to individuals contained in the system. Additional categories of information may be added or removed as HRMS continues in the operations and maintenance phase of its lifecycle.

- Social Security Numbers
- Name
- Employee Common Identifier
- Home Address
- Phone Numbers
- Date of Birth
- Age
- Emergency Contact Information
- Education

- Ethnicity and Race
- Disability Code
- Employee Benefits Information (Health/Life Insurance, Thrift Savings Plan)
- Banking Information (Direct Deposit Account Information)
- Personal Contact Information (Next of Kin, Beneficiaries)
- Payroll and Tax Information

- a. Is this information identifiable to the individual¹?** (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, Sections C through F can be marked not applicable).

Yes. The information is identifiable to the individual.

- b. Is the information about individual members of the public?** (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

The information pertains to individual members of the public who are Federal employees and Contract employees. Therefore, this PIA is included as part of the DOI IT Security C&A process and the OMB Exhibit 300.

- c. Is the information about employees?** (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes. The information in the HRMS system is about employees of the Federal Government. Therefore, this PIA is included as part of the DOI IT Security C&A process and the OMB Exhibit 300.

2) What is the purpose of the system/application?

The Human Resources Management System (HRMS) will enable the National Business Center (NBC) Human Resources Line of Business (HRLOB) to provide customer agencies with access to a variety of automated human resource solutions. HRMS is comprised of a suite of modules called the HRMS HR Management Suite (HRMS), an HR System Integration Framework (HRSIF) and a set of standardized e-Government systems integration sockets which will support agencies in key e-government initiatives (eRecruitment, eClearance, eLearning, eTravel, eTraining, eOPF (Electronic Official Personnel Folder), and EHRI (Enterprise Human Resources Integration)).

HRMS core functionality will include:

- Automation of pre-vacancy announcement business processes
- On-Boarding management
- Entrance on Duty data collection and processing
- Employee Provisioning
- Off-Boarding management
- Linkage to HSPD-12

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

- Event notifications and integration with customer solutions
- Training management through:
 - Competency Management
 - Learning Management
 - Performance Management

An initiative of the NBC Human Resources Line of Business, HRMS will integrate with all eGov initiatives and provide "Best of Breed" auxiliary Human Resources systems, i.e. staffing, learning management, classification, etc. HRMS will provide the ability to enter data once and populate information changes across multiple systems.

The HR Management Suite (HRMS) is comprised of three modules which are directly accessed by users. These modules are the Talent Management System (TMS), the Workforce Transformation and Tracking System (WTTS), and the Entrance on Duty System (EODS). TMS will provide competency management, performance management, and learning management. WTTS is used by Human Resources and Management personnel to enter projected and actual hires, transfers, and losses of Federal employees. WTTS will also be used to collect information for the issuance of HSPD-12 identification cards to Contract employees and will also provide a single, automated system with which to manage the off-boarding of DOI Contractor personnel. Future versions could include volunteer staff. EODS is used by newly-hired Federal employees to electronically capture a variety of data including tax information, health insurance, and life insurance.

2a) What Minor Applications are hosted by this system?

MINOR APPLICATION NAME	PURPOSE	PII? (Yes/No)
N/A		

3) What legal authority authorizes the purchase or development of this system/application?

The legal authority for the HRMS application is:

- 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)s.

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

Individuals covered in the HRMS application are Federal employees and Contractor employees. Future versions could include volunteer staff.

2) What are the sources of the information in the system?

HRMS is an enterprise service application that receives and transmits data to and from external information systems. Information is exchanged between HRMS and external systems using secure sockets.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The source of information is from the individual and information exchanged with partner systems interfacing with HRMS.

External partner systems which interface with HRMS are:

Federal Personnel Payroll System (FPPS): FPPS is a mainframe-based, real-time personnel and payroll system. FPPS exchanges information with HRMS when an employee's payroll record is created or updated in FPPS.

Automated Staffing Solutions: eRecruitment-related Automated Staffing solutions are provided by two vendors, e.g.: Monster Hiring Manager, and OPM USA Staffing. The Automated Staffing solutions receive position vacancy notices and publish them as advertisements for public review. HRMS will exchange information with the Automated Staffing solutions using a single XML interface standard.

Companies who provide contractor employees to the Department may provide the needed information on behalf of their employees, either at the initiation of the hiring process or subsequently.

b. What Federal agencies are providing data for use in the system?

The following organizations initially use the HRMS application to assist with the management of information:

Department of the Interior (DOI),
Fish and Wildlife Service (FWS)
Office of the Secretary (OS)
Bureau of Indian Affairs (BIA)
National Park Service (NPS)
Minerals Management Service (MMS)

Additionally, the HRMS system could be used by all NBC customers of the Federal Personnel Payroll System (FPPS).

c. What Tribal, State and local agencies are providing data for use in the system?

N/A

d. From what other third party sources will data be collected?

At this time, HRMS will not collect information from any other source. This document will be updated as new interfaces are added, and the scope of HRMS expands.

e. What information will be collected from the employee and the public?

Information will be collected directly from Federal employees in the HRMS Entrance on Duty System (EODS). EODS users populate information in electronic forms, entering personal information about themselves, decisions on benefit packages, insurance beneficiaries, etc.

Information on Contractor employees will be collected using the Workforce Transformation Tracking System (WTTS). Contractor employee information will be provided by the contractor's employer. Data will be entered into WTTS initially, but future releases could

allow the contractor to fill out information through the EODS. Future releases could also include volunteer staff.

