



# Human Resources IT Transition to Transformation (HRLinks)

*Privacy Impact Assessment*

April 15, 2021

**POINT of CONTACT**

Richard Speidel

*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](#). It requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with [1878.2A CIO P - Conducting Privacy Impact Assessments](#); is designed to align with GSA businesses 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 ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are available to the public at [gsa.gov/privacy](https://www.gsa.gov/privacy) (<https://www.gsa.gov/portal/content/102237>).

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 codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. For example:

This document contains important details about *[system, application or project name]*. *[GSA office]* may, in the course of *[program name]*, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at:

<https://www.gsa.gov/portal/getMediaData?mediaId=167954>

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):

- Jonathan Wallick

Name of Program Manager/System Owner:

- Merrick Krause

## Signature Page

Signed:

Jonathan Wallick

---

Information System Security Manager (ISSM)

Merrick Krause

---

Program Manager/System Owner

Richard Speidel

---

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for making sure the PIA contains complete privacy related information.

## Document Revision History

Date	Description	Version of Template
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 CPO email address	2.3
11/28/2018	Added new stakeholders section to streamline process when seeking signatures & specified that completed PIAs should be sent to <a href="mailto:gsa.privacyact@gsa.gov">gsa.privacyact@gsa.gov</a>	2.4
4/15/2020	Annual revision and update	2.5
4/15/2021	Annual revision and update	2.6

## **Table of contents**

### **SECTION 1.0 PURPOSE OF COLLECTION**

- 1.1 Why is GSA collecting, maintaining, using or disseminating the information?
- 1.2 What legal authority and/or agreements allow GSA to collect the information?
- 1.3 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?
- 1.4 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.
- 1.5 Has a records retention schedule been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.

### **SECTION 2.0 OPENNESS AND TRANSPARENCY**

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

### **SECTION 3.0 DATA MINIMIZATION**

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

### **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?

## **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?

## **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 ensure that the information is used in accordance with the stated practices in this PIA?

## Document Purpose

HRLinks is a major application that provides personnel action and benefits processing for all of General Services Administration's (GSA) 21,000 employees. It also provides similar but separate processing for employees of GSA's former customer entities: the Railroad Retirement Board (RRB); the National Credit Union Administration (NCUA); and the Office of Personnel Management (OPM). The General Services Administration (GSA) Human Resources Information Technology (HRIT) Division acquired the Human Resources IT Transition to Transformation (HRLinks) system from private-sector providers. GSA's adoption of HRLinks allows it to decertify as a Human Resources Line of Business (HRLOB) Shared Service Provider and migrate that responsibility to International Business Machines Corporation (IBM), who is a private HRLOB Shared Service Provider vendor. IBM provides the PeopleSoft application and GDT Hosting (GDT) operates the two Federal Risk and Authorization Management Program (FedRAMP)-certified data centers where the application is hosted.

GSA uses 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

[2]  
1974.

## System, Application or Project

Human Resources IT Transition to Transformation (HRLinks)

## System, application or project includes information about

Federal employees

## System, application or project includes

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

The HRLinks system GSA to utilize the information system supporting the day- to-day operating needs of its human resource operations and management. The system is designed to meet information and statistical needs of all types of Government organizations and provides a number of outputs.

## SECTION 1.0 PURPOSE OF COLLECTION

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

### 1.1 Why is GSA collecting the information?

GSA is collecting the information to track, produce and store personnel actions, and supply HR data used to generate reports (organizational rosters, retention registers,



retirement calculations, Federal civilian employment, length-of-service lists, award lists, etc.). It also provides reports for monitoring personnel actions to determine the impact of the GSA's 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. The system also provides other management data for administrative and staff offices.

HRLinks also provides enterprise time and attendance functions for GSA. For example, GSA employees and approved personnel can access a self-service portal, initiate electronic timecard reconciling with other systems such as PAR, and facilitate compliance with other applicable regulatory controls and guidance.

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

### **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, employees are uniquely identified by a randomly generated system identifier called EMPLID and/ employee name. [OPM-GOVT 1](#) covers the GSA's personnel and training records and [GSA PAR \(PPFM-9\)](#) covers its time, attendance and payroll records.

