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: Hiring Management Enterprise System (HMES)
Bureau/Office: Interior Business Center
Date: April 10, 2018
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: 202-208-1605
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: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Hiring Management Enterprise System (HMES) is a Major Application that provides Human Resources (HR) management and staffing solutions. HMES is a web-based system owned and operated by Monster Government Solutions (MGS). The U.S. Department of the Interior (DOI) Interior Business Center (IBC) has a contract with MGS and serves as a value-added reseller of subscriptions for the HMES to Federal agency customers. For Fiscal Year 2018, HMES subscriptions will be purchased by twenty-two IBC customer agencies and six DOI bureaus. The remaining customer agencies consist of

other Federal Departments and agencies. The HMES customer agencies purchase system subscriptions for human capital management, workforce development, and to find and hire candidates for employment.

The overall purpose of the HMES is to improve the hiring management process for DOI HR specialists. HMES does this through several functions, including posting and managing vacancies, displaying those vacancies to potential employees via the Internet (USA Jobs.gov), collecting and processing employment application and applicant personal data (i.e., contact information), and ranking applicants' qualifications based on such data. In addition, the system provides email correspondence functionality so that employment candidates once enrolled can be notified of the respective hiring decisions and interested parties can be notified of future job vacancies. The records are used when considering individuals who have applied for positions in the Federal service by making determinations of qualifications for positions applied for, and to rate and rank applicants applying for the same or similar positions. They are also used to refer candidates to federal agencies for employment consideration, including appointment, transfer, reinstatement, reassignment, or promotion. HMES relies on a computer network, including several hardware and software components to function.

All data used by the HMES is stored in electronic database format on database servers. This database is then accessed and processed by software components, each of which have their own purpose. The three HMES components are Hiring Management, Analytics, and Competency Management.

Hiring Management: The Hiring Management Component consists of many sub-components: Applicant Tracking System, Seeker, Scheduler, Fax Integration, Web Services, Nightly Service, and the database components.

Analytics Component: Analytics provides the ability to analyze, export and manipulate HMES data. The core product system provides access to pre-defined reports (including Office of Personnel and Management & Equal Employment Opportunity Commission reports), dashboard functionality and ad-hoc reporting capability. The custom reporting solution supports highly complex business logic and the ability to customize specific data relationships to meet DOI's unique environment from within the Human Capital Management and from other systems.

The Analytics Component retrieves employment-related data by establishing a JDBC database connection via TCP/IP to the group of Oracle relational database servers which store and manage the database files for HMES. This component is accessed and used by customer agency internal human resource management staff. Access to the Analytics Component is provided to DOI internal staff via the public internet.

Competency Management: Provides the ability to create and manage competencies/competency models. Users in the Competency Management product will be able to physically associate the questions initially created in the HMES Question Library to the competencies that were built in Competency Builder. The questions will continue to be entered and managed in HMES.

The data collected, used, maintained and related within MGS Competency Management will properly place competencies at the center of Talent Management in the MGS environment and provide the tools

and data that will enable DOI to incorporate competencies into their strategic and operational processes.

C. What is the legal authority?

5 U.S.C. 1302-Regulations, 3109- employment of experts and consultants; temporary or intermittent, 3301-Civil service; general, 3302-Competitive service, 3304-Competitive service; examinations, 3305-Competitive service; examinations; when held, 3306-Planning and solicitation requirements, 3307-Competitive service; maximum-age entrance requirements; exceptions, 309-Application for license, 3313-Competitive service; registers of eligibles, 3317-Competitive service; certification from registers, 3318-Competitive service; selection from certificates, 3319-Alternative ranking and selection procedures, 3326-Appointments of retired members of the armed forces to positions in the Department of Defense, 4103-Establishment of training programs, 4723-Confidentiality statutes, regulations and rules, 5533-Dual pay from more than one position; limitations; exceptions, Executive Order 9397.

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: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-999991241, Hiring Management Enterprise System

☐ 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: *List Privacy Act SORN Identifier(s)*

OPM/GOVT-5, Recruiting, Examining, and Placement Records, Federal Register Volume 79, Number 58 (March 26, 2014) https://www.gpo.gov/fdsys/pkg/FR-2014-03-26/html/2014-06593.htm

Each Federal agency retains ownership and control over its own records and is responsible for meeting the requirements under the Privacy Act for the collection, maintenance and sharing of its records. Applicants seeking information on their records owned and maintained by an agency should contact the employing agency in accordance with the applicable system of records notices published.

