Employee Relocation Resource Center (ERRC)

Privacy Impact Assessment (PIA)

June 16, 2020

POINT *of* CONTACT

Richard Speidel

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.

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.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Matthew Regan

Name of Program Manager/System Owner:

- Julie L. Blanford

Signature Page

Signed:

DocuSigned by:

Matthew Regan

92526A8616CB470...

Information System Security Manager (ISSM)

DocuSigned by:

Julie Blanford

F67E95ACBE2A43C...

Program Manager/System Owner

DocuSigned by:

Richard Speidel

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 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 Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	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
6/2/2020	Updated Using New Template	3.2
6/16/2020	PIA Approved	3.3

Table of contents

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 *Employee Relocation Resource Center (ERRC).* To accomplish its mission *The Travel and Transportation office, part of FAS*, must, in the course of *ERRC*, collect personally identifiable information (PII) about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, 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.[2]

A. System, Application, or Project Name:

Employee Relocation Resource Center (ERRC)

B. System, application, or project includes information about:

Federal agency representatives, employees and contractors that use the employee relocation programs procured through the Centralized Household Goods Traffic Management Program (CHAMP) and Multiple Award Schedules (MAS) Solicitation Special Item Numbers (SINs) (MAS SIN 531).

C. For the categories listed above, how many records are there for each?

Approximately 900 (+-) name, address, email and phone number records of agency employee relocation representatives and industry Contractors as of June, 2020.

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

Full name, address, phone numbers and emails of agency representatives and Contractors;

Uploaded notes and reports with names, addresses and;

Agency procurement solicitation documents and;

May include documents regarding federal employee's personal experiences during the relocation process including personal struggles with finances.

Overview

The FAS Employee Relocation Resource Center (ERRC) is a government-wide center for employee relocation products and services, including vendor management. ERRC delivers employee relocation products and services to Federal agencies in support of their operations at the best value possible. Additionally, ERRC helps agencies in the development of procurement strategies, and offers advice in the agency's implementation of service-effective and cost-efficient programs that respond to the individual agency's culture and philosophy.

Agency employees and Contractors using ERRC programs may contact ERRC and request assistance in troubleshooting program difficulties. Employee relocation is very stressful and personal and ERRC is often called upon to assist with reviewing the employee's relocation appraisals and home inspections. The system stores agency employee or contractor name, contact information, agency name, contractor assisting the agency employee and documents providing information on requesting services with justification. The system stores the records presented to ERRC based on the request for assistance. The records are retained for 7 years.

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?

ERRC is not an external facing system; instead it is an internal system of record to track and store the records related to the employee relocation services of GSA: https://www.gsa.gov/directives-library/gsa-records-management-program-18201-oas-p

Relocation procurement under the MAS is required to follow the Federal Acquisition Regulation and the Federal Travel Regulation. Additionally, the Office of Management and Budget (OMB) with the support of the Government -wide Category Management Program Management Office announced the designation of the Civilian Employee Relocation Home Sale Solution (GSA MAS SIN 531) as "Best in Class" (BIC). Agencies are required to use our programs unless there is a waiver.

The Centralized Household Goods Traffic Management Program (CHAMP) is a tender based procurement. This document in the Acquisition Gateway outlines the program and names the authority to procure outside of the FAR: https://hallways.cap.gsa.gov/app/#/gateway/travel/1086/household-goods-move-management-services%3Ftid=3401?tid=3401

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?

Records may be retrieved by agency employee / contractor names, email address, vendor name and case number. Retrieval can also be performed using a text search, and using name or email address as the search criterion. GSA-OCIO-3, "GSA Enterprise Organization of Google Applications and SalesForce.com" is the SORN covering this system.

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.

No, OMB's ICR process is not applicable to GSA's ERRC as it is not an information collection activity.

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.

