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)
Bureau/Office: Interior Business Center
Date: April 22, 2020
Point of Contact:
Name: Danna Mingo
Title: Office of the Secretary Associate Privacy Officer
Email: os_privacy@ios.doi.gov
Phone: (202) 208-3368
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The 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 human resources processes.

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 which are managed by the DOI IBC Office of Human Resources, and are listed below including time and attendance (T&A) 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 resource organizations. This privacy impact assessment covers all these minor applications or sub-systems that provide a full suite of human resources and payroll functions for DOI bureaus, offices, and IBC Federal agency customers.

WebFPPS
WebFPPS is a web-enabled presentation of FPPS that provides users with access to FPPS on a web browser to perform routine personnel and payroll tasks.

Quicktime
Quicktime is an online web-based T&A application. The purpose of Quicktime is to input, validate, and certify time and data for transmission to FPPS. Quicktime is a tool used by employees to enter their time, leave requests, traditional timekeeper data entry, and provides standard reports.

WebTA Federal Employee Time-Keeping
WebTA is an online web-based T&A application. WebTA is used to input, validate, and certify T&A data for transmission to FPPS. WebTA is a tool used by employees to enter their time and leave requests, and for timekeeper data entry and standard reports. WebTA is owned and developed by Kronos but is hosted at the IBC Office of the Chief Information Officer (OCIO) Data Center and is offered to new and existing Federal agency customers. The WebTA capabilities include:

- Automatic population of timesheets from pay period to pay period when applying default employee schedules, including Federal holidays
- Validation of timesheets based on Federal rules for pay plans, employee leave, and flexible schedules, including automatic alerts to discrepancies
- Online employee leave and premium pay requests, including supervisor alerts to requests and online supervisor approval
- Automated leave balance and employee timesheet updates following leave requests, including automatic population of pay-period timesheets
- Support for leave transfer programs, allowing employees to donate leave and use donated leave from within the application

- Multi-level approval process and certification to help facilitate timesheet accuracy and security
- Interface with most financial management and payroll systems

FPPS New Client Conversion
The FPPS New Client Conversion (NCC) was the associated system of FPPS for accepting personnel or payroll system data from new clients or providers. NCC converts the data to FPPS format while validating the data and then moves the data into FPPS.

Datamart
Datamart is an online web-based application that serves as a reporting system with data warehouse reporting functionality for the Human Resources (HR) line of business of numerous IBC Federal agency customers. The purpose of Datamart is to provide end users the ability to query, analyze, chart, and report on FPPS, DOI systems such as the Talent Management System, Quicktime, and WebTA, and other customer specific data. Datamart provides a library of over 185 pre-formatted analyses, plus the ability to create and run ad-hoc analyses. The pre-formatted analyses enable FPPS users to obtain timely information from Datamart and produce reports. The end-user can also export this information to many formats for processing out of FPPS. Direct access to this data for reuse in other applications can be configured through secure, direct connections to the underlying Oracle database.

Datamart Portal
The Datamart Portal is a web-based content management delivery system that provides user-friendly access to information about Datamart and provides a link to its query application tool, OBIEE (Oracle Business Intelligence Enterprise Edition). It also contains Equal Employment Opportunity (EEO) information and provides access to auxiliary applications supported by Datamart. The following are the Datamart Auxiliary Applications which are minor systems developed and managed by the Human Resources Management Systems Division Datamart to support the use of additional client application and meet reporting needs.

- **Equal Employment Opportunity Management Directive 715**
  Equal Employment Opportunity Management Directive 715 **(**EEO/MD-715) is a web-based application developed for all FPPS-based clients to produce compliant reports in accordance with the Equal Employment Opportunity Commission's (EEOC's) Equal Employment Opportunity Management Directive 715. Use of this system enables reporting to establish and maintain effective affirmative programs of equal employment opportunity under Section 717 of Title VII of the Civil Rights Act of 1964, as amended, and Section 501 of the Rehabilitation Act of 1973, as amended.

- **Indirect Cost System**
  The Indirect Cost System (ICS) is a web-based application developed for the DOI Office of Indirect Cost Services to manage the indirect cost proposal process for the Department and its servicing clients including, DOI, non-DOI Federal agencies, insular/state/local/Tribal governments and nonprofit organization. The DOI Office of

Indirect Services is a shared services provider designated by the Office of Management and Budget. Use of this system allows for the preparation of cost proposals and allocation plans to ensure that indirect costs paid by the U.S. Government are legally sound, fair, and equitable.