### **1.4. Has any 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.**

None of the forms that are automated within HRLinks trigger the PRA. For an example see the Thrift Savings Plan Election Form, [TSP-1](#).

**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.**

Please see the separate appendix.

## **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.**

Yes, the HRLinks login screens for servers and the application itself displays the following banner:

\*\*\*\*\*WARNING\*\*\*\*\*  
\*\*\*\*\*

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

Fillable forms available to GSA employees within HRLinks (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.

## **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?**

HRLinks collects information on Federal employees.

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

- **Name:** Used to identify the employee and retained for employee HR record
- **GSA Employee ID:** This is the primary, non-sensitive unique identifier which allows HR professionals to search for information about GSA employees.
- **Social Security Number:** Used and retained for employee HR record and tax reporting purposes
- **Date of Birth:** Used to identify employee age and retained for employee HR record
- **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

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

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.

**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?**

HRLinks does not create or aggregate new data about individuals.

**3.5 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.

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

HRLinks does not monitor the GSA employees.

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

HRLinks may create human resource reports related to GSA employees.

**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?**

HRLINKS does not de-identify data for reporting.

**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?**

HRLinks limits information to only what is required to carry out human resource activities.

**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?**

HRLinks transmits information to the systems listed below via secure file transfer protocol (SFTP) which provides the ability to push data to external sources through batch file transfer.

The Department of Health and Human Services (HHS) Federal Occupational Health (FOH)–HHS’ FOH provides a benefit to all federal agencies for work-life balance activities for Federal employees (<https://www.worklife4you.com/index.html>). This FOH-managed program requires that each Federal agency provide a list of current employees to the WorkLife4You vendor. HRLinks provides a full list of GSA employees to FOH on a monthly basis including name, e-mail address, birth date, gender, and home address to allow FOH to offer benefits.

OPM’s Electronic Official Personnel Folder (eOPF) – HRLinks transmits GSA employees’ personnel records (e.g. promotions, raises, etc.) to OPM’s Enterprise Human Resources Integration (EHRI) initiative to improve the Federal Government’s human capital management. eOPF is each employee’s electronic Official Personnel File. eOPF requires the employee’s name and SSN to validate records.

Benefits (EEX) – EEX allows a variety of discretionary personnel and payroll transactions (e.g., changes to Financial Allotments, Health Benefits, Thrift Savings Plan, Direct Deposit, Federal and State Taxes, and Home Address) to be performed. This service requires PII, including SSN to validate records.

Enterprise Human Resources Integration (eHRI) – EHRI is responsible for maintaining the integrity of the electronic Official Personnel Folder (eOPF), which protects information rights, benefits, and entitlements of federal employees. Through on-demand Web-based access to personnel folders, EHRI eOPF enables 24/7 concurrent access to personnel information by Human Resources (HR) staff, and employees. It also allows the

electronic transfer of the eOPF from one agency to another when the employee moves from one organization to another. The suite of EHRI analytical tools and a comprehensive Data Warehouse provides on demand, custom reports to plan and forecast the personnel needs of the Federal Government. This service requires PII, including SSN to validate records.

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.

**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)?**

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.

**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?**

Yes, 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)

## **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?**

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.

## **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?**

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.

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.

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

HRLinks maintains an up-to-date System Security Plan and the overall system received an Authority to Operate (ATO) on 03/31/2021.

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

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&M, weekly vulnerability scans, as well as monthly secure configuration baseline scans and application security scan reports).

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

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.

## **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.**

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.

**7.2 What procedures 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.

The HRLinks interface provides users with guided options to edit data. GSA is responsible for training employees on how to use the HRLinks system. Some information updates may require additional approval, for example promotions.

**7.3 Can individuals amend information about themselves? If so, how?**

HRLinks is a self-service system and employees have access to their respective data. Employees can access, redress and correct their own personnel information, and can review and update their respective HR information as necessary. Additionally, assigned managers and HR administrators will be able to update their employees' data such as reprimands, education and benefits. GSA employees should contact OHRM if they ever have any questions or concerns.

## **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.**

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.

## **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?**

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.

---

[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.