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: Federal Personnel and Payroll System (FPPS)

Date: 09-30-2015

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

All

B. What is the purpose of the system?

The Federal Personnel and Payroll System (FPPS) is an online personnel and payroll system providing support to the Department of the Interior (DOI) bureaus and offices, and Interior Business Center (IBC) Federal agency customers. FPPS is customized to meet customer needs for creating and generating the full life cycle of personnel transactions. FPPS allows for immediate updates and edits of personnel and payroll data. FPPS also handles regulatory requirements such as specialized pay, garnishments, and special appointment programs. FPPS also operates in batch mode for performing close of business, payroll calculation, and other processes. FPPS customers can use a web-enabled interface, WebFPPS, to access FPPS through a web browser to perform personnel and payroll tasks. FPPS has interconnections with other Federal agencies; private organizations; Federal agency customers; state, city and county governments; and IBC internal systems. FPPS is a major application that consists of several minor applications that are listed in question F below including time and attendance applications, a system for creating retirement cards and updating retirement records, a system for converting client data for integration into FPPS, and a data warehouse that provides reporting functions for human resources departments. Separate privacy impact assessments were conducted for these minor applications to ensure privacy implications are adequately identified and addressed.

C. What is the legal authority?

5 U.S.C. 5101, et seq; 31 U.S.C. 3512; 31 U.S.C. Chapter 11; 5 CFR part 253; 5 CFR part 297; The Office of Management and Budget Circular A-127, Revised, Financial Management Systems authorized the purchase or development of this system/application. This Circular is issued pursuant to the Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576 and the Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.).

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

010-9999991241 24-00-01-01-01-00, Federal Personnel and Payroll System

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
Indirect Cost System (ICS)	A web-based tracking system used for indirect cost proposals processed by the IBC Acquisitions Services Directorate.	Yes	PII includes name, organization, work phone number, work location. See the ICS PIA for an assessment of privacy risks.
Position Control System (PCS)	A web-based tool used by Human Resources (HR) staff for managing position data outside of FPPS.	Yes	PCS tracks positions available and filled within the Securities and Exchange Commission to prevent over hiring. PII includes employee name, position title, branch code, slot number, and position status (temporary or permanent). See the PCS PIA for an assessment of privacy risks.
Datamart Portal	A content management delivery system providing access and configurations to Datamart and other auxiliary applications. See the Datamart Portal PIA for an assessment of privacy risks.	No	
Quicktime	An online web-based time and attendance application that can be customized by clients for their requested functionality and to comply with their agency’s policies.	Yes	Quicktime provides ability to input, validate, and certify time and attendance data for transmission to FPPS. PII includes Social Security number (SSN), name, and user ID on Federal employees. See the Quicktime PIA for an assessment of privacy risks.

Subsystem Name	Purpose	Contains PII	Describe
webTA	An online web-based time and attendance application. WebTA is owned and developed by Kronos but is hosted at IBC's Denver Data Center and offered to new and existing IBC customers.	Yes	webTA provides the ability to input, validate, and certify time and attendance data of Federal employees and contractors for transmission to FPPS. PII includes SSN, Name, and User ID. See the webTA PIA for an assessment of privacy risks.
Datamart	An online web-based reporting environment that can be used by FPPS clients and other clients.	Yes	Datamart provides ability to query, analyze, chart and report data on Federal employees, retirees, volunteers, contractors, casual and emergency workers. PII includes SSN, name, Employee Common Identifier (ECI), home address, phone numbers, emergency contact information, medical and family leave, education, ethnicity and race, disability code, marital status, age, user IDs, involuntary debt (e.g. garnishments, child support), court orders, back pay, and individual bank routing numbers and account numbers. See the Datamart PIA for an assessment of privacy risks.
Retirement Sub System	A system that retains personnel and payroll transactions from an interface with FPPS, which are used to generate and store retirement card information. This information is submitted to the Office of Personnel Management (OPM) upon the employee's retirement. Access to the programs is limited to FPPS and IBC Payroll Operations Division (POD) staff.	Yes	This system retains personnel and payroll transactions with FPPS to generate and store retirement card information of current and former Federal employees. PII includes SSN, name, and age. See the Retirement Sub System PIA for an assessment of privacy risks.

