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: Equal Employment Opportunity (EEO) Management Directive 715 (MD-715)

Date: 05-02-2016

Bureau/Office: Office of the Chief Information Officer

Bureau/Office Contact Title: Departmental Privacy Officer

Point of Contact Email: Teri_Barnett@ios.doi.gov

First Name: Teri

M.I.:

Last Name: Barnett

Phone: (202) 208-1605

Address Line 1: 1849 C Street, NW

Address Line 2: Mail Stop 5547 MIB

City: Washington

State/Territory: District of Columbia

Zip: 20240

Section 1. General System Information

A. Is a full PIA required?

Yes

Yes, information is collected from or maintained on

Federal personnel and/or Federal contractors

B. What is the purpose of the system?

Equal Employment Opportunities Management Directive 715 (EEO/MD715) is a web-based user interface application that produces Equal Employment Opportunity Commission (EEOC) compliant reports in accordance with the Equal Employment Opportunities Management Directive 715, which sets forth reporting requirements for establishing and maintaining effective affirmative programs of equal employment opportunity under Section 717 of Title VII of the Civil Rights Act of 1964, as amended, and effective affirmative action programs under Section 501 of the Rehabilitation Act of 1973, as amended. EEO/MD715 supports Federal agency reporting requirements and evaluations of employment

opportunity programs under the Equal Employment Opportunities Management Directive 715, which may be viewed at http://www.eeoc.gov/federal/directives/md715.cfm. EEO/MD715 is an auxiliary application maintained by the Department of the Interior (DOI) Interior Business Center (IBC) Human Resources Management Systems Division (HRMSD) Datamart that provides a data warehouse/reporting functionality for Federal agency customers of the IBC Human Resources Line of Business. EEO/MD715 and Datamart are subsystems of the Federal Personnel and Payroll System (FPPS), a personnel and payroll system providing customer-driven full life cycle personnel and payroll support to DOI bureaus and numerous Federal government agency customers.

C. What is the legal authority?

31 U.S.C. 3512, et seq.; 5 U.S.C. 5101, et seq.; 42 U.S.C. § 2000e-16, Employment by Federal Government; 5 U.S.C. - Reorganization Plan No. 1 of 1978; 5 U.S.C. § 901 et seq., Government Organization and Employees; Executive Order 11748, Equal Employment Opportunity in the Federal Government; Section 501 of the Rehabilitation Act Amendments of 1986; EEO Management Directive 715, EEO Reporting Requirements for Federal Agencies. 5 U.S.C. 7201, Sections 4A, 4B, 15A(1) and (2), 15B(11), and 15D(11); Uniform Guidelines on Employee Selection Procedures (1978); 43 FR 38297 et seq. (August 25, 1978); 29 CFR 720.301; and 29 CFR 1613.301.

D. Why is this PIA being completed or modified?

Existing Information System under Periodic Review

E. Is this information system registered in CSAM?

Yes

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

010-999999124124-00-01-01-01-00, Federal Personnel and Payroll System (FPPS) SSP

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	Describe
None	None	No	

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-7, Applicant Race, Sex, National Origin and Disability Status Records.
Data from Datamart and FPPS are covered under DOI-84, National Business Center Datamart, and DOI-85, Personnel, Attendance, Retirement, and Leave Records
Each Federal agency customer using EEO/MD715 is responsible for meeting the requirements of the Privacy Act, including publishing notices and establishing safeguards for their own use and sharing of data at their respective agencies.

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

No

Section 2. Summary of System Data

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

- [x] Name
- [ ] Citizenship
- [ ] Gender
- [x] Birth Date
- [ ] Group Affiliation
- [ ] Marital Status
- [ ] Biometrics
- [ ] Other Names Used
- [ ] Truncated SSN
- [ ] Legal Status
- [ ] Place of Birth
- [x] Other
- [ ] Religious Preference
- [ ] Security Clearance
- [ ] Spouse Information
- [ ] Financial Information
- [ ] Medical Information
- [x] Disability Information
- [ ] Credit Card Number
- [ ] Law Enforcement
- [ ] Education Information
- [ ] Emergency Contact
- [ ] Driver's License
- [x] Race/Ethnicity
- [x] Social Security Number (SSN)
- [ ] Personal Cell Telephone Number
- [ ] Tribal or Other ID Number
- [ ] Personal Email Address
- [ ] Mother's Maiden Name
- [ ] Home Telephone Number
- [ ] Child or Dependent Information
- [ ] Employment Information
- [ ] Military Status/Service
- [ ] Mailing/Home Address

Specify the PII collected.

