# 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:** W2 Wage Statements/Leave and Earning Statements (W2/LES)
**Date:** May 6, 2021
**Bureau/Office:** Office of the Secretary/Interior Business Center
**Bureau/Office Contact Title:** DOI Departmental Offices Associate Privacy Officer

**Point of Contact**
**Email:** Danna_Mingo@ios.doi.gov
**Name:** Danna Mingo
**Phone:** 202-208-3368
**Address:** 1849 C Street NW, MIB 7112, Washington, D.C. 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
- ☒ Volunteers
- ☐ All

☐ No:

**B. What is the purpose of the system?**

The Department of the Interior, Interior Business Center (IBC) has a service contract with Xerox and Output Services, Incorporated (OSI) to prepare and print forms such as Leave and Earning Statements (LES), Form W-2s Wage Statements which are mailed to the Federal agency customer employees who have elected to receive printed hard copy forms. The Xerox/OSI contract will include printer and postal finishing services such as folding, envelope stuffing, and delivery of final product to U.S. Postal Service (USPS) facilities. The IBC provides payroll services to numerous Federal agency customers and hundreds of thousands of Federal employees, including providing LES, W-2 Wage Statements in electronic and paper format. This

contract requires temporary storage and processing of Federal Personnel and Payroll System (FPPS) data required to perform printing services by Xerox/OSI. Privacy risks associated with the use of FPPS system were addressed in the FPPS PIA.

**C. What is the legal authority?**

The Office of Management and Budget Circular A-127, Policies and Standards for Financial Management Systems, authorized the purchase or development of FPPS. 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. 3512et seq.); and 31 U.S.C. Chapter 11. Authority for maintenance of the system: 5 U.S.C. 5101, et seq; 31 U.S.C. 3512. Personnel records are per 5 CFR part 253 and 5 CFR part 297.

**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: Assess privacy risk associated with contract with third party to process and mail LES, W-2 Wage Statements and other documents.

**E. Is this information system registered in CSAM?**

☒ Yes: UII Code: 010-9999991241 24-00-01-01-01-00, Federal Personnel and Payroll System
☐ No

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

| Subsystem Name | Purpose | Contains PII | Describe |
|---|---|---|---|
| **None** | **None** | No | **N/A** |

**G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?**

☒ Yes:

DOI-85, Payroll, Attendance, Retirement, and Leave Records - 83 FR 34156 (July 19, 2018). The DOI-85 SORN does not cover the records of the IBC customers. The customers are required to develop and publish their own SORN for their agency records.

☐ No

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

☐ Yes:
☒ No

## Section 2. Summary of System Data

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

☒ Name
☒ Truncated SSN
☒ Financial Information
☒ Other: Taxes and Wages
☒ Social Security Number (SSN)
☒ Employment Information
☒ Mailing/Home Address

Any information that may be included on a W-2 form or other required document such as earnings, pay/salary; Federal, state and other taxes; benefit deductions and contributions (both employee and agency); pay plan/grade/step; Fair Labor Standards Act class; service computation date; leave balances and accruals; Thrift Savings Plan loan deductions and tax deferrals; Health Savings Account deductions; charity deductions/contributions; association dues deductions; discretionary allotments; savings allotments; Old-Age, Survivors, and Disability Insurance deductions; Medicare deductions; garnishments; dependent care benefit amounts; employer identification number.

**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: State courts for garnishments

**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 (Employee Express to FPPS)
☒ Other:

Information is provided by the employee to the agency's servicing personnel office via Workforce Transformation Tracking System Entrance on Duty System.

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

The data will be used to prepare and print forms such as LES, Form W-2 Wage Statement documents to mail to Federal agency customer employees who have elected to receive printed hard copy forms via mail. The service will include printing, folding, envelope stuffing, and delivery of the final product to USPS facilities. Data is deleted by the contractor after printing and mailing services are completed.

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

☐ Within the Bureau/Office:

☐ Other Bureaus/Offices:

☐ Other Federal Agencies:

☐ Tribal, State or Local Agencies:

☒ Contractor:

OSI (subcontractor on an IBC contract with Xerox) will provide temporary storage of the data required for printing various forms (e.g., LES, W-2, etc.) which are then mailed by OSI using USPS to DOI employees and IBC FPPS customers.

☐ Other Third-Party Sources:

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

☒ Yes:

The employee has the right to decline however, if the information is not provide the employee will not get paid and will not receive there Leave and Earning Statements and W2 which is required by law.