Subsystem Name	Purpose	Contains PII	Describe
FPPS New Client Conversion	A process and the associated systems for accepting personnel and/or payroll system data from new clients or their providers, converting the data to FPPS format, validating the data, and then moving the data into the FPPS system.	Yes	This system supports FPPS functions by accepting personnel and payroll data from new clients or their providers, converts the data to FPPS format, validates the data then moves it into the FPPS system. Data is collected from Federal employees, retirees, volunteers, contractors, casual and emergency workers. PII includes SSN, name, ECI, home address, phone numbers, emergency contact information, medical and family leave, education, ethnicity and race, disability code, marital status, age, user ID, involuntary debt (e.g. garnishments, child support), back pay, individual bank routing numbers and account numbers. See the FPPS New Client Conversion PIA for an assessment of privacy risks.
QuickSAR	A user interface to the StarTeam database to input, track, and manage Software Action Request (SAR) change management documentation throughout its life cycle, including all change requests, problem reports, and data requests for the FPPS, WebFPPS, webTA, and Quicktime systems.	Yes	QuickSAR inputs, tracks, and manages change management documentation for FPPS, WebFPPS, webTA and Quicktime on Federal employees. PII includes SSN, name, and person number. See the QuickSAR PIA for an assessment of privacy risks.
Equal Employment Opportunity (EEO) Management Directive 715 (MD-715)	A web-based application to produce EEOC compliant reports for the MD-715 Directive.	Yes	This application is available to IBC clients to produce EEOC compliant report for the MD-715 Directive on Federal employees. PII includes name, ethnicity/race, and disability preference. See the EEO/MD-715 PIA for an assessment of privacy risks.

Subsystem Name	Purpose	Contains PII	Describe
Inter-Governmental Personnel Act	A web-based tool developed for the National Science Foundation (NSF) and used by IBC HR staff to track intergovernmental personnel assignments between NSF and other agencies.	Yes	This tool allows NSF to input and report on incoming and temporary assignments that exist between NSF and other agencies. PII includes SSN, ethnicity, race, sex, name, date of birth, work address, work phone number, organization and work assignment, college degree, grade point average, and college. See the IPA PIA for an assessment of privacy risks.
U.S. Department of the Interior Integrated Charge Card Program Web-Based Training (Charge Card Training)	The U.S. Department of the Interior Integrated Charge Card Program Web-Based Training application contains DOI charge card training data used for the purpose of internal reporting, program monitoring/tracking.	Yes	This application provides the ability to report, monitor/track and meet training requirements for the DOI charge card program. PII includes Federal employee status/organizational information, charge card account and transaction information, training data and trainee personal/profile information (account numbers, first and last name, business telephone, and SSN). See the U.S. Department of the Interior Integrated Charge Card Program Web-Based Training PIA for an assessment of privacy risks.
WebFPPS	A web-enabled presentation of the Federal Personnel and Payroll System. Using a web browser, users can access FPPS through WebFPPS to perform normal personnel and payroll tasks. There is no data in WebFPPS.	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)

Records in FPPS and the minor applications are maintained under government-wide system of records notices including OPM/GOVT-1, General Personnel Records, June 19, 2006 (71 FR 35342) and GSA/GOVT-7, Personal Identity Verification Identity Management System (PIV IDMS), April 25, 2008 (73 FR 22377; and DOI system notices DOI-79, Interior Personnel Records, April 23, 1999 (64 FR 20010); DOI-84, National Business Center Datamart, December 8, 2008 (73 FR 74506); DOI-85 Payroll, Attendance, Retirement, and Leave Records,, April 8, 2008 (73 FR 19090); and DOI-90, Federal Financial System, August 27, 1999 (64 FR 46930).

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.

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
□ Biometrics
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Other

□ Religious Preference
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
□ Credit Card Number
□ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity

☒ 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.

Taxpayer Identification Number; bank account information such as routing and account numbers; beneficiary information; bond co-owner name(s) and information; family member and dependents information; professional licensing and credentials; family relationships; age; involuntary debt (garnishments or child support payments); court order information; back pay information; user ID; time and attendance data; leave time information; employee common identifier (ECI); volunteer emergency contact information; person number which is a unique number that identifies a person within FPPS; person number-emergency which is a unique number identifying an individual within FPPS for a leave share occurrence; and person number-volunteer which is a unique number identifying an individual within the FPPS volunteer database.

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

State courts

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

☒ Paper Format
☒ Email

☒ Face-to-Face Contact
☒ Web Site

☒ Fax
□ Other

☒ Telephone Interview
☒ Information Shared Between Systems

Describe

FPPS has interconnections with other Federal agencies; private organizations; Federal agency customers; state, city and county governments; and IBC internal systems. FPPS customers can use a web-enabled interface, WebFPPS, to access FPPS through a web browser to perform personnel and payroll tasks. The FPPS functionality of the minor applications are only accessible via the IBC or client intranets, and interconnections with the FPPS are outlined in Interconnection Security Agreements and/or Memorandums of Understanding. Authorized users (supervisors, HR specialists, security, and facilities) can track vacancies and view the entry on duty date and location for new hires through real time interfaces with FPPS and other automated staffing systems—Monster's Enterprise Hiring Management and OPM's USA Staffing.

