Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 368
System Name: ePayroll (PAR)
CPO Approval Date: 4/15/2022
PIA Expiration Date: 4/14/2025

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Monica Shackelford

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
ePayroll (PAR)

B: System, application, or project includes information about:
Federal Employees

C: For the categories listed above, how many records are there for each?
Approximately 26,000 federal employee records.

D: System, application, or project includes these data elements:

- Name and other biographic information (e.g., date of birth)
- Contact Information (e.g., address, telephone number, email address)
- Social Security Number and/or other government-issued identifiers
- Financial Information
- User Information to include Username and Password

Overview:

The PAR system is a major application that provides complete payroll functionality for an employee's entire service life, from initial hire through final payment at separation and submission of retirement records to the Office of Personnel Management. PAR is a fully automated, nationwide, civilian payroll system. GSA professionals developed, designed, programmed, implemented, and maintain PAR at GSA's Financial Management and Human Resources IT Services Division, Heartland Region, Kansas City, Missouri. It provides a full range of payroll services for approximately 19,000 employees, which includes GSA and 39 independent agencies or presidential commissions.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
GSA's legal authority for collecting the PAR information is contained in 5 U.S.C. Part III, Subparts D and E, 26 U.S.C. Chapter 24 and 2501, and E.O. 9397. See the Payroll Accounting and Reporting (SORN) GSA/PPFM-9.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
https://www.federalregister.gov/documents/2008/04/25/E8-8920/privacy-act-of-1974-notice-of-updated-systems-of-records

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.
Yes, ICRs have been approved by OMB for the forms that collect information from employees. Fillable forms available to GSA employees (e.g., SF2809, SF2810, SF2817; TSP1 and TSP1c) include a Privacy Act Notice that describes the legal authority for collecting the information; the primary and permissive routine uses of the information; and the potential consequences of not providing the requested information. These forms also include the OMB control numbers and revision dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
The GSA has a NARA-approved records retention schedule. The PAR financial data is retained for 6 years 3 months as required by NARA. An employee's historical records are maintained in the PAR database for 18 months after separation and are then purged from the database.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
PII is required for PAR to process payment, taxes, etc. for Federal employees. PAR needs to collect name, date of birth, and SSN because that information provides the best matching capabilities against the identity verification. Collection of SSNs is required by the Department of Treasury and IRS policy, rules and/or regulations. Any reporting that requires the identification of an employee is normally done using the name, SSN, and sometimes the date of birth.

3.2: Will the system, application, or project create or aggregate new data about the individual?
Yes

3.2 Explained: If so, how will this data be maintained and used?
PAR calculates pay, taxes, withholdings, deductions, etc. in order to ensure Federal employees are accurately paid on a bi-weekly basis.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
PAR users are required to have background investigations prior to obtaining access. They must also request access and are granted only the roles and permissions necessary to perform their duties. Users cannot directly access PAR remotely; all work must be done within the GSA boundary or network using VPN/VDI. The office location is only accessible with the use of their HSPD-12 card. Database links are secure and PAR uses secure FTP, agency/company secure portals, specific IP authentications, Connect Direct, by logging into an agency's server via Putty, STS, ESB, or an encrypted password protected email attachment for sending out/submitting files. Multi-factor authentication has enabled utilizing jump servers. The PAR data is protected by Payroll Service Branch through roles and permissions which allow only enough access for authorized users to perform their duties. The PAR servers are housed within the GSA firewall. Data sent outside the GSA firewall is encrypted and transmitted over secure FTP, an agency/company secure portal, a specific IP authentication, Connect Direct, by logging into an agency's server via Putty, STS, ESB, or an encrypted password protected email attachment.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
No, PAR does not monitor the public, GSA employees, or contractors.

3.5 What kinds of report(s) can be produced on individuals?
No. PAR does not monitor federal employees, contractors or the public. It is used to pay Federal employees.

