




**Instructions**

**Privacy Impact Assessment (PIA)**

The Privacy Impact Analysis (PIA) questionnaire is applicable to information systems which store or process privacy data. The questionnaire collects information about the types of privacy data which are stored and processed, why it is collected, and how it is handled. A PIA is required based on the results of a Privacy Threshold Analysis (PTA) questionnaire that has been completed for the information system.

Review the following steps to complete this questionnaire:

**1) Answer questions.** Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

**2) Add Comments.** You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.

**3) Change the Status.** You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

**4) Save/Exit the Questionnaire.** You may use any of the buttons at the bottom of the screen to save or exit the questionnaire. The 'Save and Close' button allows you to save your work and close the questionnaire. The 'Save and Continue' button allows you to save your work and remain in the questionnaire. The 'Cancel' button closes the questionnaire without saving your work.

**00 Default Layout** **Workflow Status:** 99 Workflow Complete

**PIA**

**General Information**

<b>PIA ID:</b>	PIA-383	<b>PIA Status:</b>	Completed
<b>Authorization Package (System Name):</b>	HRLinks	<b>This is a RPA:</b>	No
<b>Assessment Date:</b>	5/23/2022	<b>Is Latest:</b>	Yes
<b>FISCAL Year:</b>	2022	<b>PIA Required (From Authorization Package):</b>	
<b>Final FISCAL Year:</b>	2022	<b>PIA Expiration Date:</b>	5/23/2023
		<b>Final PIA Expiration Date:</b>	5/23/2023

**Override / Reopen Explanation**

<b>Override FISCAL Year:</b>	<b>Override PIA Expiration Date:</b>
<b>Reopened Explanation:</b>	

## Other Stakeholders

### Stakeholders (not in Approval Process)

**System Owner (SO):** Shackelford, Monica

**Authorization Official:** DelNegro, Elizabeth F

### System Owner (eMail)

Name (Full)

Monica Shackelford

### Authorization Official (eMail)

Name (Full)

Elizabeth Delnegro

## PIA Overview

<b>A.System Name:</b>	A. System, Application, or Project Name:	HRLinks
<b>B.Includes:</b>	B. System, application, or project includes information about:	Federal employees
<b>C.Categories:</b>	C. For the categories listed above, how many records are there for each?	12,000 employees.

**D.Data Elements:**

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

HRLinks collects Federal employee data such as

- **Name:** Used to identify the employee and retained for employee HR record.
- **GSA Employee ID:** This is the primary unique identifier which allows HR professionals to search for information about GSA employees.
- **Social Security Number (SSN):** Used and retained for employee HR record and tax reporting purposes.
- **Date of Birth (DOB):** Used to identify employee age and retained for employee HR record.
- **Home Mailing Address:** Used for communication and retained for employee HR record.
- **Phone Number(s):** Used for communication and retained for employee HR record.
- **Email Address:** Used for communication and retained for employee HR record.
- **Financial Account Information:** Used to support payroll direct deposit.
- **Beneficiary Information:** Includes contact information, SSN, DOB of beneficiaries. Retained for employee HR record.
- **Race/Ethnicity:** Voluntarily self-reported for employee HR record This Personally Identifiable Information (PII) is generally the most sensitive information included in the system. Other information includes:
  - Payroll
  - Accounting
  - Pay and leave entitlement records
  - Payroll deduction and withholding
  - Time and attendance records

**Overview:**

This Application SSP only documents the GSA specific controls. IBM is responsible for providing the HR Links Platform SSP documenting the system controls.

The Human Resources IT Transition to Transformation (HR Links) replaced the Comprehensive Human Resources Integrated System (CHRIS), Electronic Time and Attendance Management System (ETAMS), and The Authorized Leave & Overtime Help Application (ALOHA) systems with externally hosted HR and Time & Attendance (T&A) systems from IBM. HR Links integrates IBM's HR and T&A systems with the current GSA Payroll Accounting and Reporting (PAR) system.

HR Links is considered a major application and provides personnel action and benefits processing for all of GSA's employees. The system a shared services hosting model providing HR services to multiple Federal organizations. The HR Links solution diagram below conveys the high level operational end state of the system. This diagram describes the capabilities of the HR Links system and highlights the significant aspects of operations.

**PIA-0.1:**

Is this a new PIA or Recertification request?