- **Inter-Governmental Personnel Act**
  The Intergovernmental Personnel Act (IPA) system is a web-based application developed for the National Science Foundation (NSF) to manage and track intergovernmental personnel incoming and outgoing work assignments. Use of this system facilitates proper implementation of title IV of the Intergovernmental Personnel Act of 1970 and title VI of the Civil Service Reform Act that authorize the temporary assignment of employees between the Federal Government; State, local, and Indian tribal governments; institutions of higher education; and other eligible organizations.

- **Position Control System**
  The Position Control System (PCS) is a web-based application developed for the Security and Exchange Commission (SEC) to manage position data outside of FPPS. Use of this system provides a full management of agency workforce data through tracking of on-board strength, vacancies, and positions against FPPS data to maintain workforce levels authorized by Congress.

The Datamart Portal is currently being redesigned and will be placed under the web-based content management system called “FedHR Portal”.

C. What is the legal authority?

5 U.S.C. 5101, et seq., Government Organization and Employees; 31 U.S.C. 3512, et seq., Executive Agency Accounting and Other Financial Management Reports and Plans; 31 U.S.C. 1101, et seq., the Budget and Fiscal, Budget, and Program Information; 5 CFR part 293, subpart B, Personnel Records Subject to the Privacy Act; 5 CFR part 297, Privacy Procedures for Personnel Records; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers; and Public Law 101-576 (Nov. 15, 1990), the Chief Financial Officers (CFO) Act of 1990.

ICS - 31 U.S.C. 3512 et seq, the Federal Managers' Financial Integrity Act of 1982; 31 U.S.C. Chapter 11, the Budget and Fiscal, Budget, and Program Information; the Office of Management and Budget Circular A-127, Policies and Standards for Financial Management Systems.

PCS - 43 USC 1467; 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

Quicktime - 5 U.S.C. 5101 et seq, Government Organization and Employees; 31 U.S.C. Chapter 11, The Budget and Fiscal, Budget, and Program Information; 5 CFR part 293, Subpart B—Personnel Records Subject to the Privacy Act; and 5 CFR part 297, Privacy Procedures for Personnel Records. The Office of Management and Budget Circular A-127, 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; Federal Managers' Financial Integrity Act (FMFIA) of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); 31 U.S.C. Chapter 11; and Federal Financial Management Improvement Act (FFMIA) of 1996, P.L. 104-208 (31 U.S.C. 3512 et seq.)

IPA - 5 U.S. Code, Chapter 33, Subchapter VI, Section 3371-3376, Assignments To and From States; 5 CFR Part 334, Temporary Assignment of Employees Between Federal Agencies and State, and Local, and Indian Tribal Governments, Institutions of Higher Education, and other Eligible Organizations; 5 CFR Part 334 RIN 3206–AG61 Intergovernmental Personnel Act Mobility Program; Executive Order 11589 of April 1, 1971; The Intergovernmental Personnel Act of 1970; HHS Instruction 300-3: Detail and Intergovernmental Personnel Act (IPA) Assignments, July 22, 2013.

EEO/MD-715 - 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?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

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

010-9999991241, Federal Personnel and Payroll System (FPPS) System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Indirect Cost System (ICS)	A web-based tracking system used for indirect cost proposals processed by the IBC Acquisitions Services Directorate.	Yes	ICS provides tracking and management of financial services data for DOI and its clients. This data is non-FPPS related and PII includes name, organization, work phone number, work location.
Position Control System (PCS)	A web-based tool used by HR staff for managing position data outside of FPPS.	Yes	PCS tracks positions available and filled within the SEC to prevent over-hiring. PII includes employee name, position title, branch code, slot number, and position status (temporary or permanent).
Quicktime	An online web-based T&A 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 T&A data for transmission to FPPS. PII includes Social Security number (SSN), name, and user ID on Federal employees.
WebTA	An online web-based T&A application. WebTA is owned and developed by Kronos but is hosted at the OCIO Data Center and offered to new and existing IBC customers.	Yes	WebTA provides the ability to input, validate, and certify T&A data of Federal employees and contractors for transmission to FPPS. PII includes SSN, Name, and User ID.
Datamart	Datamart provides the ability to query, analyze, chart and report data on Federal employees, retirees, volunteers, contractors, casual and emergency workers.	Yes	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.
Datamart Portal	An online web-based reporting environment that can be used by FPPS clients and other clients. A content management delivery system providing access and configurations to Datamart and other auxiliary applications.	No	
FPPS New Client Conversion (NCC)	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.	Yes	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.
Equal Employment Opportunity Management Directive 715 (EEO MD-715)	A web-based application that provides EEOC compliant reports for annual and internal agency needs on the Federal workforce under EEO/MD-715.	Yes	This data is primarily FPPS related and PII includes name, ethnicity/race, and disability preference.
Inter-Governmental Personnel Act (IPA)	A web-based tool developed for the NSF and used by IBC HR staff to track intergovernmental	Yes	IPA provides tracking and management of IPA assignments for NSF employees and non-agency staff. This data is both FPPS/non-FPPS related. PII includes SSN, ethnicity, race, sex, name, date of birth, work