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

PII collected and maintained in FPPS is used to support a full suite of human resources and payroll functions for DOI bureaus, offices, and IBC Federal agency customers. FPPS also processes PII to manage regulatory requirements such as specialized pay, garnishments, and special appointment programs. PII is used for fiscal operations for payroll, time and attendance, leave, insurance, tax, retirement, debt, budget, and cost accounting programs; to prepare related reports to other Federal agencies including the Department of the Treasury and the Office of Personnel Management; for reporting purposes by the DOI component for which the employee works or the agency for which the DOI emergency worker works; and for human capital management purposes.

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 or office and how the data will be used.

FPPS currently has interconnections or interfaces with 14 external partners (Federal Government agencies or private organizations providing related services and requiring FPPS data), 35 state governments, 14 Cities/Counties, more than 40 Federal Government customers, and several IBC internal systems. This reflects the routine sending and receiving of more than one hundred interface files. These interfaces routinely change in quantity and data content. IBC maintains detailed documentation about each interface. Data routinely provided to others is detailed in the DOI--85, Payroll, Attendance, Retirement, and Leave Records--Interior System of Records Notice, and other applicable system notices.

☒ Other Bureaus/Offices

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

IBC shares data with DOI bureaus and offices to allow bureaus and offices to update and edit their personnel and payroll data.

☒ Other Federal Agencies

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

Data is shared and reported to other Federal agencies, including the Department of the Treasury and the Office of Personnel Management, as required for human resources, payroll, and tax purposes, and to Federal agencies for the purposes stated in the routine uses outlined in the DOI-85, Payroll, Attendance, Retirement, and Leave Records-Interior, System of Records Notice. FPPS data is not used in any matching programs.

☐ Tribal, State or Local Agencies

☒ Contractor

Describe the contractor and how the data will be used.

FPPS currently has interconnections or interfaces with fourteen external partners (Federal Government agencies or private organizations providing related services and requiring FPPS data), thirty-five state governments, fourteen Cities/Counties, more than forty Federal Government customers, and several IBC internal systems. This reflects the routine sending and receiving of more than one hundred interface files. These interfaces routinely change in quantity and data content. IBC maintains detailed documentation about each interface. Data routinely provided to others is detailed in the DOI-85, Payroll, Attendance, Retirement, and Leave Records-Interior, System of Records Notice. FPPS data is not used in any matching programs.

☒ Other Third Party Sources

Describe the third party source and how the data will be used.

FPPS currently has interconnections or interfaces with fourteen external partners (Federal Government agencies or private organizations providing related services and requiring FPPS data), thirty-five state governments, fourteen Cities/Counties, more than forty Federal Government customers, and several IBC internal systems. This reflects the routine sending and receiving of more than one hundred interface files. These interfaces routinely change in quantity and data content. IBC maintains detailed documentation about each interface. Data routinely provided to others is detailed in the DOI-85, Payroll, Attendance, Retirement, and Leave Records-Interior, System of Records Notice. FPPS data is not used in any matching programs.

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.

Yes, Federal employees have the option of not providing information on forms required during the application and onboarding process. These official forms contain Privacy Act Statements notifying individuals of the authority, purpose and uses of the information. The IBC FPPS customer agency determines what information should be collected from their employees, volunteers, and emergency contacts. However, employees are required by law to provide certain types of information, such as name and SSN as a part of the employment process. This information is required by applicable Federal statutes, including tax and employment eligibility regulations, and are necessary data elements in FPPS.

Federal employment forms collect the following information that is required from an individual to be considered for Federal employment; however, declining to provide this information may affect the employment eligibility and selection of the individual:

1. OF-306 - Declaration for Federal Employment. Some of the required fields include full name, SSN, date of birth (DOB), place of birth, felonies, military convictions, delinquent on federal debts.
2. I-9 - Employment Eligibility Verification. Some of the required fields include full name, address, DOB, SSN, Citizenship, proof of identity (driver's license, U.S. passport, SSN card, etc.).
3. Fair Credit Reporting Release - This document requires the applicant's signature in order for the Personnel Security Branch to obtain information for their background investigation to determine fitness for employment, security access, etc.

Below are forms that are requested but not required, and will not affect the employment eligibility and selection of the applicant:

1. SF-181, Ethnicity and Race Identification
2. SF-256, Self-Identification of Disability

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 when information is collected directly from individuals for entry into FPPS. For example, information is collected through forms that contain Privacy Act Statements, such as I-9, Employment Eligibility Verification. I-9 contains the following Privacy Act Statement:

Authorities: The authority to collecting this information is the Immigration Reform and Control Act of 1986, Public Law 99-063 (8 USC 1324a).

Purpose: This information is collected by employers to comply with the requirements of the Immigration Reform and Control Act of 1986. This law requires that employers verify the identity and employment authorization of individuals they hire for employment to preclude the unlawful hiring, or recruiting or referring for a fee, of aliens who are not authorized to work in the United States.