☐ No:

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

☒ Privacy Act Statement:

Privacy Act Statements that are provided on the various IRS forms and OPM personnel forms.

☒ Privacy Notice:

DOI-85, Payroll, Attendance, Retirement, and Leave Records - 83 FR 34156 (July 19, 2018)

☐ Other:

☐ None

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

FPPS generated files for W2 & LES are retrieved by the OSI vendor via Secure Transport. File name identifier for W2's IFIL0291 and LES is IFIL0288. In order to provide the electronic records to OSI records are retrieved by the file name.

**I. Will reports be produced on individuals?**

☐ Yes:

☒ No

## Section 3. Attributes of System Data

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

The data collected are considered a source document. The source document is created by the servicing personnel office, and the accuracy of the data is based on the information provided by the employee. The servicing personnel office is responsible for ensuring the information that is manually entered in the FPPS is accurate prior to the secure file transfer of the data being sent to OSI.

**B. How will data be checked for completeness?**

Prior to the OSI print vendor getting the file for processing. Employee information is entered into FPPS, Employee Express and Workforce Transformation Tracking System (WTTS) and a pop-up window appears to the end user that makes the user validate what they input is correct and complete prior to submitting. Certain edits are in place for these systems to not allow the end user to input certain characters or numbers that are not applicable to the field that is being updated.

The data files are checked in FPPS as described in the FPPS PIA and below.

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 FPPS client is responsible for implementing additional procedures to verify the accuracy and completeness of the payroll information that is provided on behalf of their agency. In addition, servicing personnel staff and client managers will perform various functions to check data for completeness, such as the following:

- Reviewing and editing data to ensure that all required fields are populated, complete, and in conformance with Federal government personnel rules.
- Reviewing records to validate the existence and completeness of time and attendance records for all active employees for the current pay period.
- Editing payroll transactions to ensure all required fields are populated and complete.
- Monitoring time and attendance records to ensure that all time and attendance 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).**

The data sent to OSI is from FPPS and is current at the time it is provided as it must be maintained in a current state in order to perform the system's human resources and payroll functions. In general, each agency client that provides data for use in FPPS is responsible for ensuring the data is up to date and for establishing procedures for updating data. The system also employs various data validation controls to ensure that data entered into the system is current. These controls will notify Data Custodians if certain data has been held in excess of a certain amount of time without an update.

For data files provided to OSI, FPPS runs a number of processes daily and at other times (e.g., close of business, paid dailies, one-time adjustments, time and attendance collection, pay calculation, etc.) to compile transactions and to ensure all personnel and payroll data is current.

FPPS edits and validations, and interface file agreements, which help to ensure data is current, are contained in various design documents, the online help system, and throughout FPPS code.

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

The records are copies from DOI and customer records. The original records are maintained in FPPS under the DOI records schedule, DAA-0048-2013-0001-0005, Long Term Human Resources Records. The records are cut off at the end of the tax year and destroyed 7 years after cutoff. The copied data is used for printing and mailing specific forms and is retained and disposed of at the end of the contract performance as indicated below.

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

OSI will destroy all IBC data in accordance with the Department's DI 1941 destruction process. Procedures related to disposition and retention are documented within the contract. OSI will sanitize any information system media containing IBC data in accordance with applicable organizational and/or federal standards and policies by using an approved disk wipe utility. The utility must be approved by DOI information technology (IT) Security personnel and be in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. OSI will maintain a log of all IBC data files showing, at a minimum, date received, date printed, date to USPS, date destroyed, and the log will show evidence of regular management review. The log will be reviewed for accuracy, provided to the Office of the Secretary (OS) Records Office for approval, and retained for 7 years after the destruction, and OSI will provide a copy of the log to the COR by the 5th day of each month.

**F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.**

There is a risk to individual privacy at different stages of the information lifecycle. The risk/sensitivity level designation of the activities performed under this contract is Moderate Risk. There is a risk an OSI server holding FPPS data could be compromised which could result in exposure of PII about individuals whose data is being processed by OSI. This risk is mitigated by several controls. The Xerox/OSI contract contains stringent security requirements to identify risk associated with using OSI systems. Appropriate privacy safeguards are implemented to protect DOI and FPPS customer data.

OSI is required to obtain an Authority to Operate based on an Assessment & Authorization performed by a DOI-approved assessor and must be formally approved by the DOI FPPS Authorizing Official (AO) prior to allowing FPPS data to be processed by OSI.