	personnel assignments between NSF and other organizations.		address, work phone number, organization and work assignment, college degree, grade point average, and college.
WebFPPS	A web-enabled presentation of FPPS. 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 the Office of Personnel Management (OPM) government-wide system of records notices (SORNs) including OPM/GOVT-1, General Personnel Records, December 11, 2012 (77 FR 73694); modification published November 30, 2015 (80 FR 74815); OPM/GOVT-7, Applicant Race, Sex, National Origin and Disability Status Records, June 19, 2006 (71 FR 35356); modification published November 30, 2015 (80 FR 74815), and the DOI SORN, DOI-85 Payroll, Attendance, Retirement, and Leave Records, July 19, 2018 (83 FR 34156).

Each Federal agency customer using FPPS 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.

☐ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Gender

☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: *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 dependent information; professional licensing and credentials; family relationships; age; involuntary debt (garnishments or child support payments); salary data; retirement Data; tax data; deductions; health benefits; allowances; union dues; insurance data; Flexible Spending Account; Thrift Savings Plan; information and contributions; pay plans; awards; debts owed to the government as a result of overpayment; refunds owed, or a debt referred for collection on a transferred employee or emergency worker; court order information; back pay information; user ID; T&A 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. Below is a list of sub-systems with additional PII.

- **ICS -** Entity's Contact Person Information in the Indirect Cost Proposal (ICP) Checklist, include: Entity Name and mailing address, Employer Identification Number (EIN), Point-of-Contact name and position title; Email address; Phone & fax numbers; Individuals who are sole proprietors may elect to use their Social Security number as their EIN.

- **PCS** - PII linked to an employee includes employee name, position title, branch code, slot number, and position status (temporary or permanent).

- **Datamart -** Datamart also collects Taxpayer Identification Number, Beneficiary information, Bond co-owner name(s) information, Family relationships, Involuntary debt (such as garnishments or child support payments), Court order information, Wage and benefit information, Back pay information, User ID, T&A data, Leave time information, ECI, Person Number, Person Number-Emergency and Person Number-Volunteer, Professional licensing and optional credentials such as sex identity. Federal agency customers may also upload files that contain PII specifically used by the agency.

- **FPPS NCC -** ECI, Medical and Family Leave, User IDs, Involuntary Debt (e.g. garnishments, child support), Court Orders, Back Pay.

- **IPA –** The name of the supervisor, home address, work address, work phone number, organization, work assignment, and the salary, benefit, and position title information of the employees on temporary assignment program are collected and used by NSF HR staff through OF 69 # (REV. 2-89) Form, *Assignment Agreement*, to track intergovernmental personnel assignments of NSF IPA employees, both incoming and outgoing. The sex, national origin, college degree, the name of the college, grade point average (GPA), national origin, race/ethnicity and SSN of the employee's temporary assignment program are obtained from IBC's Workforce Transformation and Tracking System (WTTS) which is an application where the users can assess the workforce management forms and fill in information. NSF staff manually enter the data into IPA after information from the employees on IPA assignment is obtained.

- **EEO/MD-715 -** 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.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records

☒ Third party source
☒ State agency
☒ Other: *Describe*

PII is also collected from state courts and records from colleges and organizations where the NSF employees on temporary assignment program for IPA.

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

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems: *Describe*
☐ Other: *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 such as 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, T&A, 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 OPM; 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.

EEO/MD-715 produces EEOC compliance reports as authorized and required by EEO/MD-715 and related directives.

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

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

Data is shared with IBC staff to support a full suite of human resources and payroll functions for DOI bureaus, offices, and IBC Federal agency customers. Data routinely provided to others is detailed in the DOI-85, Payroll, Attendance, Retirement, and Leave Records SORN, and other applicable SORNs. FPPS data is not used in any matching programs.

☒ Other Bureaus/Offices: *Describe the bureau/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.*

FPPS currently has interconnections or interfaces with more than forty Federal Government customers. Data is shared and reported to other Federal agencies, including the Department of the Treasury and OPM, as required for human resources, payroll, and tax purposes, and to Federal agencies for the purposes outlined in the routine uses in the DOI-85 Payroll, Attendance, Retirement, and Leave Records SORN published July 19, 2018 (83 FR 34156), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

PCS - Exclusively used by the SEC to manage position data.