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
Some PAR reports for internal GSA use, for example validation reports, must contain identifying information, including SSNs to ensure that the proper individuals are receiving the proper payments. However, any external reports created by PAR aggregate or mask information in order protect employee sensitive information.

3.6 Why Not: Why will the data not be de-identified?
Some PAR reports for internal GSA use, for example validation reports, must contain identifying information, including SSNs to ensure that the proper individuals are receiving the proper payments. However, any external reports created by PAR aggregate or mask information in order protect employee sensitive information.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Federal Agencies

4.2How: If so, how will GSA share the information?
The PAR outputs that GSA uses are comprehensive payroll reports; accounting distribution of costs; leave data summary reports; each employee's statement of earnings, deductions, and leave every payday; State, city, and local unemployment compensation reports; Federal, State, and local tax reports; Forms W-2, Wage and Tax Statement; and reports of withholding and contributions. For the Office of Human Resources Services, outputs include data for reports of Federal civilian employment. The system also provides data to GSA staff and administrative offices to use for management purposes. The employee's name, SSN, date of birth, and home address are reported to SERCO on behalf of the Thrift Savings Plan (TSP) which invests the employee's TSP, mails statements to the employee, and provides TSP loans. The employee's name, SSN, and address are sent to IRS for tax payments, to meet Affordable Care Act requirements, and W-2 data reporting. The employee's name, SSN, and address are sent to SSA for tax information reporting. The employee's name, SSN, and date of birth are sent to OPM with the retirement data upon separation. The employee's name, SSN, home address, and banking information are sent to OPM's Employee Express so the employee can retrieve their own pay and leave data, W-2s, and make changes to their home address and banking information. The employee's name, SSN, and address are sent to the taxing authorities for State and local entities. PII data is also sent to the following agencies/companies, on an as-needed basis and in accordance with the "routine uses" provided for in the PAR SORN, GSA/PPFM-9: - American Federation of Government Employees (AFGE) receives union dues files for union members only. -Bureau of Public Debt (BPD) receives client payroll accounting files, for example lists of employees with a debt. -Department of Labor (DOL) receives child support payments and continuation of pay statement (workmen's compensation). -Health Benefits Insurance Carriers (e.g. BlueCross/BlueShield, Aetna, HMOs) receive health insurance premiums. -National Business Center, Department Of Interior (DOI) receives aggregated accounting files. -National Credit Union Administration (NCUA) receives agency accounting files and 401k data. -Office of Personnel Management (OPM) receives employee retirement information, health insurance information, life insurance information, agency accounting files, and labor distribution data. -Railroad Retirement Board (RRB) receives agency accounting files, labor distribution data, and transit benefit data. -TALX Corporation receives unemployment and employment verification information. -Treasury Department receives payment files with banking information and treasury salary offset program file (debt collection). United States Department of Agriculture (USDA) receives certain agencies' client payroll accounting files and health benefits information. Veterans Administration (VA) receives an Occupational Safety and Health Agency (OSHA) extract file. Wells Fargo receives National Credit Union Administration (NCUA) 401k data. All data sent outside GSA is sent via secure FTP, agency/company secure portals, specific IP authentications, Connect Direct, by logging into an agency's server via Putty, STS, ESB, or an encrypted password protected email attachment.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
PAR sends and receives time and attendance data to/from the GSA HRLINKS system via the Labor Data (LABD) warehouse. PAR sends and receives Child Care Subsidy (CCS) data to/from the OCFO Accounts Payables office. PAR receives volunteer leave data from the Volunteer Leave Transfer Program (VLTP) application.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

4.4WhoHow: If so, who and how?