☐ No

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

☐ Yes: *Describe*
☒ No

Information collection requirements for this system are currently under review by the DOI Information Clearance Officer. The PIA will be updated if the determination is made that OMB approval is required for the DOI HMES in accordance with the Paperwork Reduction Act.

Section 2. Summary of System Data

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

☒ Name
☒ Disability Information
☒ Education Information
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Information stored and processed by the HMES includes employment related data such as job vacancies, position descriptions, position requirements and necessary qualifications, applicant questions, and

various other factual data. HMES also stores applicant information such as professional resumes and contact information. The overall purpose of HMES is to improve the hiring management process. Information is provided by applicants who submit resumes for Federal vacancy announcements. Resumes generally contain information identified above, and in some cases may also include additional information voluntarily provided by the applicant, such as date of birth, citizenship, gender, level of security clearance, or other pertinent information.

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: *Describe*

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: *Describe*

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

Employment related data provided by applicants in response to job vacancies, position descriptions, position requirements and necessary qualifications, applicant questions, and various other factual data are used to facilitate and improve the hiring management process. Applicant information contained in professional resumes and contact information are used for HR management and workforce development, to consider applicants who have applied for positions in the Federal Service by making determinations of qualifications, including disability status for positions applied for, and to rate and rank applicants applying for the same or similar positions. Data is also used to refer candidates to Federal agencies for employment consideration, including appointment, transfer, reinstatement, reassignment, or promotion. The information is used by the DOI HR specialists for the purpose of filling vacant positions within their respective organizations.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

DOI Bureaus utilize HMES for human capital management and workforce development, to find and hire candidates to develop the workforce. The records are used when considering individuals who have applied for positions in the Federal service by making determinations of qualifications for positions applied for, and to rate and rank applicants applying for the same or similar positions. DOI HR Specialists are restricted to data within the scope of their duties.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Information may be shared with other bureaus or any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purposes of the request, and to identify the type of information request), when necessary to obtain information relevant to an agency decision concerning hiring or retaining an employee, issuing a security clearance, conducting a security or suitability investigation of an individual, classifying positions, letting a contract, or issuing a license, grant or other benefit.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Other Federal customer agencies will have access to data for their own applicants, employees and contractors. PII data access is restricted to only the appropriate human resources personnel from each respective customer agency. Customer agencies do not have access to data from agencies other than their own. Information collected during this process may be disclosed to OPM or other Federal agency as authorized under the published routine uses in the OPM/GOVT-5, Recruiting, Examining, and Placement Records SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-03-26/html/2014-06593.htm

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Information may be shared with State or Local agencies when necessary and compatible with the purpose of the system as authorized under the published routine uses in the OPM/GOVT-5, Recruiting, Examining, and Placement Records SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-03-26/html/2014-06593.htm

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with contractors providing support services for maintenance or processing of HR functions, and as authorized under the published routine uses in the OPM/GOVT-5, Recruiting, Examining, and Placement Records SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-03-26/html/2014-06593.htm

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

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

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

HMES is an online HR management and staffing solution that allows individuals to apply for positions in the Federal service. Individuals voluntarily choose to participate in the hiring process, and have the opportunity to decline to participate or determine what information they choose to share**.** Due to the fact that the hiring process is fully online, if an applicant declines to provide information or to consent to its use, they will not be considered as an applicant for a position.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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

☒ Privacy Act Statement: *Describe each applicable format.*

The Monster Government Solutions System/HMES posts vacancy announcements to the OPM USA Jobs Website. A Privacy Act Statement link is what the Job Seeker sees on the USA Jobs Website which may be viewed at: https://www.usajobs.gov/Help/Privacy/

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through this privacy impact assessment and the published OPM/GOVT-5, Recruiting, Examining, and Placement Records, system of records notice, which may be viewed at: https://www.gpo.gov/fdsys/pkg/FR-2014-03-26/html/2014-06593.htm

☐ Other: *Describe each applicable format.*

☐ None

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

There are a number of Structured Reports built into the system with the option to create Ad-Hoc Reports. There is the option to schedule reports. Reports are based on a series of pre-defined datasets. In all of these reports, applicants are given a randomly assigned Applicant ID. SSN is not an option to run these reports.