3) Accuracy, Timeliness, and Reliability

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

The HRMS XML gateway is configured with custom rules that perform data validation routines prior to accepting information from external systems. The HRMS system utilizes application level input validation 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 HRMS XML gateway is configured with custom rules that perform data validation routines prior to accepting information from external systems. WTTTS and EODS both have application level input validation that inspects user input for expected results prior to accepting the information provided by the end user.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Yes, the data is current. The system will update data automatically between systems.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, the data elements are described in detail and documented in the HRMS Data Dictionary.

D. ATTRIBUTES OF THE DATA:

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

The use of the data is both relevant and necessary to ensure consistent information exists across partner systems.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

3) Will the new data be placed in the individual's record?

Not Applicable.

4) Can the system make determinations about employees/public that would not be possible without the new data?

Not Applicable.

5) How will the new data be verified for relevance and accuracy?

Not Applicable.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Data is being consolidated. Controls are in place to protect the data from unauthorized access or use in accordance with NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems".

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Controls are in place to protect the data and prevent unauthorized access. Access to the data is via user id and password via RACF authentication.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

A personal identifier will be used to retrieve the data. Data can be retrieved by name. The Mobility Module for WTTS will be able to retrieve data associated with a known Social Security Number. Social Security Number (SSN) must be used for identification of job applicants in the initial stages of the hiring process. An Alternate Identification Code will be generated at a later point in the hiring process.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

WTTS will produce statistical reports to assist in forecasting hires, transfers, and losses of federal staff. WTTS will produce reports to assist in the identification and on-and-off boarding management of Contract employees. Reports identifying actual hires, transfers, and losses of federal staff will also be produced. Only Human Resources personnel, Contracting Officers, Contracting Officers Technical Representatives, facilities and security staff, and management will have access to these reports.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Prospective or current Federal Individuals consent to providing personal information in EODS through the use of an online consent form that individuals agree to before submitting information. Contractor employees provide their employee information to their contractor companies, who in turn will submit the information to WTTS. While a consent form is used for Federal employees, provision of the information by both Federal employees and contractor employees is a requirement to fulfill the hiring process for new hires and receive HSPD-12 badges for all Federal workers and contractors.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system is operated in only one site, the NBC Denver Data Center.

2) What are the retention periods of data in this system?

Data is retained according to NARA-approved records schedules established by the Office of the Secretary for Department of the Interior data. The Electronic Official Personnel File, with which HRMS will ultimately interface, is the System of Record, and mandates retention of records for 65 years after separation.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

At the end of the retention period data will be disposed of in accordance with Privacy Act Policy – 383 DM 8.8 and NIST SP 800-53. The procedures are documented in the HRMS System Security Plan.

Reports generated from the system are retained according to NARA-approved records schedules established by the Office of the Secretary for Department of the Interior.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

Not Applicable.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

7) What kinds of information are collected as a function of the monitoring of individuals?

N/A

8) What controls will be used to prevent unauthorized monitoring?

N/A

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

In addition to being covered by OPM/GOVT-1, as cited below, records maintained in this system for agencies other than the Department of the Interior are covered by their own Privacy Act systems of records notices.

The Privacy Act system of records notices that cover this system for the Department of the Interior are:

- OPM/GOVT-1 (government-wide system for general personnel records maintained by the Office of Personnel Management)
- OPM/GOVT-5: Recruiting, Examining, and Placement Records for the applicants.
- Interior Personnel Records – Interior, DOI-79 [for Department of the Interior records]
- Payroll, Attendance, Retirement, and Leave Records – Interior, Office of the Secretary – DOI 85 [for Department of the Interior records]
- HSPD 12: Identity Management System and Personnel Security Files – Interior

- System of Records Notice DOI—45 [for Department of the Interior records]

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

The system is being modified to include the collection of Contractor employee data. The Privacy Act system of records notice does not require amendment or revision because the above System of Records Notice DOI—45, HSPD-12 Identity Management System and Personnel Security Files, covers the contemplated changes including collection and use of contractor employee data.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Only Contracting Officers, Contracting Officers' Technical Representatives, HSPD-12 Sponsors, facilities and security staff, Human Resources personnel and hiring managers will have access to information in HRMS WTTS and EODS. New Federal hires will have access to only their own information in EODS.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

User access to the data is determined by the requirements associated with their professional responsibilities. Access to the data is based upon the concept of Least Privilege and is allowed only in keeping with professional responsibilities. Criteria, procedures, controls, and responsibilities regarding access are documented in the HRMS System Security Plan.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Users will not have access to all data on the system. User access to data will be restricted by Department, Bureau, Sub bureau, Organization, and Role.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

HRMS system will log user activity to provide non-repudiation of data access. Database Administrators, Application Security Administrators, and others with privileged access to HRMS information agree to specific Rules of Behavior, and agree to follow NBC policy pertaining to the protection of sensitive government information.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Contractors will participate in the design and development of the system and will be involved with maintenance of the system. FAR Privacy Act clauses were included in the contract.

6) Do other systems share data or have access to the data in the system? If yes, explain.

Yes. Information is replicated to partner systems that subscribe to HRMS. The most recent information is updated on external partner systems so that information does not require updating on multiple systems.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Ultimately the Privacy Officer and the Information System Security Officer (ISSO) of external systems are responsible for protecting the privacy rights of those affected.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

No. Data contained in this system will be shared with other agencies only to the extent authorized (in routine uses) by applicable Privacy Act Systems of Records Notices.

9) How will the data be used by the other agency?

Data shared with other agencies when authorized by routine uses in applicable Privacy Act Systems of Records Notices will be used in accordance with the respective mandates of the applicable routine uses.

10) Who is responsible for assuring proper use of the data?

The HRMS Program Manager, the Information System Security Officer (ISSO), and users of the system are responsible for assuring proper use of the data. All users of the system sign accountability forms in the form of Rules of Behavior when they are granted access to the system and the information it processes.