Annual Recertification

<b>PIA-0.1Changes:</b>	If you are reviewing this for annual recertification, please confirm if there are any changes in the system since last signed PIA?	No, Changes
------------------------	--	-------------

Comments				
Question Name	Submitter	Date	Comment	Attachment
No Records Found				

### 1.0 Purpose of Collection

<b>PIA-1.1:</b>	What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?	The legal authorities permitting the collection, maintenance and dissemination of PII through HRLinks are: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are the authorities for maintaining personnel information. Authorities for recording Social Security Numbers are E.O. 9397, 26 CFR 31.6011(b)-2, and 26 CFR 31.6109-1. Client users of HRLinks must originate from GSA IP space as defined and documented in the Interconnect Security Agreements (ISAs) and Memoranda of Understanding (MOUs) that govern how the agency connects to HRLinks over a point to point IPsec VPN connection.
<b>PIA-1.2:</b>	Is the information searchable by a personal identifier, for example a name or Social Security number?	Yes
<b>PIA-1.2a:</b>	If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?	Existing SORN applicable
		<b>PIA-1.2 System Of Record Notice (SORN) CR:</b>
<b>PIA-1.2 System of Records Notice(s) (Legacy Text):</b>	What System of Records Notice(s) apply/applies to the information?	<a href="https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf">https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf</a> <a href="https://www.federalregister.gov/documents/2008/04/25/E8-8920/privacy-act-of-1974-notice-of-updated-systems-of-records">https://www.federalregister.gov/documents/2008/04/25/E8-8920/privacy-act-of-1974-notice-of-updated-systems-of-records</a>
<b>PIA-1.2b:</b>	Explain why a SORN is not required.	
<b>PIA-1.3:</b>	Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?	No
<b>PIA-1.3 Information Collection Request:</b>	Provide the relevant names, OMB control numbers, and expiration dates.	
<b>PIA-1.4:</b>	What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.	<a href="https://www.gsa.gov/cdnstatic/20200504%20-%20HRLinks%20Appendix_%20Record%20Retention%20%20Destruction%20Schedules.pdf">https://www.gsa.gov/cdnstatic/20200504%20-%20HRLinks%20Appendix_%20Record%20Retention%20%20Destruction%20Schedules.pdf</a>

## 2.0 Openness and Transparency

<b>PIA-2.1:</b>	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
<b>PIA-2.1 Explain:</b>	If not, please explain.	

## 3.0 Data Minimization

<b>PIA-3.1:</b>	Why is the collection and use of the PII necessary to the project or system?	The system is the official repository of the personnel information, reports of personnel actions and the documents associated with these actions. The personnel action reports and other documents give legal force and effect to personnel transactions and establish employee rights and benefits under pertinent laws and regulations governing Federal employment. They provide the basic source of factual data about a person's Federal employment while in the service and after his or her separation. Records in this system have various uses, including screening qualifications of employees; determining status eligibility, and rights and benefits under pertinent laws and regulations governing Federal employment; computing length of service; and other information needed to provide personnel services.
<b>PIA-3.2:</b>	Will the system, application, or project create or aggregate new data about the individual?	No
<b>PIA-3.2 Explained:</b>	If so, how will this data be maintained and used?	
<b>PIA-3.3:</b>	What protections exist to protect the consolidated data and prevent unauthorized access?	HRLINKS has implemented the required security and privacy controls according to NIST SP 800-53. HRLINKS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.
<b>PIA-3.4:</b>	Will the system monitor the public, GSA employees, or contractors?	None
<b>PIA-3.4 Explain:</b>	Please elaborate as needed.	HRLinks does not monitor the GSA employees.
<b>PIA-3.5:</b>	What kinds of report(s) can be produced on individuals?	HRLinks may create human resource reports related to GSA employees.
<b>PIA-3.6:</b>	Will the data included in any report(s) be de-identified?	No
<b>PIA-3.6 Explain:</b>	If so, what process(es) will be used to aggregate or de-identify the data?	NO - HRLINKS does not de-identify data for reporting.
<b>PIA-3.6 Why Not:</b>	Why will the data not be de-identified?	This is an HR system and needs the PII.