IPA - This system is developed for NSF. The system allows NSF to input and report on both incoming and out-going temporary assignments that exist between NSF and other agencies or colleges.

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

FPPS currently has interconnections or interfaces with thirty-five state governments and fourteen cities and counties. This reflects the routine sending and receiving of interface files. These interfaces routinely change in quantity and data content. IBC maintains detailed documentation about each interface. FPPS data is not used in any matching programs.

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

Data is shared with IBC contractors that support FPPS.

IBC also shares data with Xerox and Output Services, Incorporated (OSI) as part of a service to prepare and print forms such as Leave and Earning Statements (LES), Form W-2s Wage

Statements, and other documents from FPPS to mail to Federal agency customer employees who have elected to receive printed hard copy forms. See the Printing and Postal Handling Services Contract PIA for details on the sharing of this data, which may be viewed on the DOI PIA website at https://www.doi.gov/privacy/pia.

☒ 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 and 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. Routine disclosures outside DOI are made pursuant to the routine uses outlined in the DOI-85 SORN. 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.*

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 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:

- 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.
- 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.).
- Fair Credit Reporting Release. This document requires the applicant’s signature in order for the DOI 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:

- SF-181, *Ethnicity and Race Identification*
- SF-256, *Self-Identification of Disability*

IPA - OF 69 # (REV. 2-89) Form, *Assignment Agreement,* used by NSF has Privacy Act Statement which gives the employees the opportunity to decline or consent to the collection and specific uses of their PII.

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

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

☒ Privacy Act Statement: *Describe each applicableformat.*

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*.

☒ Privacy Notice: *Describe each applicable format.*

Individuals are also provided notice on how their PII is managed during these personnel and payroll activities through the publication of this PIA; government-wide SORNs including OPM/GOVT-1, General Personnel Records, and OPM GOVT-7, Applicant Race, Sex, National Origin and Disability Status Records; and DOI-85 Payroll, Attendance, Retirement, and Leave Records. These SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

Users are provided with a security and privacy DOI Warning Banner when accessing the system.

☐ None

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

Certain personnel within IBC that are involved in the operations and maintenance of FPPS payroll operations, can manually retrieve information on an individual by:

- 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
- 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.

ICS - The contract proposal is retrieved by grant number.

PCS - Information is retrieved by FPPS transaction number or job position number.

Datamart - The primary retrieval method will be one of the pre-formatted analyses. Most analyses provide data on groups of personnel and not individuals; however, a few pre-formatted analyses report on individuals is based on SSN. End users also have the ability to submit ad-hoc analyses based on the following personal identifiers: Name, Citizenship, Gender, Birth Date, Group Affiliation, Marital Status, Other Names Used, Legal Status, Place of Birth, Security Clearance, Spouse Information, Financial Information, Medical Information, Disability Information, Education Information, Emergency Contact, Driver's License, Race/Ethnicity, SSN, Personal Cell Telephone Number, Personal Email Address, Home Telephone Number, Child or Dependent Information, Employment Information, Military Status/Service, Mailing/Home Address, Taxpayer Identification Number, Beneficiary Information, Bond co-owner name(s) information, Family relationships, Involuntary debt (such as garnishments or child support payments), Court order information, Wage and benefit information, Back pay information, User ID, T&A data, Leave time information, ECI, Person Number, Person Number-Emergency and Person Number-Volunteer, Professional licensing, and optional non-mandatory field such as sexual orientation or gender identification.

IPA - Data is used to create aggregate and summary information. In some cases, the data will be retrieved by SSN, name, and organization.

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 SORN.

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.

PCS - Reports are developed to list slots, positions, and the positions filled by the employees within SEC.

IPA - Reports that can be generated in IPA include: Employee, organization lists, assignment summary reports, organization rosters, EEO data, work assignment information for employees, salary, full-time/part-time status, total employee counts and separation reports used by NSF's HR staff, management, and workforce planning team to track intergovernmental personnel assignments. The users of IPA and the DOI Datamart administrator staff have access to these reports. DOI has no control on who the NSF share its reports with.

☐ No

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, 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.

The EEO information processed by this application is taken from Datamart, which collects EEO data from Federal employees through two 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 OPM that allows employees to initiate personnel and payroll actions and obtain payroll information.

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 T&A 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 T&A 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 EEX 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.