Users who are authorized access to the system must provide work phone number, work email address and a Resource Access Control Facility user ID, which are required by the IBC-DM-101 "IBC Datamart User Access Request Form". However, this information is used to grant requests for access and is not maintained in the EEO/MD715 system.

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

- [x] Individual
- [x] Federal agency
- [ ] Tribal agency
- [ ] Local agency
- [x] DOI records
- [ ] Third party source
- [ ] State agency
- [x] Other

Describe

The EEO information processed by this application is taken from FPPS Datamart, which collects EEO data from Federal employees through two Human Resources (HR) survey forms that the individuals voluntarily complete during the hiring process at the employing agency. Employees have different methods to correct data, including updated HR forms or the use of online applications such as Employee Express ("EEX"), an application maintained by the U.S. Office of Personnel Management (OPM) that allows employees to initiate personnel and payroll actions and obtain payroll information.

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

- [ ] Paper Format
- [ ] Email
- [ ] Face-to-Face Contact
- [ ] Web Site
- [ ] Fax
- [x] Other
- [ ] Telephone Interview
- [x] Information Shared Between Systems

Describe

Information is originally collected from employees through Standard Form 181 and Standard Form 256 during the hiring and onboarding process at each employing agency, which is entered into personnel records at Federal agency HR systems. Federal employees can voluntarily access the forms and fill in information through an IBC hosted website, which is programmatically integrated with FPPS. Updates may also be made through agency HR organizations or by the individual employee through EEX, which has an interface with FPPS. The EEO/MD715 system does not collect PII directly from individuals, it only imports data from HRSMD Datamart, a sub-system of FPPS, to generate EEOC compliance reports.

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

To produce EEOC compliance reports as authorized and required by the Equal Employment Opportunities Management Directive 715 and related directives.

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

- [x] Within the Bureau/Office

Describe the bureau or office and how the data will be used.

Data will be used by bureaus and offices for statistical and reporting purposes in compliance with Equal Employment Opportunities Management Directive 715 and related directives.

☐ Other Bureaus/Offices

☒ Other Federal Agencies

Describe the federal agency and how the data will be used.

Federal agency customers generate aggregate reports to be shared with EEOC as required by the Equal Employment Opportunities Management Directive 715 and related directives. Data may be shared as authorized pursuant to routine uses outlined in the published system of records notices, OPM GOVT-7 and other applicable system notices.

☐ Tribal, State or Local Agencies

☒ Contractor

Describe the contractor and how the data will be used.

Contractors may be used for the development or support of the system, or internally by Federal agency customers.

☐ 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

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

The EEO-MD 715 system does not collect information directly from individuals, it only imports data from HRSMD Datamart to generate EEOC compliance reports. However, individuals do have the opportunity to decline to provide information at the time it is requested during the HR onboarding or hiring process. HR uses Standard Form 181 and Standard Form 256, which contain Privacy Act Statements that inform individual employees of the authority, purpose, and uses of the collected survey information. Employees can decline to provide information or voluntarily choose to identify their ethnicity/race and/or handicap status at that time.

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

☒ Privacy Act Statement ☒ Privacy Notice ☒ Other ☐ None

Describe each applicable format.

Privacy Act Statements are provided through standard forms when information is collected directly from individuals during the hiring process. The statements are as follows:

Standard Form 181 ETHNICITY AND RACE IDENTIFICATION
Ethnicity and race information is requested under the authority of 42 U.S.C. Section 2000e-16 and in compliance with the Office of Management and Budget's 1997 Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity. Providing this information is voluntary and has no impact on your employment status, but in the instance of missing information, your employing agency will attempt to identify your race and ethnicity by visual observation.

This information is used as necessary to plan for equal employment opportunity throughout the Federal government. It is also used by the U. S. Office of Personnel Management or employing agency maintaining the records to locate individuals for personnel research or survey response and in the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies.

Social Security Number (SSN) is requested under the authority of Executive Order 9397, which requires SSN be used for the purpose of uniform, orderly administration of personnel records. Providing this information is voluntary and failure to do so will have no effect on your employment status. If SSN is not provided, however, other agency sources may be used to obtain it.