Please refer to 4.3 for a list of PAR data exchanges. GSA leverages MOUs or ISAs for these connections. All external systems have an Assessment and Authorization (A&A) validated via the MOU/ISA. Each MOU/ISA has an agreement to notify GSA IT Service Desk in case of any suspected or confirmed security incidents involving PAR data.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?
Please refer to 4.3 for a list of PAR data exchanges. GSA leverages MOUs or ISAs for these connections. All external systems have an Assessment and Authorization (A&A) validated via the MOU/ISA. Each MOU/ISA has an agreement to notify GSA IT Service Desk in case of any suspected or confirmed security incidents involving PAR data.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
PAR leverages HRLinks and EEX, employee driven applications to ensure accuracy personal payment information. PAR does not allow duplicate agency/SSN combinations. Some data entered is required to be in a certain format. Many validation edits are performed against reference tables. Message/error reports are generated for the Payroll Services Branch to research/correct prior to running the final pay calculation every two weeks. Separation of duties is a requirement handled by the role(s) and permissions an employee with access to PAR is assigned. Queries are generated and reviewed to prevent payroll fraud.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Data access is restricted with the use of roles and permissions within the PAR application. Table changes in the PAR application are captured including: the previous data, what the data was changed to, who changed it, and the date/time it was changed. The Payroll Services Branch employees are instructed to not update their own data except through the OPM EEX application. Queries are run and checked to audit this safety measure. The PAR roles are defined: Role - Authorized Privileges and Functions Performed APPDETECTIVE_ROLE - Role for AppDetective database security audit scan and has query only access to certain Oracle data dictionary tables/views in database. DBA - Role only applicable to authorized staff to allow database administration. IMP_FULL_DATABASE - This role is the default Oracle database import role. LABOR_DIST - This role will allow the user query privileges to a group of tables in PAR to perform the labor distribution processing. OSU_ROLE - Allows insert, select, update, and delete from the temporary Pay and Leave message tables. PAR_ACCTG - This role will have update, delete, and insert ability into accounting, budget, and month end PAR tables in order to maintain the Accounting and month end processes. Also allows user to execute PAR reports. PAR_CONNECT - This role allows the user the ability to connect to the PAR database. PAR_CONTROL - This role will have create session, create view, and update, insert and delete privileges on a limited number of PAR tables in order to perform the balancing and disbursement of each bi-weekly payroll. PAR_DEVELOPER - All accesses are select only. PAR_ETAMS - This role will have insert, update, delete, and query from PAR tables used in the PAR T&A processing. PAR_HARP - This role allows insert, update, delete, and query privileges to History Access Reports for Payroll (HARP) tables in order to maintain the process. PAR_HARP_QUERY - This role allows query privileges to the HARP tables. PAR_HR_AUDIT - This role allows query privileges to the HR tables that provide an audit of what was processed. PAR_MAINTENANCE - This role's users allow software programs to create, modify and alter tables and views within the production database. PAR_MANAGER - This role allows the Payroll Managers to have query privileges on most PAR tables and PLS Message approval privileges. PAR_MONTHEND - This role grants update and query privileges to the table that controls month end reporting. PAR_OWNERS - No one's userid is under this role. It's users represent the owner schema that the PAR tables have been placed under. PAR_PARTAX - This role allows insert, update, delete and query privileges to the tax formulas. PAR_PDW - This role allows query privileges to the Employee Data Store (EDS) tables and insert, update, query, and delete to the process control table. PAR_PDW_QUERY - This role allows query privileges to the PAR Data Warehouse (PDW) tables. PAR_PEGASYS - This role allows insert, update, and System delete privileges to the PEGASYS batch tables. PAR_PLH - This role allows execute to several PAR Reports and insert, update, query, and delete privileges to the Pay and Leave History (PLH) tables. PAR_PRODUCTION_IDS - This role is used to run the production programs. PAR_QUERY - This is a query role with create session and query