ERRC follows the federal record retention policy of 7 years from the date the record was created in Salesforce instance. The information is retained for reference in further appeals or congressional inquiries, which occasionally occur. Info is used internally for training and case studies. ERRC application owner and application team manages the information and creates a request to either delete or archive records.

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.

Information is voluntarily provided by the individual involved or provided to GSA by the individual via email. Individuals supply the information they believe is needed to resolve their inquiry and permit follow-up contact by the Government.

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?

System collects the following PII;

- Full Name
- Physical address;
- Phone number;
- Email address;
- Agency Name
- Vendor
- GSA Program - Types of Services needed/requested
- Documents with Case Information

Documents related to case can be anything that is needed to resolve their queries such as agencies may send a formal letter of appeal from a transferring employee, challenging the appraised value. Oftentimes the appeals are very personal regarding the employee's living situation or financial situation.

The information collected by GSA with regards to Agency employees / contractor is bare minimum and is required for GSA to assist the Agency employees in providing requested services. All privacy controls are in place in accordance with GSA's Privacy Policies and Procedures.

The information collected by GSA with regards to Agency employees / contractor is the minimum required for GSA to assist the Agency employees in providing requested services. The agency sends the information necessary to review, analyze and comment and some of the information is PII and some is not.

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?

ERRC does not aggregate or create new data about individuals that could be used to identify individuals.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

This control is implemented by the Salesforce Organization. Assigned authorizations for controlling access are enforced through Force.com, which is a part of Salesforce. Administration Setup Permission Sets & Public Groups.

1.) Practice least privilege permissions, where any user of the ERRC Salesforce app will have only the minimum privileges necessary to perform their particular job function.

2.) Assign a designated application owner. That application owner will:

- *receive auto-generated emails from the GSA Helpdesk (ServiceNow) to review and either approve/reject or ask for additional clarification for any pending tickets regarding system modifications (including adding users to access the application);*
- *attend Security de-briefs, to review and then digitally sign updated security packages as appropriate and outlined by their respective Security team;*
- *work with release managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes*

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

No, the system does not monitor the public, employees or contractors. All logs of internal GSA associates who access the system are reviewed on a monthly basis per GSA policy.

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

Information relating to service requested from ERRC by Agency Employee / Contractor. The record can include documents provided by Agency Employee / Contractor.

Application activity logs can be produced when needed.

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?

ERRC does not use any reports to de-identify the data.

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?

Any PII is submitted voluntarily by the requestor, and not at the request of GSA. Therefore, any PII collected is deemed relevant to the request, by the requestor.

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?

No. ERRC does not share agency or employee information with anyone outside of ERRC generally. However, it may be disclosed in accordance with SORN routine uses.

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)?

Information is being directly provided by the individuals or indirectly provided by the agency that authorized to transfer the employee. It is the responsibility of the individual or agency to assure the data provided is correct.

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?

No. The ERRC application has no internal or external connections to other systems.

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?

The Program Manager and Application Owner are responsible for ensuring data is monitored for relevance and accuracy. In addition, the information is being directly provided by the individuals or indirectly provided by parties acting on behalf of the individual and whom the individual had contacted. It is the responsibility of the individual to assure the data provided is *correct. Apart from that GSA can also request to the employee or transferring agency if additional information is needed to assist in their inquiry.*

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?

