



# ePayroll (PAR)

## *Privacy Impact Assessment (PIA)*

4/7/2021

**POINT of CONTACT**

Richard Speidel

[gsa.privacyact@gsa.gov](mailto:gsa.privacyact@gsa.gov)

Chief Privacy Officer  
GSA IT  
1800 F Street NW  
Washington, DC 20405

## Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at [gsa.gov/pia](https://gsa.gov/pia).

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

**Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response.** Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to [gsa.privacyact@gsa.gov](mailto:gsa.privacyact@gsa.gov).**

## Stakeholders

Name of Information System Security Manager (ISSM):

- Richard Banach

Name of Program Manager/System Owner:

- Monica Shackelford

## Signature Page

Signed:

DocuSigned by:  
*Richard Banach*  
21B998D30FCE4B6...

---

Information System Security Manager (ISSM)

DocuSigned by:  
*Monica Shackelford*  
0C9D8301687C4C8...

---

Program Manager/System Owner

DocuSigned by:  
*Richard Spidel*  
171D5411183F40A...

---

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

## Document Revision History

Date	Description	Version #
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to <a href="mailto:gsa.privacyact@gsa.gov">gsa.privacyact@gsa.gov</a>	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1
3/4/2020	Annual update for PIA to new template for PAR	3.2
4/7/2021	Annual Update	3.3

# Table of contents

## SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
- 1.2 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 1.3 Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers and expiration dates.
- 1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

## SECTION 2.0 OPENNESS AND TRANSPARENCY

- 2.1 Will individuals be given notice before to the collection, maintenance, use or dissemination and/or sharing of personal information about them? If not, please explain.

## SECTION 3.0 DATA MINIMIZATION

- 3.1 Why is the collection and use of the PII necessary to the project or system?
- 3.2 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.3 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.4 Will the system monitor members of the public, GSA employees, or contractors?
- 3.5 What kinds of report(s) can be produced on individuals?
- 3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

## 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, maintenance, use, or dissemination?
- 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 GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

## **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 (SSP) for the information system(s) supporting the project?

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

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

## **SECTION 7.0 INDIVIDUAL PARTICIPATION**

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

## **SECTION 8.0 AWARENESS AND TRAINING**

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

## **SECTION 9.0 ACCOUNTABILITY AND AUDITING**

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

## Document purpose

This document contains important details about *ePayroll (PAR)*. To accomplish its mission IC must, in the course of *PAR*, collect personally identifiable information (PII) about the people who use such products and services. PII is any information<sup>[1]</sup> 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.<sup>[2]</sup>

### **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 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.*

*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.*



## **SECTION 1.0 PURPOSE OF COLLECTION**

*GSA states its purpose and legal authority before collecting PII.*

### **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? If so, what System of Records Notice(s) apply/applies to the information?**

*Yes. Please refer to the PAR SORN, [GSA/PPFM-9](#).*

### **1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (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.*

### **1.4 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.*

## **SECTION 2.0 OPENNESS AND TRANSPARENCY**

*GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.*

### **2.1 Will individuals be given notice before the collection, maintenance, use or dissemination 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.*

## **SECTION 3.0 DATA MINIMIZATION**

*GSA limits PII collection only 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 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.*

### **3.2 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.*

### **3.3 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?**

*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? 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.*

## **SECTION 4.0 LIMITS ON USING AND SHARING 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.*

**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 and how? 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.*

**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, 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.*

## **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:*

<i>Role</i>	<i>Authorized Privileges and Functions Performed</i>
<i>APPDETECTIVE_ROLE</i>	<i>Role for AppDetective database security audit scan and has query only access to certain Oracle data dictionary tables/views in database.</i>

<i>DBA</i>	<i>Role only applicable to authorized staff to allow database administration.</i>
<i>IMP_FULL_DATABASE</i>	<i>This role is the default Oracle database import role.</i>
<i>LABOR_DIST</i>	<i>This role will allow the user query privileges to a group of tables in PAR to perform the labor distribution processing.</i>
<i>OSU_ROLE</i>	<i>Allows insert, select, update, and delete from the temporary Pay and Leave message tables.</i>
<i>PAR_ACCTG</i>	<i>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.</i>
<i>PAR_CONNECT</i>	<i>This role allows the user the ability to connect to the PAR database.</i>
<i>PAR_CONTROL</i>	<i>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.</i>
<i>PAR_DEVELOPER</i>	<i>All accesses are select only.</i>
<i>PAR_ETAMS</i>	<i>This role will have insert, update, delete, and query from PAR tables used in the PAR T&amp;A processing.</i>
<i>PAR_HARP</i>	<i>This role allows insert, update, delete, and query privileges to History Access Reports for Payroll (HARP) tables in order to maintain the process.</i>
<i>PAR_HARP_QUERY</i>	<i>This role allows query privileges to the HARP tables.</i>
<i>PAR_HR_AUDIT</i>	<i>This role allows query privileges to the HR tables that provide an audit of what was processed.</i>



