Privacy Impact Assessment

Human Resources IT Transition to Transformation (HR Links)

May 31, 2018

Privacy Impact Assessment (PIA) for the

General Services Administration

Human Resources IT Transition to Transformation (HR Links)

February 15, 2018

Contact Point:
Joseph Hoyt
GSA IT – Staff Office ISSO Support Branch
202.969-7181

Abstract
HR Links is a major application that provides personnel action and benefits processing for all of GSA's 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). GSA's adoption of HR Links allows it to decertify as a Human Resources Line of Business (HRLOB) Shared Service Provider and migrate that responsibility to IBM, who is a private HRLOB Shared Service Provider vendor. GSA and its former customer entities are hereinafter referred to as "HR Links client entities."

The General Services Administration (GSA) Human Resources Information Technology (HRIT) Division acquired the Human Resources IT Transition to Transformation (HR Links) system from private-sector providers. International Business Machines Corporation (IBM) provides the PeopleSoft application and QTS Realty Trust, Inc. (QTS) operates the two Federal Risk and Authorization Management Program (FedRAMP)-certified data centers where the application is hosted.

This Privacy Impact Assessment covers the GSA's use of HR Links. Each of HR Links' client entities may choose to use HR Links in different ways and may provide supplemental information to their employees about such use.

Overview

HR Links has replaced GSA's 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 also integrates IBM's HR and T&A systems with the current GSA Payroll Accounting and Reporting (PAR) system, for example in order to reconcile GSA's electronic timecards.

The HR Links system allows each client entity 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, described further below.

For each client entity's Office of the Chief Human Capital Officer, the system tracks, produces and stores personnel actions, and supplies 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 client entity's policies and practices on hiring and retaining minorities, women, and disabled persons, analyzing their status in the work force; and for

establishing workforce diversity goals and timetables. The system also provides other management data for administrative and staff offices.

HR Links also provides enterprise time and attendance functions for client entities. 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.

The system has been designed to comply with the following laws, regulations, policies and legal authorities:

- Federal Information Security Modernization Act of 2014
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996."
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors."
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource."
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies."
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems."
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems."
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."
- NIST Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems."
- NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments."
- NIST Special Publication 800-34 Revision 1, "Contingency Planning Guide for Information Technology Systems."
- NIST Special Publication 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach."
- NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems."
- NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."
- NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans."

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the application in question?

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.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

Each HR Links client entity is responsible for identifying the SORN for their agency's personnel, training, time, attendance, and payroll records. OPM-GOVT 1 covers the GSA's personnel and training records and GSA PAR (PPFM-9) covers its time, attendance and payroll records.

1.3 Has a System Security Plan (SSP) been completed for the information system(s) supporting the application?

A System Security Plan (SSP) has been drafted for HR Links, utilizing the GSA specified template. Each of the client's Authorizing Official is responsible for reviewing and approving the ATO package.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

HR Links complies with all GSA retention and disposal procedures specified by 1820.1 CIO P GSA Records Maintenance and Disposition System. Records contained in the HR Links system will be retained consistent with section 2.2 of NARA General Records Schedule, "Employee Management Records". See https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

None of the forms that are automated within HR Links trigger the PRA. For an example see the Thrift Savings Plan Election Form, TSP-1.

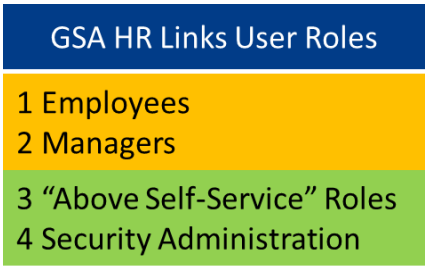
Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the application collects, uses, disseminates, or maintains.

HR Links collects Federal employee data such as Name, Social Security Number (SSN), Employee Number, Date of Birth/Age, Home address and telephone number, Race and National Origin data, Gender, Handicap Code, Birth Date, Marital Status, Reprimands and Warnings, Education History, and Benefits. 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, and time and attendance records.

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. Examples of "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.



HR Links 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. HR Links 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 HR Links with the resulting payroll information after each payroll processing cycle. GSA employee PII shared from PAR to HR Links and from HR Links to PAR includes the employee's name, date of birth, and social security number. However, HR Links 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 and contractors. HR Links 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. HR Links has a bidirectional connection to GSA JOBS to track which positions are open or being filled.

HR Links 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. HR Links 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.