Federal records retention policies are followed for data in all FPPS MA applications. IBC retains records held in FPPS MA applications, belonging to customer agencies, in accordance with the General Records Schedule (GRS) and the Department of the Interior (DOI) Departmental Records Schedules (DRS), both approved by the National Archives and Records Administration (NARA), or with applicable agency records retention schedules when provided to the Interior Business Center (IBC) Records Manager. Customers are responsible for notifying IBC of all litigation or holds affecting their records held in FPPS MA applications. Retention and disposition may vary based on the type of record and needs of the agency. Customer agencies should provide IBC with the appropriate records retention schedule for their data and are responsible for managing their own records in accordance with the Federal Records Act.

Records are maintained in accordance with General Records Schedule (GRS) 1.0, Finance, and GRS 2.0, Human Resources, and Departmental Records Schedule (DRS) 1.2C, Retirement and Payroll Records Warranting Extended Preservation (DAA-0048-2013-0001-0008), which are approved by NARA. The system generally maintains temporary records, and retention periods vary based on the type of record under each item and the needs of the agency. DOI records schedules are available at https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-the-interior/rg-0048.

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 FPPS 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 deceased. 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 resource 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 GRS 1.0, Finance, GRS 2.0, Human Resources, and DRS 1.2C, Retirement and Payroll Records Warranting Extended Preservation (DAA-0048-2013-0001-0008).

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 privacy, security, and records management awareness training. DOI personnel authorized to manage, use, or operate the system information are required to complete additional privacy and security role-based training and sign DOI Rules of Behavior prior to accessing the system.

Although IBC hosts and processes payroll and personnel transactions on behalf of its customers, each customer retains ownership and control over its own records and is responsible for meeting requirements under the Privacy Act for the collection, maintenance and sharing of their records. Federal agency customers have published their own system of records notices for their employees' payroll and personnel related records hosted or processed by DOI. Individuals seeking access to, notification or correction of their records owned and maintained by external Federal agency customers must submit their requests to the employing Federal agency customer

that owns the records in accordance with the applicable SORN published by that Federal agency customer.

IBC also restricts access to a client's instance via firewall restrictions. IBC reviews the access of staff to customer data annually in accordance with the appropriate DOI use policy. Physical controls are also in effect to limit access to the IBC Denver Data Center. IBC conducts internal reviews to help ensure compliance with the Privacy Act law. IBC reviews staff access to customer data annually in accordance with the appropriate DOI use policy. FPPS maintains an audit trail of activity sufficient to reconstruct security relevant events. 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. Certain audit logs are sent to the OCIO ArcSight audit management tool and automatically evaluated and are reviewed manually as needed. Any suspected attempts of unauthorized access or scanning of the system are reported to IT Security.

IPA collects SSN, name, phone number, home address and position information from the employees through the OF-69 form. The identified privacy risks are moderate. The mitigation measures include a Privacy Act Statement about the purpose of the PII collection, the specific use of the PII, to whom the PII will be shared, and the voluntary nature of the data collection which is provided to the employees prior to filling in the information in the OF-69 form.

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.

☐ No

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

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

Datamart uses aggregate data to reduce the time to query large sets of data. Searches can be customized and saved by individual user. Access is managed by OCIO IT Security using the

Resource Access Control Facility (RACF) application. Datamart access is granted only to existing FPPS users. Datamart users might not use FPPS but must have FPPS access and authorities to use Datamart.

☐ No

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

☒ Yes: *Explanation*

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

☐ No

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

☐ Yes: *Explanation*
☒ No

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

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 (EEX)

EEX is an online employee self-service program made available by OPM 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 EEX 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 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 IRS after all data is verified. The payment is issued by the Department of the Treasury through EFTPS. The Department of the 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?

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

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

☒ No, data or processes are not being consolidated.

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

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*

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 a 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

Datamart access is managed by OCIO IT Security using a RACF application. Datamart access is granted only to existing FPPS users. Datamart users might not use FPPS but must have FPPS access and authorities to use Datamart.

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.

☐ No

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

☐ Yes. *Explanation*
☒ No

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

☒ Yes. *Explanation*

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.

☐ No

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.

FPPS audit and security logs produced by the various platforms can be used to support an "after-the-fact" investigation into questionable or unauthorized activities.

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 Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges

☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

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

(3) Administrative Controls. Indicate all that apply.

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

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

The Acting Associate Director and Deputy Associate Director, Human Resources Directorate, IBC 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, in consultation with the Office of the Secretary Associate Privacy Officer.

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 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 DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with DOI 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 in accordance with Federal and DOI privacy breach response policy.