Payroll, Accounting and Reporting

Privacy Impact Assessment

12/28/2018

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

SECTION 2.0 OPENNESS AND TRANSPARENCY

SECTION 3.0 DATA MINIMIZATION

SECTION 4.0 LIMITS ON USES AND SHARING OF 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?

4.2 Will GSA share any of the information with other individuals , Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about PAR. *IC* may, in the course of PAR, 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

Payroll, Accounting and Reporting (PAR)

System, application or project includes information about

Federal employees

System, application or project includes

- *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*

[1] OMB Memorandum Preparing for and Responding to a 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.

PAR shares payroll data as required with the United States Department of Agriculture (USDA), Department of Labor (DOL), Office of Personnel Management (OPM), Social Security Administration (SSA), Unions, Bureau of the Public Debt (BPD), the Federal agencies GSA payrolls, Internal Revenue Service (IRS), Department of Interior (DOI), BENEFEDS, SERCO North America, Inc., State and local tax authorities, TALX Corporation, Department of the Treasury, Veterans Administration (VA), Wells Fargo, as well as with all of the individual employees the GSA payrolls.

Overview

The Payroll Accounting and Reporting (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. The Office of Corporate IT Services, Financial Management & Human Resources IT Services Division is the owner of PAR. GSA was selected as one of four agencies to payroll the entire Executive Branch.

A hire transaction and employee benefit transactions are received from the HR system and updated in PAR. Employee banking, address, and other payroll data is collected from the employee and updated in PAR. The employee's payroll is calculated every two weeks and disbursed. Once the employee separates, the retirement data is sent to the Office of Personnel Management. The employee's historical records are maintained in the PAR database for 18 months after separation and are then purged from the database.

The PAR data is protected by Payroll Service Branch users having roles and permissions which allow only enough access 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 file transfer protocol (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.

Data shared within GSA and externally is encrypted. No employees outside GSA have access to directly update the PAR system. Employees outside GSA who receive PAR data only receive the data necessary to perform their duties.

Historically, Payroll Services Branch employees manually distribute payroll reports to customer agencies to assist them with reconciling their payroll accounting entries. The PII information in these files is needed to reconcile with the payroll accounting entries generated. This report distribution occurs bi-weekly, monthly, quarterly, and yearly. Due to the time consuming nature of manually distributing payroll reports, GSA is pursuing the use of a leading Robotic Process Automation (RPA) vendor that provides a software platform to help efficiently automate business processes. The Payroll RPA will distribute payroll files via email to Point of Contacts (POCs). Required formats and POCs are specified in the "File Distribution List." The PII stored in most of the files include a combination of the employee's name, SSN, their earnings, and the contributions made on the employee's behalf.

This PIA applies to both direct access to PAR via traditional means and processing of payroll data extracted from PAR reports using a Payroll RPA (a.k.a., software bot or bot).

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

The PAR system provides complete functionality for an employee's entire service life from initial hire through final payment and submission of retirement records to the U.S. Office of Personnel Management (OPM). The system holds payroll records, and includes information received by operating officials as well as personnel and finance officials administering their program areas, including information regarding nonsupport of dependent children. The system also contains data needed to perform detailed accounting distributions and provide for tasks such as mailing checks and bonds and preparing and mailing tax returns and *reports.*

1.2 What legal authority and/or agreements allow GSA to collect 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.

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

Yes. Please refer to the PAR SORN, GSA/PPFM-9.

1.4 Has any information collection request (ICR) been submitted to or approved by OMB? If yes, 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.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

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.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

GSA mitigates potential risks related to the purpose of collection by publishing this PIA on its website as well as through the use Privacy Act Statements on the forms that collect the information from employees.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Certain personal information for federal employees is available via the Freedom of Information Act (FOIA) and in accordance with GSA's Data Release Policy. However, personally identifiable information (PII) which is required for Payroll transactions is kept confidential. Federal employees consent to disclose their personal and transactional information in order to be paid electronically.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

No. As discussed above, the system and the forms used to collect information present Privacy Act Statements to users that explain how and why the information is collected and used.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

All Federal employees payrolled by GSA.

3.2 What PII will the system, application or project include?

Please see section 1.1, above. Collection of SSNs is required by the Department of Treasury and IRS policy, rules and/or regulations.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

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.

3.4 Will the system, application or project create or aggregate new data about the individual? 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.

3.5 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.

The Payroll RPA is operated in a virtual desktop infrastructure (VDI) environment which uses the credentials of a RPA Custodian ("Custodian") for identification, accountability and authentication. The process will access only authorized systems or applications and will have only authorized permissions to perform each function it needs to do in each system it accesses, while taking into account the principle of least privilege.

Payroll files with PII are encrypted, zipped, and password protected prior to distribution to specific point of contacts. These files are also encrypted at rest.

3.6 Will the system monitor the public, GSA employees or contractors?

No. PAR does not monitor federal employees, contractors or the public. It is used to pay Federal employees.

