# PRIVACY IMPACT ASSESSMENT

*(Rev. 2/2020)*
*(All Previous Editions Obsolete)*

Please submit your responses to your Liaison Privacy Official.
***All entries must be Times New Roman, 12pt, and start on the next line.***
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

| | |
|---|---|
| **System Name:** <br><br> **Human Resources Line of Business (HR LoB).** | |
| **Preparer:** <br><br> **Bobby Moore** | **Office:** <br><br> **OMS-ARM/AITSSS** |
| **Date:** <br><br> **06-12-2020** | **Phone:** <br><br> **202-564-7542** |

**Reason for Submittal:  New PIA__X__      Revised PIA____      Annual Review____   Rescindment ____**

**This system is in the following life cycle stage(s):**

Definition ☐  Development/Acquisition ☐  Implementation ☒

Operation & Maintenance ☒   Rescindment/Decommissioned ☐

**Note:  New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system.  For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).**

**The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**

## Provide a general description/overview and purpose of the system:

In June 2014, EPA officially migrated to the Department of Interior, Interior Business Center (DOI-IBC), for their HR and Payroll shared services.  Currently, the Federal Personnel Payroll System (FPPS) is a modern, mainframe-based, online, and real-time personnel and payroll system, providing personnel and payroll support to numerous Federal government agencies, servicing more than 240,000 individual accounts under the DOI HR LoB initiative.  The system is customer-driven, creating and generating the full life cycle of personnel transactions, enabling agencies to maintain records electronically.  The system handles all current

regulations including specialized pay, garnishments, special appointment programs, and more. FPPS is the EPA personnel and payroll accounting system of record.

FPPS has HRMS modules, also called bolt-ons, a System Integration Framework (HRMS SIF), and a set of standardized integration connectors. Currently the modules that are operational and used by EPA are: Workforce Transformation and Tracking System and Entrance on Duty System (WTTS/EODS) is a web-based Human Resources Management Suite (HRMS) and FedTalent for eLearning. Datamart/Analytics - Oracle's Business Intelligence Enterprise Edition (OBIEE) is Oracle 12c. These collection of systems above EPA refer to as HR LoB, all hosted by Interior Business Center (IBC).

The HR LoB is owned and operated by DOI/IBC as a Federal Shared Service. They are responsible for the hardware, software, general operating environment and as such most of the security controls relevant to keeping EPA information safe.

## Section 1.0 Authorities and Other Requirements

### 1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

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.).

### 1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. HR LoB has an SSP and an ATO that expires December 11, 2020.

### 1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

### 1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No. HR LoB is not maintained in a Cloud.

# Section 2.0 Characterization of the Information

*The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.*

**2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).**

HR LoB collects the following employee data elements: Name, Citizenship, Gender, Birth Date, Group Affiliation, Marital Status, Other Names, Used, Truncated SSN, Legal Status, Place of Birth, Other, 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, 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 HR LoB; person number-emergency which is a unique number identifying an individual within HR LoB for a leave share occurrence; and person number-volunteer which is a unique number identifying an individual within the HR LoB volunteer database.

**2.2 What are the sources of the information and how is the information collected for the system?**

The Sources of information comes from: Individuals; EPA records; Federal, State and Local agency; Third party source and State courts.

This Information is collected by: Paper Format; Face-to-Face Contact; Fax; Telephone Interview; Email; Web Site and Information Shared Between Systems (WTTS/EODS, EZHire).

**2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

No. However, HR LoB has integrated HRMS modules and interconnections with other Federal agencies; and EPA internal systems.

**2.4 Discuss how accuracy of the data is ensured.**

Data collected from new employees, such as name and SSN, is verified for accuracy using TALX for E-Verify or directly with the Social Security Administration. HR LoB 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 HR LoB.

## 2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

*Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.*

**<u>Privacy Risk</u>:**

There's a risk that users input data incorrectly or perhaps falsify in hopes of benefiting financially or disclosing privacy information to unauthorized users.