Standard Form 256 SELF-IDENTIFICATION OF DISABILITY
Collection of the requested information is authorized by the Rehabilitation Act, as amended (29 U.S.C. 701, et seq.). Solicitation of your Social Security Number (SSN) is authorized by Executive Order 9397, which permits agencies to

use the SSN as the means for identifying persons with disabilities in personnel information systems. Your SSN will only be used to ensure that your correct disability code is recorded along with other employee information that your agency and OPM maintain on you. Furnishing your SSN or any other data requested for this collection effort is voluntary and failure to do so will have no effect on you. It should be noted, however, that where individuals decline to furnish their SSN, the SSN will be obtained from other records in order to ensure accurate and complete data. Employees appointed under Schedule A, Section 213.3102 (u) (Severe physical or mental disabilities) are requested to furnish an accurate disability code, but failure to do so will not affect them. Where employees hired under one of these appointing authorities fail to disclose their disability(ies), however, the appropriate code will be determined from the employee's existing records or medical documentation physically submitted upon appointment.

Privacy Notice
Individuals are also provided notice on how their PII is managed through the publication of this PIA, and system of records notices published in the Federal Register, such as OPM GOVT-7, Applicant Race, Sex, National Origin and Disability Status Records, DOI-84, National Business Center Datamart, and DOI-85, Payroll, Attendance, Retirement, and Leave Records. These system notices may be viewed on the DOI SORN page at https://www.doi.gov/privacy/sorn.

Other
Employee Express website has Privacy Policy that addresses the collection, transfer, and sharing of PII provided by the individual when updating personnel or payroll records. See excerpt below (https://www.employeeexpress.gov/PrivacyPolicy).

Providing Personal Information
If you provide us with personally identifiable information ((name, email address, Social Security Number, Login ID, your Employee Express Password or other unique identifier) this information is used only in connection with Employee Express and for such purposes as are described at the point of collection. If you complete a personnel or payroll action through Employee Express, we transfer the personal information you provided only to your servicing payroll office to process your transaction. We only share the information you give us with another government agency if your transaction relates to that agency, or as otherwise required by law. Information is collected for statistical purposes, and for history reports required to document the transactions you complete through Employee Express. Also, Employee Express sometimes performs analyses of user behavior in order to measure customer interest in the various areas of our site. We will disclose this information to third parties only in aggregate form. We do not collect information for commercial marketing.

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

The fields that are used to retrieve summary data include Date, Component, Status and Employment, which are filters for ranges of customized reports.

I. Will reports be produced on individuals?

Yes

What will be the use of these reports? Who will have access to them?

The data processed by this application will be used to generate numerous EEO compliance reports, such as those EEO reports submitted to EEOC on an annual basis, the internal EEO investigation research report, the internal EEO diversity statistics report and HR workforce analysis report. The reports do not identify specific individuals or contain sensitive PII related to specific individuals.

These reports will be used by EEO staff and Federal government compliance programs, Human Resources, EEOC, Veterans programs, and Disability programs. Statistical reports may be provided to partners for workforce purposes, however, they do not contain any PII.

Section 3. Attributes of System Data

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

Information is originally collected directly from individuals through Standard Form 181 and Standard Form 256 during the HR processes, and is maintained in FPPS. Updates may be made by the individual through hiring agency HR processes or use of Employee Express. Accuracy of data provided is verified by the individuals who voluntarily enter their own data.

B. How will data be checked for completeness?

All data provided for use in the EEO/MD715 application is collected directly from individuals on a voluntary basis during the hiring process, and is as complete as determined by the individual who wishes to provide it.

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

Individual employees may update their data at any time through agency HR processes and use of EEX. Data obtained through system interfaces is re-imported if there is any indication of transmission errors (e.g., file transfer was cut-off, faulty transmission). Specific procedures are followed through guidance from the Datamart Operations Manual, or through coordination with the IBC officials or FPPS standard process.

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

DOI EEO records maintained in EEO/MD715 are covered under DOI Office of the Secretary Records Schedule 7554.10 Equal Employment Opportunity/Management Directive 715 (EEO/MD715)(N1-048-09-06), which has been approved by the National Archives and Records Administration (NARA). The disposition is temporary, and files are cut off when report are finalized and destroyed 10 years after cut-off.

Records maintained in EEO/MD715 belonging to customer agencies are retained in accordance with applicable agency records retention schedules or General Records Schedules (GRS) approved by NARA, and customers are responsible for managing and disposing of their own records. Retention and disposition may vary based on the type of record and needs of the agency. The customer agency provides the IBC with the appropriate records retention schedule for the customer agency data and is responsible for managing their own records in accordance with 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?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

The records belonging to agency customers are handled by the records disposal authorities those customers have established with DOI. Procedures for disposing of data are followed in accordance with approved NARA regulations. Disposition procedures are documented at http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records.