DOI requires that OSI follow the ongoing authorization process and associated continuous monitoring requirements as prescribed by the Office of Management and Budget (OMB) and NIST. OSI will participate in assessments as to the effectiveness of required controls on an ongoing basis to inform the AO's decisions regarding the continued use and operation of a system where FPPS data is located.

OSI must follow all relevant NIST Federal Information Processing Standards (FIPS) Publications and SP to include, but not limited to, FIPS Publications 199 and 200, SP 800-39, 800-37, 800-137, 800-60, 800-53, 800-53A, 800-34, 800-30, and 800-18. OSI must also comply with all DOI IT security and privacy policies and standards including, but not limited to, Departmental Manual (375 DM 19); DOI Security Control Standards (SCS) and the DOI Privacy Impact Assessment (PIA) Guide.

OSI will be required to ensure compliance with the privacy and security control requirements of the current version of NIST SP 800-53, which are applicable to the security categorization of the data or system. FIPS 199 and the NIST SP 800-60 will be used to determine information types and security categorizations. FPPS data has been determined to have a Moderate classification.

OSI must have a robust security architecture to protect the Confidentiality, Integrity, and Availability of the FPPS data contained within their system. This architecture shall include, but are not limited to, items such as, packet-filtering firewalls, intrusion detection/prevention systems (IDS/IPS), security technical implementation guides for the secure installation of operating systems and applications, anti-virus/anti-malware, patch management, configuration and change management, and other tools, techniques, policies, procedures, and processes to secure the environment.

The OSI system that receives the secure file transfer must be scanned monthly with a vulnerability analysis tool that is comparable with the software in use by DOI at the time. All safe or non-destructive checks must be turned on, and an electronic copy of each report and session data will be provided to the COR or designee. At least annually, all high and moderate risk impact systems and systems accessible from the Internet must be independently penetration tested, and electronic and hard copy reports of penetration test results will be provided to the COR or designee. DOI may conduct unannounced and prearranged independent vulnerability scans using government personnel or another contractor. Pursuant to the OSI Interconnection Security Agreement (ISA) with DOI, OSI will comply with all ISA security requirements, including conformance with NIST standards. A secure VPN connection will be used for initial data transfer. Subsequently a dedicated circuit between DOI and OSI will be established to complete printing services. Information passed through the interconnection is protected with the use of FIPS 140-2 approved encryption mechanisms.

All OSI personnel who may have access to IBC data will sign a non-disclosure agreement. The IBC considers information obtained and used as part of these services to be Controlled Unclassified Information. OSI will take all reasonable precautions to ensure sensitive information about IBC or its clients is not divulged or inappropriately released to any other organization (outside the IBC) without written permission from the IBC.

All OSI personnel with access to DOI data will be subject to IBC security and privacy policies and procedures.

Background investigations are required for OSI personnel who have physical or logical access to DOI data, or otherwise handle or process DOI data, and will be performed by the Office of Personnel Management (OPM) unless otherwise specified by OPM.

## 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:

IBC is legally required to print, and mail certain documents forms to individuals whose payroll is calculated by FPPS. IBC only provides the data necessary to print and mail these required documents.

☐ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

Not applicable as new data is not being created.

**F. Are the data or the processes being consolidated?**

☐ Yes, data is being consolidated.

☐ Yes, processes are 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
☒ Contractors
☐ Developers
☐ System Administrator
☒ Other:

IBC will transmit data by secure connection as described in the ISA. OSI personnel are required to have access to the data files in order to print and mail the forms. The individuals are business managers, operations personnel, system analysts, and developers. Access is granted by IBC in accordance with the contract requirements for background investigation and security policy compliance.

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

Authorized OSI personnel have access to the data required to print and mail documents. Access is on a need-to-know basis to perform these contract services.

**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.

OSI is performing these services under contract and Privacy Act clauses are included in the contract.

☐ 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.

☒ No

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

☐ Yes.

☒ No

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

N/A

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

N/A

**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.

(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.

(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.

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

The FPPS System Owner and System Manager are responsible for protecting the privacy of individuals for this system and for addressing Privacy Act requests or complaints. Procedures for submitting Privacy Act requests or complaints are outlined the published Privacy Act system of records notice, DOI-85, Payroll, Attendance, Retirement, and Leave Records - 83 FR 34156 (July 19, 2018).

**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 System Owner and System Manager are responsible for assuring proper use of data in FPPS under the OSI contract. All individuals with access to the data are responsible for reporting the loss, compromise, unauthorized disclosure or unauthorized access of this data. This responsibility is described in mandatory Rules of Behavior and other documents and is covered in mandatory IT security and privacy training and in IBC's ISA with OSI.