Disclosure: Submission of the information required in this form is voluntary. However, failure of the employer to ensure proper completion of this form for each employee may result in the imposition of civil or criminal penalties. In addition, employing individuals knowing that they are unauthorized to work in the United States may subject the employer to civil and/or criminal penalties.

Routine Uses: This information will be used by employers as a record of their basis for determining eligibility of an employee to work in the United States. The employer will keep this form and make it available for inspection by authorized officials of the Department of Homeland Security, Department of Labor, and Office of Specialist Counsel for Immigration-Related Unfair Employment Practices.

Individuals are also provided notice on how their PII is managed during these personnel and payroll activities through the publication of this PIA, the PIAs conducted for the related minor applications, systems of records notices published in the Federal Register, such as DOI-85, Payroll, Attendance, Retirement and Leave Records, and published government-wide system notices, such as OPM/GOVT-1, General Personnel Records.

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

Certain personnel within the DOI, Interior Business Center, involved in operations and maintenance of FPPS payroll operations, can retrieve information on an individual using:

- Employee Common Identifier (ECI) - unique number identifying employees across Federal automated systems
- SSN and full name
- Person Number - unique number which identifies a person within FPPS
- Person Number-Emergency - unique number identifying an individual within FPPS for a leave share occurrence
- Person Number-Volunteer - unique number identifying an individual within the FPPS volunteer database
- Taxpayer Identification Number (TIN) - unique number identifying the Trustee for the Estate of a deceased employee

FPPS authorized users, including customer agencies, may retrieve information on an individual using full name, SSN and ECI.

I. Will reports be produced on individuals?

Yes

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

Reports can be produced on an individual containing many of the data elements in FPPS. FPPS also routinely generates a variety of reports related to employment that are required by law, such as Internal Revenue Service (IRS) forms (1099-MISC and W-2); reports of withholdings and contributions for benefits and union dues; and reports on individuals who are delinquent on child-support payments. Access to the reports is limited to employees who process or file the reports and individuals who are granted access on a need-to-know basis. Copies of the reports may also be provided to government entities as required by law, such as tax forms to the IRS. Authorized disclosure of information outside DOI are described in the routine uses section of the DOI-85, Payroll, Attendance, Retirement, and Leave Records, system of records notice.

Information about individuals whose data is in FPPS cannot be retrieved without knowing specific information about the employee. For example, information about a trustee, family member, bond co-owner, or beneficiary cannot be retrieved without knowing certain information about the employee.

FPPS has a special reporting system which provides statistical summaries of the workforce showing breakdowns by relevant demographics and comparison between the representation in specific agency occupations in the civilian labor force.

FPPS provides various employee and position management information reports. These reports may also be generated from the public library using Super Natural Query. The Super Natural Query tool is used to extract information from FPPS to produce reports, either online or in batch format. Super Natural Query maintains the data integrity of FPPS so users will only be able to access records within their range of authorization as defined in FPPS. Users may also access preconfigured reports from the public library or from an agency's common library. Many of the preconfigured reports are also available in the Management information reports process. All FPPS users have access to the Super Natural query tool.

FPPS also provides a security report that lists termination or change transactions affecting system users.

Section 3. Attributes of System Data

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

Some data that is collected from new employees, such as name and SSN, is verified for accuracy using the U.S. Customs and Immigration Services’ E-Verify system or directly with the Social Security Administration. Other information, such as bank account information, is verified for accuracy by requesting copies of supplemental supporting documents directly from the individual, such as a voided check which validates the bank account routing and account numbers. In some cases, information such as home telephone numbers and emergency contact information is not verified for accuracy. It is the responsibility of the individual to provide the accurate information.

FPPS contains validity and relational edits designed to ensure the data entry technician inputs accurate information. The payroll data fields have the capability to ensure that the data entered is correct and cannot be altered such as validating employee SSN and state abbreviations; restricting the deletion of addresses; and requiring the use of numeric dates. Without valid data elements, actions cannot be processed by FPPS. The Payroll Operations Division (POD) requires authorized documentation from clients, or relies on regulatory requirements (i.e., tax law changes), before making adjustments to data in the system.

Where feasible, data entry modules in FPPS utilize a variety of data integrity validation controls to limit data entry errors, such as drop down menus, check boxes, text field size limitations, and predefined formats. A field may also use an edit mask to force entry of an SSN 999999999 as 999-99-9999 or the date 20000114 as 2000/01/14.