privileges on the PAR_EDS tables. This role will be granted to many other roles. PAR_QUERY_ALL - This is a query role that allows query of all database objects owned by PAR. PAR_SCRIPT_ACCESS - This role allows the scripts to run and sends out the automated email messages. PAR_SEMI_MONTHLY - This role is used by the Forms application to control who has access to adjust Flexible Spending Accounts and Long Term Care. PAR_SLTAX - This role allows the users to verify the State and local tax formulas have been implemented in production. PAR_STUDENT_LOANS - This role has insert, update, and query privileges to the PAR tables necessary for processing student loans. PAR_SUPERVISOR - This role allows the Payroll Operations Supervisors to have create session, and update, insert, query and delete privileges on most PAR tables. PAR_TBLUPDATE - This role will allow designated users insert, update, query, and delete privileges to reference tables and certain HR and retirement tables. PAR_TECH - This role will have create session, create view, and insert, update, query and delete privileges on T&A tables; insert, update, and query privileges on EDS and History tables; execution privileges on PAR reports; query privileges on disbursement tables and PLH tables; and insert, update, query, and delete privileges on a few reference tables. This role will allow the designated Payroll technician to update the necessary tables in PAR to keep the database current and up-to-date. PAR_TPP_MSG - This role allows the users to input and approve the messages that are on the Employee's Pay and Leave Statements. PAR_UPDATE - This role allows unique users in the Payroll Operations Office insert, update, query, and delete privileges to make the necessary changes to correct data when there are program problems that require data to be corrected. PAR_WEB - This role will allow Web Site users insert, update, query, and delete privileges to the EDS tables; execute privileges to PAR reports; query privileges to the PDW, a select few reference, and the PLH tables; and insert, update, query, and delete privileges to the PLS messages tables. PAYABLES - This role allows users from Accounts Payables query privileges on a few EDS and reference tables. RUN_PROCEDURES - This role allows the user to execute the HR procedures and other accesses to process the transactions from HR. SELECT_CATALOG_ROLE - Role only applicable to authorized staff at IC and has query only access to any Oracle data dictionary tables/views in database. SHAREDLV_ROLE - This role is only to be used by the system account via the database link to the PAR system. It allows users to input Shared Leave information via the HR Shared Leave application. THWEB_BATCH - This role allows query privileges to the PLH views and insert, update, and query privileges to the PLS message tables.

6.1b: What is the authorization process to gain access?
Data access is restricted with the use of roles and permissions within the PAR application.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
12/15/2021

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
PAR is a closed system limited to GSA network access only. Payroll Services branch works in a guarded federally leased building that requires PIV card access. The PAR infrastructure is located in a secure federally owned data warehouse. Logical restrictions apply to PAR via Firewalls, multi-factor authentication, Role based user access, passwords, etc. Regular monitoring of systems occurs via logging and monitoring of system use, data changes, vulnerability scanning, and annual audits and assessments. All data is encrypted at rest utilizing Oracle TDE and encrypted in transit via TLS 1.3.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
PAR leverages the GSA Incident Response (IR) guide. In case of a suspected security incident/ breach of PII, the IT Service Desk as well the Privacy Officer and Incident Response team are notified immediately to start investigations.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?

The information collected and utilized by PAR is necessary for payroll processing, for example making direct deposits and ensuring appropriate deductions.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
ISSO is to fill

7.2: What are the procedures that allow individuals to access their information?
Individuals do not access PAR data directly. Instead, individuals may update their personal information via HRLinks which then transmits updates to the PAR system and which they can review in EEX.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
Individuals do not access PAR data directly. Instead, individuals may update their personal information via HRLinks which then transmits updates to the PAR system and which they can review in EEX.

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
All employees are required to take the IT Security Awareness and Privacy 101, Privacy 201 training, and Sharing in a Collaborative Environment training annually. The Rules of Behavior is included in the required security training.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
PAR is subject to annual Financial Statement Audits, Statement on Standards for Attestation Engagements (SSAE 18) audits, OIG audits, OMB A-123 audits, as well as annual FISMA Self Assessments, and 3 year Authorization and Accreditation assessments.