#### 4.0 Limits on Using and Sharing Information

<b>PIA-4.1:</b>	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
<b>PIA-4.2:</b>	Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?	Federal Agencies
<b>PIA-4.2How:</b>	If so, how will GSA share the information?	GSA employee information is shared externally as described below or pursuant to an approved routine use identified in the OPM GOVT-1 and PAR (PPFT-9) SORNs. Information is collected via bidirectional SFTP connections or unidirectional connections with interfacing systems. The GSA HRLinks team maintains approved interconnection system agreements (ISA) for all organizations and systems that interface with GSA's instance of HRLinks.
<b>PIA-4.3:</b>	Is the information collected:	Directly from the Individual
<b>PIA-4.3Other Source:</b>	What is the other source(s)?	On an ongoing basis, GSA employees review, update and enter data directly into the system as needed. Each GSA employee is responsible for checking the accuracy of their data and should contact OHRM with any questions. The HRLinks system does not collect information from commercial sources or publicly available data. HRLinks receives information about GSA employees from the systems listed below: Payroll, Accounting and Reporting (PAR) system – PAR is GSA’s payroll processing system and the link between the GSA’s HR and accounting systems. HRLinks sends updated personnel data to the payroll system along with the time and attendance information required to perform payroll actions. GSA’s payroll system provides HRLinks with the resulting payroll information after each payroll processing cycle. GSA employee PII shared from PAR to HRLinks and from HRLinks to PAR includes the employee’s name, date of birth, and social security number. However, HRLinks and PAR do not exchange employee home addresses, or phone numbers. GSA Credential and Identity Management System (GCIMS) - GCIMS contains credential and background investigation information for all GSA employees. HRLinks has a bidirectional connection to GCIMS and shares PII including SSN as part of the background investigation process. GSA JOBS - GSA JOBS contains information on GSA positions. HRLinks has a bidirectional connection to GSA JOBS to track which positions are open or being filled.
<b>PIA-4.4:</b>	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	Yes

**PIA-4.4Who How:**

If so, who and how?

The system will interact with other systems outside of GSA. The following agreements are in place:

- Non-Disclosure Agreements (NDAs) apply to HRLinks data and prohibit further dissemination of information. NDAs are required for all tenants of HRLinks. HRLinks tenants include General Services Administration (GSA), National Credit Union Association (NCUA), Office of Personnel Management (OPM), and Railroad Retirement Board (RRB).
- All system connections are governed by Interconnect Security Agreements (ISAs) and Memoranda of Understanding (MOUs), which are approved and validated no less than once annually.

HRLinks receives information about GSA employees from the systems listed below:

- Payroll, Accounting and Reporting (PAR) system
- GSA Credential and Identity Management System (GCIMS)

HRLinks receives information about GSA employees from the systems listed below:

- GSA JOBS

HRLinks sends information about GSA employees from the systems listed below:

- Department of Health and Human Services (HHS) Federal Occupational Health (FOH)
- OPM's Electronic Official Personnel Folder (eOPF)
- OPM's Benefits (EEX)
- OPM's Enterprise Human Resources Integration (eHRI)



**PIA-4.4Formal Agreement:**

Is a formal agreement(s) in place?

**PIA-4.4No Agreement:**

Why is there not a formal agreement in place?

## 5.0 Data Quality and Integrity

**PIA-5.1:**

How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

Accuracy of the initial load of GSA employee information (e.g. from CHRIS, ALOHA and ETAMS) was checked via functional specification testing by GSA OHRM staff to validate data values and mappings, functional scenarios based testing to include both positive and negative testing, and during data uploading phase from various interfaces. On an ongoing basis, GSA employees review, update and enter data directly into the system as needed. Each GSA employee is responsible for checking the accuracy of their data and should contact OHRM with any questions.

## 6.0 Security

PIA-6.1a:

Who or what will have access to the data in the system, application, or project?

There are four tiers of users, as categorized by PII access.

- "Tier one" users are employees that can access their own personal data only, for example personal contact information, benefit election information and time and attendance records.
- "Tier two" users are an employee's supervisor who has access to information including that employee's home address, personal contact information, and time and attendance records but specifically excluding Social Security Number (SSN) and date of birth (DOB).
- "Tier three" users are comprised of a subset of GSA OHRM staff users who may have a need to access employees' SSNs or DOBs, as well as the information available at tiers one and two.
- "Tier four" users are a different subset of GSA OHRM staff who may need access to voluntarily reported employee data including race and national origin to evaluate how GSA is meeting its policies and practices on hiring and retaining minorities, women, and disabled persons, analyzing their status in the workforce; and for establishing workforce diversity goals and timetables.