During Quicktime and WebTA processing, time and attendance (T&A) data transfers into FPPS. The mainframe then executes an Oracle SQL script to flag records that have been uploaded to FPPS to avoid duplication of data. After Quicktime and WebTA bi-weekly processing is complete, a regularly scheduled job is run from Quicktime and WebTA servers to generate the results of the bi-weekly mainframe run. All results including errors are included in this file. In addition, an output file is generated to capture any specific T&A errors. The Systems Analysis and Training (SAT) group in POD is notified via email if T&A files have been processed. SAT will review the applicable T&A errors file on the IBM and notify the IBC Payroll Operations Branch if corrective actions are required.

Each FPPS client is responsible for implementing procedures to verify the information their users enter directly into FPPS where FPPS data validation controls are not in place are accurate and complete.

B. How will data be checked for completeness?

FPPS clients can configure the system to make data fields mandatory or optional. If a data field is mandatory, data validation checks, such as a block on creating a new record, are employed to ensure that all mandatory data is entered. The user can bypass an optional field by pressing the ‘Enter’ key.

Where feasible, data entry modules in FPPS utilize a variety of data integrity validation controls to limit data entry errors, such as drop down menus, check boxes, text field size limitations, and predefined formats. A field may also use an edit mask; for example, to force entry of an SSN 999999999 as 999-99-9999 or the date 20000114 as 2000/01/14.

Each individual FPPS client is responsible for implementing additional procedures to verify the accuracy and completeness of the information that is provided on behalf of their agency. In some cases, the information provided by individuals is not verified, and the individual providing the information is responsible for the accuracy of the information that is supplied.

In addition, servicing personnel staff and client managers will perform various functions to check data for completeness, such as the following:

- Review and edit data to ensure that all required fields are populated, complete, and in conformance with Federal government personnel rules.

- Review records to validate the existence and completeness of time and attendance records for all active employees for the current pay period.

- Edit payroll transactions to ensure all required fields are populated and complete.

- Monitor time and attendance records to ensure these records have been received from the time and attendance modules.

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

Data in FPPS must be maintained in a current state in order to perform the system’s human resources and payroll functions. Each agency supplying data for use in FPPS is responsible for keeping the data they provide up to date, including establishing procedures for updating data. The system also employs various data validation controls to ensure that data entered into the system is current. These date validation modules can notify Data Custodians if certain data has been held in excess of a certain amount of time without an update.

The Employee Express interface with FPPS allows employees the opportunity to input data for many types of personal transactions which are loaded into FPPS on a regular basis. The effective date of the transaction initiated in Employee Express is based on the type of transaction, when it is initiated, and whether a transaction is starting or stopping an action. Therefore, if the transaction affects payroll, it may or may not be implemented for the pay period in which the transaction was entered based on the effective date.

FPPS runs a number of processes daily and other designated times (e.g., close of business, paid dailies, one-time adjustments, T&A gathers, pay calculate, etc.) to compile transactions and help to ensure all personnel and payroll data is current. If data is not current, payroll will be inaccurate.

There are no documents that describe all FPPS edits and validations or interface file agreements, which help to ensure data is current. This information is contained in design documents, the online help system, and within the FPPS codes.

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

Records maintained in FPPS belonging to customer agencies are retained in accordance with applicable agency records retention schedules or General Records Schedules (GRS) approved by the National Archives and Records Administration (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.

FPPS data is covered under General Records Schedule 1 “Civilian Personnel Records” and Schedule 2, “Payrolling and Pay Administration Records” and under DOI Office of the Secretary (OS) Schedules 1400 and 7551. These schedules have various retention for different types of data.

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

Each customer agency storing data in the system maintains those records under NARA approved records schedules for the retention of reports and data. While the IBC provides system administration and management support to agency clients, any records disposal is in accordance with customer agency approved data disposal procedures and each customer agency is responsible for meeting records requirements and managing the disposition of those records at the end of the retention period.

Customer agencies are responsible for purging employee data according to the customer agency records schedule after an employee’s access authority is terminated or the employee retires, changes jobs, or dies. The IBC may purge or delete any customer payroll or personnel records if it is a requirement of the customer agency and is agreed upon in the Inter-Agency Agreement with the IBC.

DOI records are disposed of by shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

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 volume of sensitive PII contained in the system. FPPS supports a full suite of human resources functions, including calculating payroll for DOI and numerous Federal customers. The data in FPPS is necessary to perform those functions and to comply with related Federal laws and regulations. To prevent misuse (e.g., unauthorized browsing) FPPS clients sign a Service Level Agreement (SLA) with the IBC to clearly establish and document IBC and client security roles and responsibilities. Most of the employee data in FPPS is collected from individuals and entered into FPPS by an authorized Federal human resources professional with access to the system.

The FPPS system has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with FISMA and NIST standards. FPPS is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.