In the Hiring Management section, there is an option to search applicants based on one or more of the following criteria: Last Name, Middle Name, First Name, E-mail and last 4 of SSN.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports will be produced for purposes of hiring management and may be generated by HR Specialists for vacancy information, including pre-defined reports for the Office of Personnel and Management and Equal Employment Opportunity Commission reports. Reports will be accessible to DOI HR personnel. As mentioned in the previous section, in the Hiring Management section, there is an option to search applicants based on one or more criteria. This section allows the user to view the following information on a single applicant: View Vacancies Applied, View Applicant Assessments, View External Assessments, View History and View Documentation. Anyone with access to the Hiring Management section of Monster has access to this functionality. It is possible to create an Ad-Hoc report to pull information on a single applicant. Anyone who has access to the Analytics section would have access to this functionality.

☐ No

Section 3. Attributes of System Data

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

Information in the HMES is received from individual applicants and is only as reliable as that provided by the applicant and inputted by the HMES user. The use of field restrictions and user confirmation where the user must validate that the information submitted is accurate. Also, applicants have an interest in ensuring their information is accurate during the hiring process.

B. How will data be checked for completeness?

Information in the HMES is received from individual applicants and is only as reliable as that provided by the applicant and inputted by the HMES user. HMES uses field restrictions and user confirmation where the user must validate that the information submitted is complete. Also, applicants have an interest in ensuring their information is accurate during the hiring process.

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

Information in the HMES is received from individual applicants and is only as reliable as that provided by the applicant and inputted by the HMES user. The applicant is responsible for the currency of the data submitted at the time of their job application.

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

Data for this system, as it relates to hiring/workforce general management and activities is maintained under the Departmental Records Schedule (DRS) 1.2.0004 Short-Term Human Resources Management Records, which was approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0001-0004). These records are maintained for 3 years after completion of the pertinent activity (e.g., hiring for a position is completed/canceled). Some extremely short-term lists or registers may be destroyed when no longer needed or are able to be superseded when necessary (DRS 1.2.0009, DAA-0048-2013-0001-0009).

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

Some records are destroyed by shredding or burning while magnetic tapes or disks are erased in accordance with NARA guidelines.

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 personally identifiable information collected from individuals during the application process. All data processed by HMES is considered to be sensitive data. The loss, misuse, or unauthorized access to or modification of data in HMES could violate the provisions of the Privacy Act of 1974 and Federal privacy policy. In order to ensure the confidentiality of the data, the HMES data is encrypted in compliance with National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) - 199. HMES provides single sign-on for the Position Classification, Hiring Management, Analytics, On-Boarding and Competency Management components in addition to having a central place to launch these applications.

There is a risk that DOI will collect more information than is necessary to make appropriate hiring decisions. This risk is mitigated by only requesting the information necessary to effectively recruit, assess, select, and hire qualified candidates for Federal positions. The information requested is necessary to make suitability, eligibility, and qualification determinations as part of the hiring and onboarding process.

There is a risk of collecting inaccurate information from applicants that may result in unfavorable hiring decisions. This risk is mitigated through the use of field restrictions and user confirmation where the user must validate that the information submitted is accurate and complete. Also, applicants have an interest in ensuring their information is accurate during the hiring process.

There is a risk that unauthorized individuals may access the information in HMES, use it for an unauthorized purpose, or use it outside the scope of the purpose for which it was collected. This risk is mitigated by ensuring effective access controls are implemented, and only authorized personnel are granted access to the records in HMES and agree to adhere to the DOI Rules of Behavior. Access to the

DOI network requires two-factor authentication. User access is based on least privilege in order to perform their official duties. Audit trail features are utilized to record and monitor user access and activities in the system to include event types, date and time of events, user identification, successful or failed access attempts, and security actions taken by system administrators. DOI and customer agency employees and contractors are required to complete privacy, security, and records management training and must adhere to rules of behavior.