3.7 What kinds of report(s) can be produced on individuals?

PAR produces reports that include information linked to individuals, for example PAR validation reports that are used to ensure accuracy of payments, as well as aggregated reports about the workforce as a whole. Note that PII is masked in reports distributed to external customers.

3.8 Will the data included in any report(s) be de-identified? 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.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

GSA mitigates the potential risks related to data over-collection by analysing the PAR business needs and the information collected to meet that need. The PAR system owner periodically reviews the information collection and holdings to ensure that only the minimum amount of PII is being maintained in order to accomplish the business of payroll.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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, as discussed above, PAR collects and maintains the minimum amount of PII necessary accomplish the business of payroll.

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

For the Payroll RPA, it will use a "file distribution list" that contains all of the files to be distributed to the customer POCs. Each line on the "file distribution list" contains the file name, the adjustments required to the file, the POCs for the distribution, their email addresses, and whether the file needs to be encrypted. Encryption is determined based on a flag within the "file distribution list." Files flagged for encryption are encrypted and password protected. The encryption flag is based on PII and/or who is getting sent the file. If it has PII and being sent outside of GSA, then it is encrypted. The encryption flag is determined by the Payroll Team. The bot can only pull contacts off of one line at a time and after each line is completed, the variables are cleared, so that should mitigate any risk of sending files to incorrect contacts.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, 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? If so, who, how and is a formal agreement(s) 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.

The Payroll RPA will use Excel, Word, Notepad, and Google Sheets.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

GSA mitigates the potential risks through the use of MOUs/ISAs in order to establish the data exchanges and appropriate protections. All external information sharing has been reviewed by the system owner and determined necessary to conduct PAR business.

Like what was said in 4.2, the Payroll RPA can only pull contacts off of one line at a time and after each line is completed, the variables are cleared, so that should mitigate any risk of sending files to incorrect contacts.

The "file distribution list" is updated on a more ad hoc basis. There are many within the payroll group that are in contact with the POCs on the distribution list. As PSB learns of changes to the POC's, it is communicated to all within PSB so that communications and reports are sent to the correct POC.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected 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.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

PAR performs many relationship edits and data checks to ensure data entered is as accurate as possible. Fields are defined in the database to ensure valid data. Users are assigned specific accounts for update and not allowed access to all employees in the system. A query is run and reviewed to ensure a Payroll Technician has not changed their own data except through the allowed Employee Express. PAR roles ensure separation of duties to prevent anomalies and fraud.

In addition to the Payroll Services Branch processing the bi-weekly payroll, the Payroll IT Branch performs a payroll balancing process to prevent anomalies and fraud. Queries are also run every pay period to check for potential overpayments, missing input files, as well as data integrity checks.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

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.

The Payroll RPA access and permissions will be dependent on the Custodian's access and permissions. The Custodians are current Payroll Services Branch employees.

The Payroll Services Branch employees should be the only users with access to run the bot to distribute payroll files to customers. User access and authorization to the payroll files is performed through IT, and requires supervisory approval from the Payroll Services Branch.

The Payroll RPA may be used to replicate input and resulting output of user interactions, using established processes and permissions normally done by human users. Payroll RPA operations will be governed by the Custodian Rules of Behavior form signed by the Custodian and Process Owner. The Custodian is responsible for monitoring the performance of the software bot, ensuring completeness and accuracy of processing.

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes, PAR was last granted an Authorization to Operate on August 19th, 2015. The system is currently performing a full Assessment and Accreditation to renew the ATO.

The Payroll RPA had a privacy threshold assessment (PTA) developed, which triggered updating this PIA.

6.3 How will the system or application be secured from a physical, technological, 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 system occurs via logging and monitoring of system use, data changes, vulnerability scanning, and annual audits and assessments.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, 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.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

PAR is in the process of implementing Oracle Transparent Data Encryption (TDE) for table column encryption at rest to mitigate potential security risks.

All employees are required to take the IT Security Awareness and Privacy 101, Privacy 201 training, and Sharing in a Collaborative Environment training annually *to ensure no PII data is shared. The Rules of Behavior are included in the required security training.*

For the Payroll RPA, logs document major points of activity throughout automation via Diagnostic and Run Time Execution Logs and alert Custodians if errors are identified. All automations are completed within the standard GSA user environment and security controls and data encryption completed during process execution are inherited through the GSA Vmware BF2 environment and the applications the process interacts with. The Custodian logs into the VDI and is tracked the same as any user. The Custodian also signs a Rules of Behavior specific to accepting all responsibility for the bot.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

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

7.2 What procedures 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? If so, how?

Please see previous section.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

No, only authorized Payroll Services employees are able to access PAR.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

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.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

Any employee that works with the PAR system is required to take role-based Privacy 201 training, which focuses on identifying and reporting incidents and potential breaches of PII.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with 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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Logging and Monitoring of the system is sanitized of PII data. The system is monitored for appropriate use and only reports on objects changed, not specific data.

For the Payroll RPA, auditing is performed by the Custodian who is ultimately responsible for what the bot does. The Custodian's responsibility is to perform audits of process activities. Auditing/ logging review of the applications is done per GSA's Audit Guide.