Data is maintained to support agency personnel and payroll operations in accordance with approved records retention schedules. The retention and procedures for disposition for FPPS data is covered under General Records Schedule 1 “Civilian Personnel Records” and Schedule 2, “Payrolling and Pay Administration Records” and under DOI Office of the Secretary (OS) Schedules 1400 and 7551.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will 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, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The IBC follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training, 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.

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 FPPS data is both relevant and necessary. FPPS supports a full suite of human resources functions, including calculating payroll, for DOI and numerous Federal customers. The data in FPPS is necessary to perform those functions and to comply with related Federal laws and regulations.

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?

Yes

Explanation

The cumulative data figures described above will become part of each individual’s record, and will be used for payroll and various types of reporting.

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?

POD has procedures in place to validate pay data calculations, make timely disbursements, and correct errors to ensure the employee receives an accurate paycheck. Various validation tools help identify processing discrepancies so that adjustments can be made as appropriate. Any necessary corrections to payroll are completed on a daily basis both prior to and after the payroll calculation process.

Time and Attendance (T&A)
Once the T&A data has been loaded into FPPS, the Payroll Operations Branch (POB) reviews the data to determine whether T&A records are missing. POB notifies the clients of missing T&A records so that the client may send in the missing data prior to the bi-weekly calculation.
POB analyzes and reviews any FPPS error messages that may be a result of input of inaccurate data. The edits invoked in FPPS on T&A data identify most T&A errors that would result in incorrect or incomplete pay. The POB staff researches inaccuracies prior to processing payroll calculations and resolves errors where possible. POB relies upon authorized input (i.e., signed timesheet) from the client in order to resolve any problems with T&A. No correction or adjustment is made in payroll without an authorization, (either by law or regulation),
or an authorized document provided by the client. This authorization procedure applies to changes that are requested by an individual client employee as well as changes/procedures requested by an agency as a whole.

Employee Express
Employee Express is an online employee self-service program made available by the Office of Personnel Management that allows the individual to make certain changes to their payroll or personnel data. Occasionally, the interfacing transactions fail and do not update FPPS correctly. The POB receives daily Employee Express interface error listings that are reviewed within the current pay period and the status of resolution is tracked during the bi-weekly review performed by the Supervisor and Lead.

Payroll Calculate Processing
After the bi-weekly calculate the POB reviews FPPS reports daily to identify any incomplete or inaccurate payments that were made. Inaccurate payments may occur when T&A or other authorizing documentation was not received by POB prior to processing payroll calculate. Based on the type of error, POB will contact either the employee's timekeeper or Servicing Personnel Office (SPO) to start the process of correcting the employee's record. Depending on the type of corrective action processed POB can make a supplemental payment (paid daily) to the employee after the payroll calculating process has been completed for the current pay period. Before processing a paid daily, POB requires an amended T&A or confirmation that the SPO has completed the corrective personnel action. POB procedures require that authorizing documentation from the client support all corrections made in the system. Corrections and adjustments are reviewed by a supervisor, lead, or Payroll Program Technician. The following pay period, during the recompensation review process, POB processes the corrected T&A or personnel action for payment while offsetting the paid daily payment. This completes the corrective cycle and ensures a correct pay record for the employee. Source documentation is maintained for each action taken by payroll. Most documentation is electronically imaged and maintained indefinitely in the POD's Document Retrieval System.

The Certifying Officer (CO) uses the Threshold Exception listing to support the validity of the bi-weekly disbursements being scheduled for payment that exceed a predetermined dollar threshold. The CO may conduct research if the payment is not included on the Threshold Exception listing to determine whether it is a valid override of the threshold or may choose to suspend the payment, removing it from the disbursement schedule altogether to be further analyzed to determine if it is a valid payment.

POB logs and tracks the resolution of work activities in FPPS. The Open Report is available to Supervisors and Leads to monitor status of open records and ensure work assigned to staff is completed in a timely manner. The type of work activity will determine the time period the Payroll Technicians are allowed for resolution. If the work activity is not corrected within that time period, the Supervisor will meet with the Leads to determine the next steps taken. At this point in time the activity is either closed and prior follow-up is noted in the tracking system or the Supervisor or Lead will work with the Payroll Technician to obtain the missing information needed to close the activity. It is the responsibility of the Payroll Technician to keep the status of their work activities up-to-date within the tracking system.

Federal Employment and Income Taxes
FPPS provides a report to the Review and Analysis Branch (R&A) that summarizes all federal tax withholdings and contributions. Tax Accountants within R&A reconcile this report bi-weekly to the general ledger to ensure that all federal employment and income taxes are accounted for and will be paid correctly.

The taxes and earned income credit (EIC) payments are entered manually into the Electronic Federal Tax Payment System (EFTPS) once the bi-weekly payroll taxes are reconciled to the general ledger. The payment is authorized to be issued to the Internal Revenue Service (IRS) after all data is verified. The payment is issued by Treasury through EFTPS. U.S. Treasury's (Treasury's) CA$H-LINK II system is used to confirm that the payments were issued. Once the payment has been confirmed in CA$H-LINK II, an entry will be made into the accounting system to record the payment.