- *ERRC users who have a designated responsibility and have been granted access to the application.*
- *Salesforce administrative staff has access to the system and all Salesforce System Administrators are required to have a GSA Short Name Account (SNA). The SNA is used to grant administrative access to workstations, servers, or sensitive applications. Salesforce System Administrators need administrative access to Salesforce orgs and minor applications in order to provide support to Salesforce users and their associated permissions, groups and sharing rules. Additionally, they require administrative access in order to effectively perform Salesforce deployments and data loads. Salesforce System Administrators are required to login with a SNA token to keep their administrative duties separated from their regular duties. System changes made by these users will be tracked by Created By & Modified By fields. Login activity to the ORG is reviewed by the ISSO, per GSA Policy, on a weekly basis. Additionally logs are downloaded and archived/reviewed on a monthly basis. Any unauthorized activity is reported to the Information System Security Manager (ISSM) and the GSA IT Service Desk upon discovery.*
- *All access is granted via a request made to the GSA IT Service desk (Service Now) which is then approved by the Salesforce minor application owner. Once approved, the user is then granted role-based access to the system by system administrators.*
- *This application is hosted in the Customer Engagement Org (CEO) of Salesforce. All GSA employees and contractors who require access to this application must have a Salesforce or Salesforce Platform license within CEO as well as one of the custom ERRC Permission Sets in order to have access to this application.*

- *Designated app owner has control over approving/denying user access requests (via ServiceNow).*
- *Practice least privilege permissions, where any user of the ERRC Salesforce app will have only the minimum privileges necessary to perform their particular job function.*
- *Salesforce system administrators operating within the Salesforce CEO org are required to have Tier 2S clearance to be granted their designated SNA account/credential. All System Administrators are required to access the system with provided SNA credentials. Designated by OPM, Tier 2S clearance is a moderate risk (formerly MBI Level 5B) required for Non-Sensitive Moderate Risk (Public Trust) positions.*
- *Using the aforementioned Profiles & Permissions the application allows users across GSA to set up primary controlled document records, and manage the collaboration, approval, and concurrence processes needed for the primary record. The application leverages a custom Salesforce.com data object to store information about the primary records, leverage Salesforce.com sharing settings and criteria-based sharing rules to control visibility and access to the primary records, and utilize a Visualforce user interface to allow users to add approvers and designate different approval types from one centralized approval step screen.*
- *There is permission (PS) set GSA ERRC - CRED for this application. This PS provides Create, Read. Edit and delete access to the users.*
- *Per GSA Salesforce Technical Guideline, profiles "GSA System Administrator" and "GSA System User" will receive access to all objects and fields at the profile level. These administrative profiles also will have modify all/view all access to all records in this application. This is an existing construct that will not be altered through this project.*

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

Yes, Salesforce is an element in the Enterprise Application Services (EAS) SSP with an ATO expiration date of 3/25/2023.

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

As Salesforce is a cloud-based product, the minor application is protected by a multitier security process. The cloud platform along with GSA's implementation of security controls provides a robust security profile. The data is protected by multiple access controls to the data, including login controls, profiles within the application and permission sets in the program. Program management has authority to grant access to the application at all application levels. All higher level system support staff is granted access based upon need to know/requirement based needs.

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?

Intrusion systems at the agency level provide a layer of security monitoring. Access to the GSA ORG unit is reviewed on a weekly basis, application permission sets are annually reviewed by the application owner.

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.

GSA does not actively solicit any information from individuals. Any information submitted by individuals (personal or otherwise) is completely voluntary. Additionally an individual would not request information to be sent to them. Agency and individuals are sending information to ERRC.

7.2 What procedures allow individuals to access their information?

Should an individual request access to their information, it can and would be provided, in accordance with GSA's Privacy Act Rules at 41 C.F.R. 105-64 et seq..

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

Individuals supply the original information. If information relevant to the inquiry is incorrect, it would be amended as part of the inquiry resolution.

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 GSA employees and contractors with access to this system are required to complete IT Security Awareness and Privacy Training on an annual basis. Users who fail to comply may have all access to GSA systems revoked. High level system users receive annual role-based training for accessing systems with elevated rights. Those who fail to comply have access revoked.

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?

Salesforce event monitoring is available for activity audits. Designated app owner has control over approving/denying stakeholder user access requests (via ServiceNow). Salesforce system administrators operating within the Salesforce CEO org are required to have Tier 2S clearance and use their designated SNA account. Access controls are monitored in accordance with GSA IT Policy.

---

[1] 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."

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