**<u>Mitigation</u>:**

HR LoB has audit features and additional controls that monitor authorized user activity. In addition, standardized audit reports are run to verify actions entered by users and validated by EPA and DOI that oversee the HR LoB.

# Section 3.0 Access and Data Retention by the System

*The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.*

### 3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

Yes. HR LoB has multiple levels of role-based access controls. The level of these access controls determines the security privileges assigned in HR LoB. Each level of security follows the separation of duties outlined in NIST guidance. The level of role-based security are listed below:

- **<u>User access</u>**: are employees who consists of Supervisor/Managers, HR Specialists and Report Writers. Access is granted via access request submitted electronically using HR LoB Access Request form in BAP. 1st level approval by Supervisor/Manager, 2nd level approval by PMO/RHRO. Privileges granted by Security Administrators within OHR as final approval.

- **<u>Security Administrator</u>**: employees in OHR who submits request for access using the HR LoB Access Request form in BAP. They provide user security privileges, maintain control tables and statistical analysis. Additional forms are submitted to DOI to inherit these security admin privileges designated by the EPA Data Custodian.

- **Administrator**:  employees at DOI who program and administer full system security controls maintained in FPPS.  Also, the Payroll/Personnel staff who audits payroll/personnel transactions.

## 3.2  In what policy/procedure are the access controls identified in 3.1, documented?

Access controls are documented on the HR LoB SharePoint site under HR System Access. The site provides guidance for users on security access procedures.

## 3.3  Are there other components with assigned roles and responsibilities within the system?

Yes.  Role-based access controls exist for the modules integrated in HR LoB.  The three levels of role-based security (User, Security, Administrator) defined in 3.1 exist for the following modules:

- Workforce Transformation and Tracking System and Entrance on Duty System (WTTS/EODS) - web-based Human Resources Management Suite (HRMS)
- FedTalent - eLearning
- OBIEE - Datamart/Analytics

## 3.4  Who (internal and external parties) will have access to the data/information in the system?  If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

EPA has Contractor users in HR LoB, and DOI has Contractors who support and maintain the FPPS system.  Their contracts on both sides include the appropriate FAR clauses.

## 3.5  Explain how long and for what reasons the information is retained.  Does the system have an EPA Records Control Schedule?  If so, provide the schedule number.

The retention of data in the system is in accordance with applicable EPA Records Schedules 0161 and 0553 as approved by the National Archives and Records Administration. Employee records are retained on magnetic tapes for an indefinite period. Hard copy records are maintained for varying periods of time, at which time they are disposed of by shredding.

## 3.6  Privacy Impact Analysis: Related to Retention

*Discuss the risks associated with the length of time data is retained.  How were those risks mitigated? The schedule should align the stated purpose and mission of the system.*

**Privacy Risk:**

There is a risk of maintaining large volumes of sensitive data and could be unintentionally accessed and compromised.

**Mitigation:**

EPA limits access to HR LoB to only those with a very clear need-to-know. HR LoB employs role-based access controls limit the access to a small, defined group of EPA personnel within OHR.

# Section 4.0 Information Sharing

*The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.*

### 4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

HR LoB shares data with its integrated HRMS modules and interconnections with 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 EPA-1, HR LoB.

### 4.2 Describe how the external sharing is compatible with the original purposes of the collection.

HR LoB external sharing is required for human resources, payroll processing and regulatory reporting for human capital management purposes.

### 4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

HR LoB has an Interconnection Security Agreements and/or Memorandums of Understanding between EPA and DOI using a secure Tier3 VPN connection. The EPA/DOI ISA+MOU is reviewed and updated annually by security officials at both EPA and DOI.

### 4.4 Does the agreement place limitations on re-dissemination?

The EPA/DOI Interconnection Security Agreements and/or Memorandums of Understanding has limitations addressing the re-dissemination of information in the agreement.

### 4.5 Privacy Impact Analysis: Related to Information Sharing

*Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?*

**Privacy Risk:**

There is a Risk that information shared outside of the agency could be intercepted during transmission.