F. Are the data or the processes 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 ☒ Developers ☒ System Administrator

☒ Contractors ☒ Other

Describe

Access to the data in the system will be granted as follows:

• FPPS system administrators, programmers, developers, analysts, database administrators, payroll operations staff, and others (who may be contractors) supporting the system and performing system maintenance and other related activities and may have access to the data in the system.

• Each FPPS client has a Data Custodian who is responsible for granting access to their agency's data in FPPS. The Data Custodians have access to all of the data for their agency. This may include human resources personnel, supervisors, and administrative support staff for the agency. Access to FPPS will vary among customers depending on the policies implemented by the individual customer.

• Bureau/Office Data Custodians may have access to another bureau/office’s record on an authorized need-to-know basis. This can occur, for example when one bureau is cross servicing another bureau to provide support for certain HR functions.

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

Each FPPS client (including IBC) has an appointed Data Custodian who is responsible for granting access to their agency’s FPPS data. The Data Custodian appoints Security Points of Contact (SPOC), who can set and restrict data access privileges for system users. Access for Data Custodians and SPOCs is granted by the IBC through the Decentralized Security Administration Facility (DSAF) application. The DSAF controls access to the mainframe computer that hosts FPPS.

The following three forms that contain relevant guidance, are used for delegating access and rights to Data Custodians and SPOCs:

• DEN-NBC-IT-01: Data Custodian Responsibility Statement
• DEN-NBC-IT-02: Data Custodian and SPOC Designation
• DEN-NBC-IT-03: SPOC Responsibility Statement and Rules of Behavior

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 in the design, development and maintenance of the system. Privacy Act clauses are included in each contract where FPPS design, development, and maintenance is performed as part of services provided.

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

FPPS monitors authorized users by maintaining an audit trail of activity. The audit trail includes the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator’s identification); and activities that could modify, bypass, or negate the system’s security controls. 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.

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

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

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

IBC fully complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any FPPS equipment. The use of DOI IT systems, including FPPS, 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 Cards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Other
☐ Combination Locks
☒ Locked Offices

(2) Technical Controls. Indicate all that apply.

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

Describe

TLS

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Other
☒ 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

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The IBC Office of Human Resources, Deputy Chief Financial Office Director serves as the FPPS Information System Owner and the official responsible for oversight and management of the FPPS security controls and the protection of customer agency information processed and stored by the FPPS system. 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 Federal laws and policies for the data managed and stored in FPPS. Customer agency data in FPPS 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 providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing 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 FPPS Information System Owner is responsible for oversight and management of the FPPS security and privacy controls, and for ensuring to the greatest possible extent that FPPS customer agency and agency 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 is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of customer agency and agency PII is reported to the customer agency and US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures. The customer agency data in FPPS 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 or management of the data.

Department of the Interior
Privacy Impact Assessment

Name of Project: Datamart
Bureau: Office of the Secretary
Project's Unique ID (Exhibit 300): 010-00-01-07-01-1245-24

A. CONTACT INFORMATION:

1) **Who is the Bureau/Office Privacy Act Officer who reviewed this document?** (Name, organization, and contact information)

Rachel Drucker
NBC Privacy Officer
1951 Constitution Ave., NW, Mailstop 116-SIB
Washington, DC 20240
Phone: 202-208-3568
Email: Rachel_Drucker@nbc.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

Datamart provides two separate applications. The two applications are the FPPS Datamart and the FFS Data Warehouse. Access to FFS data is controlled by the FFS Data Warehouse administrators.

1) **Does this system contain any information about individuals** *{this question is applicable to the system and any minor applications covered under this system}***?**

The Datamart application may contain the following personal information about individuals:

- Social Security Numbers
- Name
- Employee Common Identifier (ECI)
- Home Address
- Phone Numbers
- Emergency Contact information
- Medical and Family Leave
- Education
- Ethnicity and Race
- Disability Code
- Marital Status
- Age
- User IDs
- Involuntary Debt (e.g. garnishments, child support)
- Court Orders
- Back Pay
- Individual bank routing numbers and account numbers

a. **Is this information identifiable to the individual**[1]*{this question is applicable to the system and any minor applications covered under this system}***?** (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. If YES complete all sections for system and any applicable minor applications).