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. The data collected and maintained is limited to the minimal amount needed to support human capital management, workforce development, and hire candidates for employment. Records are maintained in accordance with short term human resources management records schedules that were approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

There is a risk that individuals may not have sufficient privacy notice prior to providing information or may not have opportunity to consent to the collection or specific uses of their PII. This risk is mitigated by the detailed Privacy Act statement provided on the page where information is collected from individuals who are interested in applying for Federal employment, publication of this privacy impact assessment, and the OPM/GOVT-5 system of records notice.

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. Appropriate Privacy Act clauses were inserted into the vendor contract for the operation and maintenance of the system. HMES is categorized as a "Moderate" impact level system and is compliant with the Federal Information Security Modernization Act (FISMA). The privacy risks are mitigated throughout the information lifecycle. Data is collected directly from individual job applicants via an encrypted, secure Web connection. The use, processing, and retention of this data is by MGS and HMES HR personnel who have necessary access for the purpose of conducting their professional duties. Disclosure of data to other parties is subject to all applicable Federal laws and regulations. Destruction of the data is subject to Federal record retention policies and the requirements of DOI.

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: *Explanation*

HMES is a human resources management system, and the use of personal data is both relevant and necessary to the use of the system. The information collected in the HMES is directly related to the reason for which the system has been designed. The data elements are required for employment

purposes and for electronic automation of staffing management vacancies, notifying potential applicant data, and ranking applicants' qualifications based on such data.

☐ No

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

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*
☒ No

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

☐ Yes: *Explanation*
☒ No

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

Information in the HMES is received directly from individual applicants and is only as reliable as that provided by the applicant. The use of field restrictions and user confirmation where the user must validate that the information submitted is accurate and complete. Also, applicants can pursue an interest in ensuring their information is accurate during the hiring process.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ 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 HR employees (Hiring Specialists) who review the applications, apply the regulations for government hiring, and generate certificates of eligible job candidates. They cannot change data that an applicant has entered in the job application.

Applicants access the vacancy announcement and complete the job application via USAjobs.gov using their resume and supporting documents - this is outside of the HMES application and the applicant has full data management rights (access/edit/delete) over the data they provide. Once they submit an application, that application is sent to an HR Specialist for consideration. Once the application has been submitted, the applicant does not have data management rights (access/edit/delete).

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

Job applicants have access only to their personal data. HR personnel will have access only to that data necessary for the performance of their official duties. Access restrictions are based on least privilege for each employing DOI bureau or office and Federal customer. MGS personnel, in their role as administrators and developers, have access to data submitted by applicants to manage and operate the system.

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. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved with system maintenance on a limited basis and Privacy Act contract clauses are included. Most of the design and maintenance of the HMES is done internally by Monster Government Solution employees. However, some MGS contractors are involved in some of the design. These contractors have no access to PII, and there is a NDA in place. An adjudicated MGS employee escorts all contractors if there is the possibility of the presence of PII (i.e., cage access).

☐ 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. *Explanation*
☒ No

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

☐ Yes. *Explanation*
☒ 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 HMES 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. *Describe*

All network-related hardware (cabling, switches, routers, firewalls, etc.) include servers and other hardware components which constitute a support system for the HMES application, is physically secured at the vendor location in Virginia.

(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 HMES Information System Owner and Information System Security Officer share overall responsibility for ensuring privacy controls are implemented to protect the privacy of individuals, developing guidelines and standards which must be followed, and meeting the requirements of the Privacy Act. Privacy Act complaints, requests for access or amendment of records are addressed by the System Manager and DOI Privacy Officials. Customer agency 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, including decisions on Privacy Act requests for notification, access, and amendments, and addressing complaints.

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 Information System Owner and Information System Security Officer are responsible for oversight and management of privacy and security controls, ensuring proper use of data in the HMES, and reporting any potential loss, compromise or unauthorized access or disclosure of information to DOI-CIRC in accordance with Federal policy and established DOI procedures. HR Specialists and authorized users also share responsibility for protecting privacy and reporting any loss or compromise in accordance with Federal and DOI policy. Customer agency data is under the control of the customer agency. Each customer agency is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities, processing or management of the data.