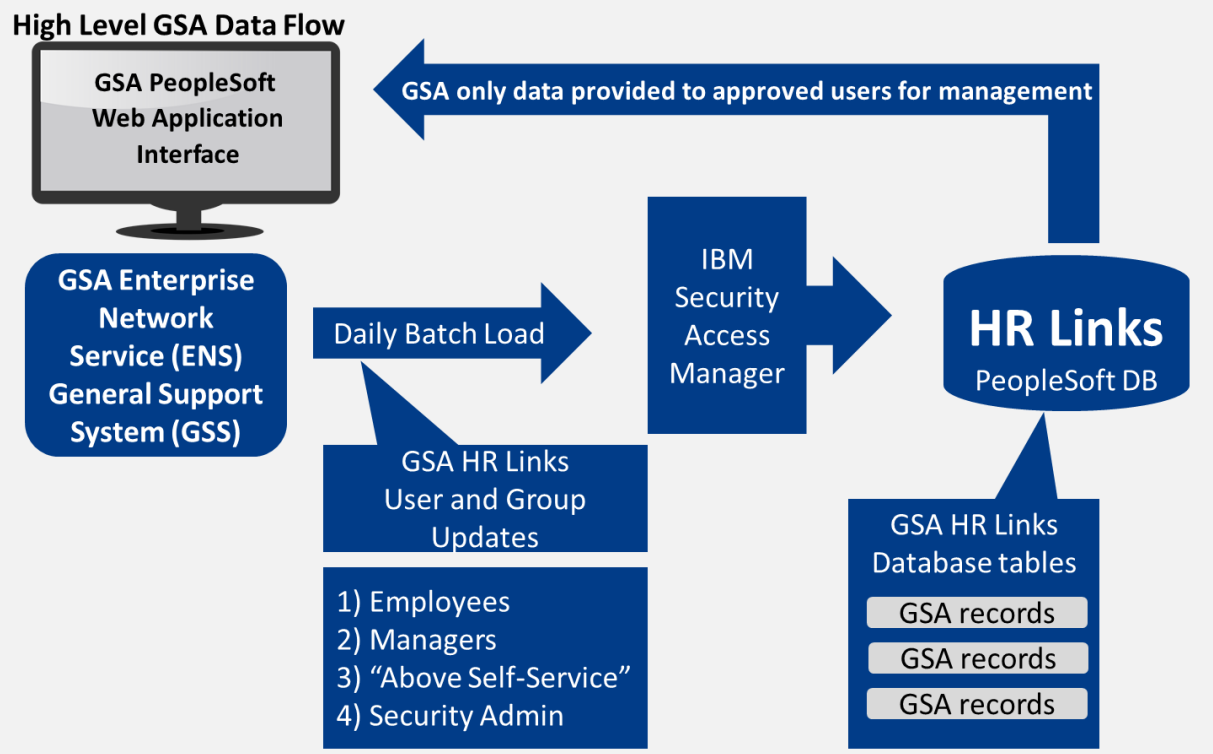
OPM's Electronic Official Personnel Folder (eOPF) – HR Links transmits GSA employees' personnel records (e.g. promotions, raises, etc.) to OPM's Enterprise Human Resources Integration (EHRI) initiative to improve the Federal Government's human capital management. eOPF is each employee's electronic Official 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.

2.2 What are the sources of the information and how is the information collected for the application?

The diagram below depicts the flow of GSA employee information to and from HR Links.



2.3 Does the application use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The HR Links system does not collect information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the initial load of GSA employee information (e.g. from CHRIS, ALOHA and ETAMS) is 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 after the initial set of information is loaded into HR Links, GSA employees will 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.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: HR Links collect sensitive Personally Identifiable Information (PII). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, and/or financial harm may result for the individuals affected.

Mitigation: HR Links has implemented the required security and privacy controls according to NIST SP 800-53. HR Links 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.

Section 3.0 Uses of the Information

The following questions require a clear description of the application's use of information.

3.1 Describe how and why the application uses the information.

- **Name**: Used to identify the employee and retained for employee HR record
- **GSA Employee ID:** This is the primary unique identifier which allows HR professional 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
- **Compensation data**: Used to support payroll and compensation function
- **Warnings and reprimands**: Used for personnel management by Human Resources
- **Benefits information**: Used to provide and validate employee benefits
- **Time and Attendance**: Used to document hours worked by employees on daily basis

For an example of use of privacy information of employee and employee beneficiaries, see the bottom of page 5 of the Health Benefits Election Form (SF2809-15).

3.2 Does the application use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how GSA plans to use such results.

HR Links is a human capital information system and does not include tools to perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. In addition, the system does not create or makes available new or previously unutilized information about an individual.

Reporting and analytic options enable HR Links approved users to integrate reporting as a strategic part of enterprise business processes. Specifically, reporting is embedded directly into business process flows as an integral part of the user interface. Users generate reports in context, within transactions, where the data can be used for better decision support and the data is both current and secure. User reports are limited in scope to data they are approved to access under their existing and organizationally-defined roles.

3.3 Are there other components with assigned roles and responsibilities within the system?

HR Links provides Human Resource information management services to HR Links client entities. Each of the HR Links client entities can allocate user roles to its employees across the four "tiers" described in section 2.1 above.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: HR Links collects a variety of sensitive PII as described above. Due to the highly sensitive nature of this data, there is a risk that, if the data were to use for purposes other than intended, could result in personal and financial damage to individuals involved and GSA.

Mitigation: Controls are in place to ensure data is used and protected in accordance with legal requirements, GSA policies, and GSA's stated purpose for using the data. Controls include mandatory training completion for all employees and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. HR Links has implemented required security and privacy controls according to NIST SP 800-53. Additionally, personnel with access to the system are subject to applicable personnel security investigations and must be deemed suitable prior to system access rights being granted.