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 are risks to the privacy of individuals due to the sensitive PII contained in the system. The risks are mitigated by a combination of administrative, physical and technical controls.

The EEO/MD715 application only imports necessary PII that is authorized and required by Directive 715, as indicated in the published OPM and DOI SORNs. Each government agency using EEO/MD715 is responsible for meeting the requirements of the Privacy Act for their own notices, where appropriate, and for the collection, use, sharing and safeguarding of data for their agency.

Data from EEO/MD715 is only used to produce EEOC compliance summary reports as specifically required by the Equal Employment Opportunity Management Directive 715. To prevent misuse, agency customers sign a Service Level Agreement (SLA) with the IBC to clearly establish and document IBC and customer security roles and responsibilities. Only authorized Federal agency human resources professionals with access to the system can process the data or generate reports.

These reports are submitted to the EEOC in accordance with the Equal Employment Opportunity Management Directive 715. The reports do not contain PII or identify specific individuals.
Retention and Disposal of data is in accordance with approved records retention schedules and methods for disposition in accordance with NARA guidelines. Customer agencies are responsible for managing their own records in accordance

with the Federal Records Act and providing appropriate records retention schedule requirements for their agency data.

IBC system access is granted using the concept of "least access" required to perform official duties. Physical controls are also in effect to limit access to IBC facilities. IBC applications, hardware, and network configurations have undergone numerous audits and reviews from internal and external organizations that validated privacy compliance.

All DOI employees and contractors are required to complete security and privacy awareness training on an annual basis, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training and sign DOI Rules of Behavior.

There are levels of security to prevent unauthorized access and monitoring for the EEO/MD715 application, including network security restrictions into DOI's wide area network and Resource Access Control Facility security, which is used to prevent unauthorized access to IBC mainframe resources. Application security is used to control access to the EEO/ MD715 application commands and range of data, and audit logs that record username, date, time, and user activities to ensure only authorized access and use of data. Security controls from FPPS are applied to data access tables containing FPPS data, including access restrictions based on least privileges.

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

The use of the data is both relevant and necessary to produce EEOC compliant reports for the Equal Employment Opportunity Management Directive 715.

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

No

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

No

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

No

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

Accuracy of the data entered into the system is verified by the individual employee at the time the data is provided.

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.

Data access is controlled through standard IBC mainframe access controls. System access is granted using the concept of "least access" required to perform official duties.

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

- ☒ Users
- ☐ Developers
- ☒ System Administrator
- ☒ Contractors
- ☐ Other

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

The data owner decides who has access to the specific data based on a user's job role and function. IBC system access

is granted using the concept of “least access” required to perform official duties.

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?

Yes, contractors are involved in the design and continued development of the EEO/MD715 application and privacy clauses are inserted in the contracts.

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

No

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

Yes

Explanation

The EEO/MD715 application utilizes audit features to monitor user activities as a security control to ensure only authorized access to and uses of data.

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

The EEO/MD715 application utilizes audit features to monitor user activities. Audit logs record authorized username, date and time of access, and user activities within the application.

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

There are five levels of electronic security to prevent unauthorized access and monitoring for the EEO/MD715 application.

• Network security limits access into DOI’s wide area network.
• RACF (Resource Access Control Facility) security is used to prevent unauthorized access to IBC mainframe resources.
• Application security is used to control access to the EEO/MD715 application commands and range of data. This system uses audit features that record username, date, time, and user activities to ensure only authorized access and use of data.
• Low level security from FPPS is applied to data access tables containing FPPS data, including access restrictions based on least privileges.
• Rules of Behavior are signed by all users.

All IBC system access is granted using the concept of “least access” required to perform official duties. Physical controls are also in effect to limit access to the IBC facilities.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

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

(3) Administrative Controls. Indicate all that apply.

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

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 FPPS Information System Owner and Information System Security Officer will have the ultimate responsibility implementing adequate controls and protecting the privacy rights of individuals affected by the use of the system and interface with other systems. The Information System Owner and the FPPS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with the Privacy Act and other Federal laws and policies for the data managed and stored within the system, and for making decisions on Privacy Act requests for notification, access, amendments, and complaints

For any customer agency data in the system, the customer agency is responsible for protecting the privacy rights of employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints. FPPS maintains a list of Data Custodians of the customer agencies.

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 Branch Chief, Applications Management & Technical Services Branch, Human Resources Management Systems Division (HRMSD), Interior Business Center has responsibility for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The FPPS Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the DOI Privacy Officer.