Yes. The information in Datamart is identifiable to the individual.

b. **Is the information about individual members of the public** *{this question is applicable to the system and any minor applications covered under this system}***?** (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes. The information in Datamart may be about members of the public if the individual is a federal retiree, casual worker, volunteer, contractor or individual designated as an emergency contact of a volunteer.

c. **Is the information about employees** *{this question is applicable to the system and any minor applications covered under this system}***?** (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 Datamart 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 purpose of Datamart is to provide end users the ability to query, analyze, chart, and report on FPPS, FFS, and other data. Datamart provides a library of over 185 preformatted queries, plus the ability to create and run ad-hoc queries. The preformatted queries enable FPPS and FFS users to get timely information from Datamart and produce reports. The end-user can also export this information to many formats for processing elsewhere. Direct access to this data for reuse in other applications can be configured through secure, direct connections to the underlying Oracle database.

2a) List all minor applications that are hosted on this system and covered under this privacy impact assessment:

There are no minor applications hosted under Datamart.

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

The legal authority for the Datamart application is defined in the Office of Management and Budget Circular A-127, Policies and Standards for Financial Management Systems. This Circular is issued pursuant to the Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-

[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).

576 and the Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); and 31 U.S.C. Chapter 11.

C. DATA IN THE SYSTEM:

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

Categories of individuals covered in the Datamart application include employees, casual workers, contractors, retired federal employees, and volunteers of executive branch and independent agencies, government corporations, commissions, panels, councils, and foundations, and emergency contacts for employees and volunteers.

The Datamart application contains information about employees under a wide range of pay authorities covering individuals under the General Pay Schedule, Title 4 (National Park Service Law Enforcement), Title 5 (Government Organization and Employees), Title 6 (Bureau of Indian Affairs Contract Educators), OPM-approved pay plans, and public laws unique to FPPS application clients (e.g., Presidio Trust, Casuals, Overseas Private Investment Corporation, Securities and Exchange Commission, and Department of Transportation).

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

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 information in the Datamart application is received from the following sources:

- The initial personnel information on each employee is provided through interface files and other interface methods from the FPPS application.
- Financial data is provided from interface files from the FFS application.
- Employee information that is not received from the FPPS may be received as a file for input into the Datamart.

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

Datamart: The following entities use the FFS data in Datamart:

- DOI/Office of the Secretary
- Equal Employment Opportunity Commission
- National Transportation Safety Board

The agencies listed below may use the Datamart to perform queries and reports on FPPS information:

- Advisory Council on Historic Preservation
- African Development Foundation
- Arctic Research Commission
- Chemical Safety and Hazard Investigation Board
- Commission of Fine Arts
- Consumer Product Safety Commission
- Department of Education
- Department of the Interior
- Department of Transportation
- Equal Employment Opportunity Commission

- Federal Energy Regulatory Commission
- Federal Labor Relations Authority
- Federal Retirement Thrift Investment Board
- Federal Trade Commission
- Harry S. Truman Scholarship Foundation
- Institute of Museum and Library Sciences
- Inter-American Foundation
- International Trade Commission
- James Madison Memorial Fellowship Foundation
- Millennium Challenge Corporation
- National Aeronautics and Space Administration
- National Commission of Libraries & Information Science
- National Labor Relations Board
- National Science Foundation
- National Transportation Safety Board
- Nuclear Regulatory Commission
- Office of Navajo and Hopi Indian Relocation
- Overseas Private Investment Corporation
- Pension Benefit Guaranty Corporation
- Presidio Trust
- Public Defender Service for the District of Columbia
- Securities and Exchange Commission
- Selective Service System
- Social Security Administration
- U.S. Holocaust Memorial Council
- U.S. Forest Service
- U.S. Trade and Development Agency
- Utah Reclamation Mitigation Conservation Commission
- Valles Caldera National Preserve

Other Department of Interior bureaus and other agencies may be added in future years

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

No Tribal, State, or local agencies are providing data for use in the Datamart application.

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

Data is not collected from any other third-party source for the Datamart application.

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

No data is collected from the general public for the Datamart application.

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?

For the Datamart application, the use of the data is both relevant and necessary to process reports, queries, and management of information.

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?

Datamart does not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

Not applicable for Datamart (see previous answer).

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

Not applicable for Datamart.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

Retention periods for Datamart data are covered under the DOI Office of the Secretary (OS) Records Schedule series 1400 and 7554.

2) 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?

Procedures for disposing of data in Datamart are fully documented in the DOI OS Records Schedule.

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

Datamart contains information from two separate systems already covered by several existing Privacy Act Systems of Records Notices: OPM/GOVT-1 (the government-wide system for general personnel records maintained by the Office of Personnel Management), DOI-79, Interior Personnel Records, DOI-85 Payroll, Attendance, Retirement, and Leave and DOI-90, Federal Financial System, as well as a separate Privacy Act System of Records Notice DOI-84, Datamart.

Each government agency using Datamart is responsible for their own system of records notice covering the collection of data at their agency.

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

The system is not being modified.