Section 4.0 Notice

4.1 How does the application provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The HR Links 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 HR Links (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.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the application?

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.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that client entities' employees will not know that HR Links collects, maintains, and/or disseminates sensitive PII about them.

Mitigation: The HR Links system mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the prominent Privacy Act Notice (above) and SORNs published in the Federal register. In addition, this PIA will be published to gsa.gov/privacygsa.

Section 5.0 Data Retention by the application

The following questions are intended to outline how long the application retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

HR Links data is retained online for GSA employees. GSA employee data is retained for a minimum of seven years, per NARA chapter 3 guidance, but may be retained longer for example in cases of court order, pursuant to open litigation. Final disposal of data is in accordance with GSA's disposal policy.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Maintaining employee PII data longer than the required period in HR Links may lead to information being out-of-date or inaccurate and to an increased risk of information compromise or breach.

Mitigation: To mitigate the risk posed by information retention, HR Links system adheres to the GSA schedules for each category or data it maintains. When the retention data is reached for a record, the HR Links team will carefully disposes of the data by the determined method as described by GSA policies. All electronic storage media used to store, process, or access HR Links records will be disposed of in accordance with the GSA Electronic Media Sanitization policy.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the application information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of GSA as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

HR Links shares information with organizations and systems as described in section 2.1 above.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

GSA employee information is shared externally as described in section 2.1 above or pursuant to an approved routine use identified in the OPM GOVT-1 and PAR (PPFT-9) SORNs.

6.3 Does the application place limitations on re-dissemination?

Non-Disclosure Agreements (NDAs) apply to HR Links data and prohibits further dissemination of information. NDAs are required for all tenants of HR Links. HR Links tenants include General Services Administration (GSA), National Credit Union Association (NCUA), Office of Personnel Management (OPM), and Railroad Retirement Board (RRB).

6.4 Describe how the application maintains a record of any disclosures outside of the Agency.

HR Links does not routinely share client entity (GSA/ OPM/ NCUA/ RRB) data with other client entities, or with external agencies, except as described in section 2.1 above or in SORNs OPM/GOVT-1, PPFM-9 or other applicable SORNs.

For example, in the case of an information breach, a client entity using HR Links may communicate with an impacted agency in accordance with its Incident/Breach Response policy, with records of the incident and client communication recorded in HR Links enterprise ticketing system. HR Links client entities may also disclose information when it is reasonably necessary to assist the impacted agency as it responds.

6.5 Privacy Impact Analysis: Related to Information Sharing

The HR Links solution does not share client entity (GSA/ OPM/ NCUA/ RRB) data with other client entities, or with external agencies, except as described in section 2.1 above or SORNs OPM/GOVT-1, PPFM-9 or other applicable SORNs.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 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.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

HR Links 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.

7.3 How does the application notify individuals about the procedures for correcting their information?

The HR Links interface provides users with guided options to edit data. GSA and other client entities are responsible for training employees on how to use the HR Links system. Some information updates may require additional approval, for example promotions.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals whose records contain incorrect information may not receive notification of HR changes. Furthermore, incorrect information in an HR record could result in improper compensation or benefits.

Mitigation: HR Links mitigates the risk of incorrect information in an individual's records by authenticating information and validating data accuracy. GSA employees will have access to their own individual online records using a username and password credentials, or by using Personal Identity Verification (PIV). Additionally, GSA-assigned managers and HR administrators will be able to update their employees' data such as reprimands, education and benefits. Privileged users such as managers, Human Resources Administrators, and report generators will access online records other than their own, consistent with their authority and organizational affiliations using username and password credentials.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

User PII is required by core functions of the application. Functional and technical features have been designed to safeguard PII against misuse.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the application.

The HR Links solution team is responsible for providing basic security awareness training to its employees. Security awareness training is also given as part of the on-boarding process to all GSA employees and contractors and must be completed prior to gaining access to any HR Links environment. All HR Links solution team personnel receive initial security awareness training upon on-boarding, and conducts annual refresher training.

8.3 What procedures are in place to determine which users may access the information and how does the application determines who has access?

Access control is managed through roles and permissions at the PeopleTools level in the PeopleSoft application with tight integration with the solution's Active Directory. It restricts users' ability to execute functions above and beyond their permitted level. IBM resources working on the HR Links project undergo a GSA background check and must go through the onboarding process, where all necessary GSA approvals occur. QTS resources do not have access to the application.

GSA follows its onboarding/access control procedure for access to HR Links. The solution utilizes IBM Security Access Manager (ISAM) to identify and authenticate client entities users with a PIV card and SecureAuth authentication mechanism. End user application roles such as regular user, HR specialist, and employee manager roles are assigned and enforced by GSA according to an individual's role and responsibility within the agency.

8.4 How does the application review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within GSA and outside?

Information is collected via bidirectional SFTP connections or unidirectional connections with interfacing systems. The GSA HR Links team maintains approved interconnection system agreements (ISA) for all organizations and systems that interface with GSA's instance of HR Links.