<b>PIA-6.1b:</b>	What is the authorization process to gain access?	<p>GSA employees have access to their own individual online records using a username and password credentials (with additional multi-factor authentication using SecureAuth), or by using Personal Identity Verification (PIV). Additionally, GSA-assigned managers and HR administrators are able to update their employees' data such as reprimands, education and benefits. Privileged users such as managers, Human Resources Administrators, and report generators access online records other than their own, consistent with their authority and organizational affiliations using username and password credentials. HRLinks IBM Implementation for Account Granting / Termination: HRLinks identifies and selects the types of information system accounts needed including individual, system, application, and process accounts and employs Least Privilege / Least Function. Administrative accounts for Windows and Linux are managed via active directory. Access is approved by appropriate personnel prior to account creation. All IBM personnel must go through the GSA onboarding and PIV issuance process. Removal employs the same processes. Details are documented in the HRLinks System Security Plan. GSA Implementation for Account Granting / Termination: GSA roles have been identified as Admin Mgr Contractor (MBI), Agency Superuser, Agency Superuser Waiver, Analytics, and Analytics Waiver. The individual places a request in EARS for their specific role, based on guidance from the supervisor. The supervisor is responsible to approve that it is a valid request. The Data Owner is responsible for verifying that the user does need the permissions requested based on their job responsibilities.</p>
<b>PIA-6.2:</b>	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
<b>PIA-6.2a:</b>	Enter the actual or expected ATO date from the associated authorization package.	3/31/2021

<p><b>PIA-6.3:</b></p>	<p>How will the system or application be secured from a physical, technical, and managerial perspective?</p>	<p>HRLinks is hosted in datacenters that meet the necessary physical, technological, and managerial requirements to meet FedRAMP Infrastructure as a Service accreditation. The details of site perimeter hardening, power supply continuity, multifactor identity controls and man traps, as well as armed guards, 24/7/365 CCTV monitoring, automated incident response, personnel security requirements, as well as key control, cage access, and associates managerial controls over all the preceding domains of security are all externally validated by independent third party assessors and documented in either the respective FedRAMP IaaS package or in the SSAE19 audit report. HRLinks application maintenance and development teams specifically own all hardware encryption, data at rest encryption, network and VPN encryption, backup and recovery services, annual testing, as well as identity and access management within the system. These controls are internally assessed in partnership with GSA and also undergo periodic testing by independent third-party assessors for the purpose of Authority to Operate controls testing. The details of IBM's security posture are maintained in the Accreditation Package (which includes PIA, PTA, IR Plan, IR Test, DR Plan, DR Test, FIPS-199 System Categorization, third party Security Controls Assessment audit report, POA&amp;M, weekly vulnerability scans, as well as monthly secure configuration baseline scans and application security scan reports).</p>
<p><b>PIA-6.4:</b></p>	<p>Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?</p>	<p>Yes</p>
<p><b>PIA-6.4What:</b></p>	<p>What are they?</p>	<p>HRLinks employs a robust and automated incident response capability to thwart, minimize, contain, or otherwise quickly recover from any security incident involving a break or compromise of PII. The details of the HRLinks incident response capability are documented in the HRLinks System Security Plan as well as the HRLinks Incident Response Plan.</p>

## 7.0 Individual Participation

<b>PIA-7.1:</b>	What opportunities do individuals have to consent or decline to provide information?	Individuals can decline to provide information, and if so, may not be able to complete human resources and payroll activities necessary for employment. Certain data fields are mandatory for human resources and payroll processing; however, individuals have the ability to voluntarily self-report personnel information including race, national origin, and ethnicity data.
<b>PIA-7.1Opt:</b>	Can they opt-in or opt-out?	Yes
<b>PIA-7.1Explain:</b>	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	
<b>PIA-7.2:</b>	What are the procedures that allow individuals to access their information?	A basic account is created for all GSA employees through which they can view and update their personal information, for example benefits elections.
<b>PIA-7.3:</b>	Can individuals amend information about themselves?	Yes
<b>PIA-7.3How:</b>	How do individuals amend information about themselves?	They can submit changes which get routed for approval to HR.

## 8.0 Awareness and Training

<b>PIA-8.1:</b>	Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.	GSA has developed, implemented, and regularly updates annual training modules on IT Security and Privacy Awareness and Sharing Securely in a Collaborative Environment. All GSA account holders also electronically sign the GSA Rules of Behavior.
-----------------	--	---

## 9.0 Accountability and Auditing

<b>PIA-9.1:</b>	How does the system owner ensure that the information is used only according to the stated practices in this PIA?	HRLinks implements secure coding and development best practices to support and enhance privacy controls. Database encryption enhances the security and privacy of the PII processed and stored in the HRLinks solution. Restrictive network design for HRLinks implements a multi-tiered architecture consistent with GSA CIO guidance and in direct compliance with NIST 800-53 Rev 4 security controls for Government information systems. Additionally, HRLinks is subject to external audits as well as annual internal controls testing. Further, HRLinks implements controls and reporting required under the NIST Risk Management Framework.
-----------------	---	---