**Mitigation:**

EPA has a Tier3 VPN encrypted connection between EPA and DOI which is used for transmitting information outside of the Agency.

# Section 5.0 Auditing and Accountability

*The following questions are intended to describe technical and policy‑based safeguards and security measures.*

### 5.1  How does the system ensure that the information is used as stated in Section 6.1?

HR LoB 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.

### 5.2  Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The Information Security and Privacy Awareness Training is required by all EPA employees and contractors each year.  The course includes information regarding policies and practices that EPA users should follow.  The Privacy Act of 1974 and Rules of Behaviors are also discussed.

### 5.3  __Privacy Impact Analysis__: Related to Auditing and Accountability

**Privacy Risk:**

There's a risk of not ensuring users are being held accountable for compliance with policy regarding access to HR LoB and complying with their intended security privileges.

**Mitigation:**

HR LoB have access controls and audit logs for users accessing information.  All EPA users of HR LoB must sign the Rules of Behavior when requesting access.  Required IT Security and Privacy Awareness training annually.

# Section 6.0 Uses of the Information

*The following questions require a clear description of the system's use of information.*

**6.1 Describe how and why the system uses the information.**

PII collected and maintained in HR LoB is used to support a full suite of human resources and payroll functions. HR LoB also processes PII to manage regulatory requirements such as specialized pay, garnishments, and special appointment programs. PII is used for fiscal operations for payroll, 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 EPA component for which the employee works or the agency for which the EPA emergency worker works; and for human capital management purposes.

**6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_ No___. If yes, what identifier(s) will be used.** *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)*

HR LoB authorized users may retrieve information on an individual employee using full name, SSN and Employee Common Identifier (ECI) - unique number identifying employees across Federal automated systems.

**6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?**

Security controls used to protect personal sensitive data in HR LoB are commensurate with those required for an information system rated moderate for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 4.

Administrative Safeguards

- EPA personnel are required to complete annual agency Information Security and Privacy training. EPA personnel are instructed to lock their computers when they leave their desks.

Technical Safeguards

- Electronic records are restricted to authorized users with appropriate security privileges, including the use of 2-factor PIV Card authentication. Web-based connections are Tier3 VPN encrypted sessions between EPA and DOI. The database is maintained behind a firewall.

Physical Safeguards

- These records are maintained in controlled access areas. Identification cards are verified to ensure that only authorized personnel can access.

### 6.4    Privacy Impact Analysis: Related to the Uses of Information

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

**Privacy Risk:**

There is a risk that information collected and maintained in HR LoB could be misused.

**Mitigation:**

To protect access to HR LoB information authorized EPA users who complete the Rules of Behavior, for HR Access follow the guidance on the HR LoB SharePoint site for user role and responsibilities.  HR LoB also has an audit trail of all users that's reviewed in the event of misuse.

\*If no SORN is required, STOP HERE.

*The NPP will determine if a SORN is required.  If so, additional sections will be required.*

# Section 7.0 Notice

*The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.*

### 7.1    How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

### 7.2    What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

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. 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 HR LoB.

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 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:

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

## 7.3    <u>Privacy Impact Analysis</u>: Related to Notice

*Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.*

**<u>Privacy Risk</u>:**

There is a risk that HR LoB users aren't being made aware of the privacy notice prior to their information being collected.

**<u>Mitigation</u>:**

EPA employees review and fill out official forms that contain Privacy Act Statements notifying individuals of the authority, purpose and uses of the information they provide during employment. Employees are also made aware of their rights during the required IT Security and Privacy Awareness training annually.

# Section 8.0 Redress

*The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.*

## 8.1    What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

## 8.2    What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

## 8.3    <u>Privacy Impact Analysis</u>: Related to Redress

*Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.*

**<u>Privacy Risk</u>:**

None.  HR LoB will leverage the established procedures to provide redress.

**<u>Mitigation</u>:**

None.