<i>PAR_MAINTENANCE</i>	<i>This role's users allow software programs to create, modify and alter tables and views within the production database.</i>
<i>PAR_MANAGER</i>	<i>This role allows the Payroll Managers to have query privileges on most PAR tables and PLS Message approval privileges.</i>
<i>PAR_MONTHEND</i>	<i>This role grants update and query privileges to the table that controls month end reporting.</i>
<i>PAR_OWNERS</i>	<i>No one's userid is under this role. It's users represent the owner schema that the PAR tables have been placed under.</i>
<i>PAR_PARTAX</i>	<i>This role allows insert, update, delete and query privileges to the tax formulas.</i>
<i>PAR_PDW</i>	<i>This role allows query privileges to the Employee Data Store (EDS) tables and insert, update, query, and delete to the process control table.</i>
<i>PAR_PDW_QUERY</i>	<i>This role allows query privileges to the PAR Data Warehouse (PDW) tables.</i>
<i>PAR_PEGASYS</i>	<i>This role allows insert, update, and System delete privileges to the PEGASYS batch tables.</i>
<i>PAR_PLH</i>	<i>This role allows execute to several PAR Reports and insert, update, query, and delete privileges to the Pay and Leave History (PLH) tables.</i>
<i>PAR_PRODUCTION_IDS</i>	<i>This role is used to run the production programs.</i>
<i>PAR_QUERY</i>	<i>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.</i>
<i>PAR_QUERY_ALL</i>	<i>This is a query role that allows query of all database objects owned by PAR.</i>

<i>PAR_SCRIPT_ACCESS</i>	<i>This role allows the scripts to run and sends out the automated email messages.</i>
<i>PAR_SEMI_MONTHLY</i>	<i>This role is used by the Forms application to control who has access to adjust Flexible Spending Accounts and Long Term Care.</i>
<i>PAR_SLTAX</i>	<i>This role allows the users to verify the State and local tax formulas have been implemented in production.</i>
<i>PAR_STUDENT_LOANS</i>	<i>This role has insert, update, and query privileges to the PAR tables necessary for processing student loans.</i>
<i>PAR_SUPERVISOR</i>	<i>This role allows the Payroll Operations Supervisors to have create session, and update, insert, query and delete privileges on most PAR tables.</i>
<i>PAR_TBLUPDATE</i>	<i>This role will allow designated users insert, update, query, and delete privileges to reference tables and certain HR and retirement tables.</i>
<i>PAR_TECH</i>	<i>This role will have create session, create view, and insert, update, query and delete privileges on T&amp;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.</i>
<i>PAR_TPP_MSG</i>	<i>This role allows the users to input and approve the messages that are on the Employee's Pay and Leave Statements.</i>
<i>PAR_UPDATE</i>	<i>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.</i>

<i>PAR_WEB</i>	<i>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.</i>
<i>PAYABLES</i>	<i>This role allows users from Accounts Payables query privileges on a few EDS and reference tables.</i>
<i>RUN_PROCEDURES</i>	<i>This role allows the user to execute the HR procedures and other accesses to process the transactions from HR.</i>
<i>SELECT_CATALOG_ROLE</i>	<i>Role only applicable to authorized staff at IC and has query only access to any Oracle data dictionary tables/views in database.</i>
<i>SHAREDLV_ROLE</i>	<i>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.</i>
<i>THWEB_BATCH</i>	<i>This role allows query privileges to the PLH views and insert, update, and query privileges to the PLS message tables.</i>

## **6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?**

*Yes, The Authority To Operate (ATO) was granted on September 19<sup>th</sup>, 2018.*

## **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? 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.*

**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 do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?**

*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.*

**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.*

## **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 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.*

---

<sup>[1]</sup>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."

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