Employee Relocation Resource Center (ERRC)

Privacy Impact Assessment

June 13, 2019

POINT *of* CONTACT

Richard Speidel

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

Stakeholders

Name & Email of Information System Security Manager (ISSM):

- Thomas Eaton - Thomas.Eaton@gsa.gov
- Katie Jaworski - katie.jaworski@gsa.gov

Name & Email of Program Manager/System Owner:

- Julie Blanford - julie.blanford@gsa.gov
-

Signature Page

Signed:

_____

Information System Security Manager (ISSM)

_____

Program Manager/System Owner

_____

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for evaluating the PIAs for completeness of privacy related information.

Table of contents

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?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

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?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

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?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about *Employee Relocation Resource Center (ERRC). The Travel and Transportation office part of FAS* may, receive and store and collect personally identifiable information ("PII") about the people who are requesting information and action from GSA. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name and address.

GSA uses Privacy Impact Assessments (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 1974.[2]

System, Application or Project

Employee Relocation Resource Center

System, application or project includes information about

Federal employees and Contractors that are requesting relocation services from GSA.

System, application or project includes

- Full Name
- Personal address
- Personal or work phone number
- Agency Name
- Vendor Company Name
- Vendor Contact's Full Name
- GSA Program - Types of Services needed/requested
- Documents with Case Information
- Names and email addresses (personal or work) may be stored in searchable data fields, but other data is only contained in documents attached to system records.
- 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.

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. They provide a streamlined acquisition process, flexible programs, subject matter expertise and program support. 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.

The Agency employees / contractors utilizing ERRC services contact ERRC with request for relocation services. The system collects Agency employee / contractor name, contact information, Agency name, Vendor assisting Agency employee and documents providing information on requesting services with justification.

The system records the service information for Agency Employee / Contractor on request. 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 Why is GSA collecting the information?

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.

- Full Name
- Personal address
- Personal or work phone number
- Agency Name
- Vendor Company Name

- Vendor Contact's Full Name
- GSA Program - Types of Services needed/requested
- Documents with Case Information
- Names and email addresses (personal or work) may be stored in searchable data fields, but other data is only contained in documents attached to system records.

1.2 What legal authority and/or agreements allow GSA to collect the information?

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

Relocation procurement under the Schedule 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 Schedule 48 SINs 653-1 and 653-5) 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

1.3 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?

Records may be retrieved by Agency employee / contractor names, Agency name, 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.

1.4. 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*:*

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

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.

ERRC follows the federal record retention policy of 7 years from the date the record was created in Salesforce. The information is retained for reference in further appeals or congressional inquiries, which occasionally occurs. 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.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

No. Requestors voluntarily submit information attached to a request that they decide to initiate.

There are potential privacy risks due to the type of information being submitted. ERRC will mitigate those risks in the following ways:

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.

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.

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.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

No. As discussed above, information is voluntarily provided by the individual involved or provided to GSA on behalf of the individual via email. This information is only accessed by those who need to review it.

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?

Names and email addresses for Federal employees, vendors and contractors may be included.

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

- 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.

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

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.

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?

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

3.5 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

3.6 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.

3.7 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.

3.8 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?

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

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

All information collected is necessary, but voluntary. Agencies may share private or sensitive information depending on the issue, however it is not shared or accessed by anyone outside the ERRC team.Therefore privacy risks are minimal .

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?

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, how and is a formal agreement(s) in place?

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

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Not applicable as there is no external information sharing. The application data is not shared outside ERRC

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?

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.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

No, as each GSA Program Manager and System Owner is responsible for maintaining the accuracy and completeness of the information under their control, each product owner decides who gets access to their application and what kind of visibility is needed.

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 also have access to the system. 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 either 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 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 3/20/2020.

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

As Salesforce is a cloud-based product, the minor application is protected by a multitiered 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 are granted access based upon need to know/requirement based needs.

6.4 Are there mechanisms in place to identify 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.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

As with any application there are risks and GSA is required to follow all Federal mandates to secure information systems, regardless of PII status. By adhering to those mandates, GSA provides a high threshold of data security for data within its Information Systems.

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.

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.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Individuals who have submitted information have no access to data once it has been submitted since this is an internal application. The individual will not need access to the information as they are the originator of information and would have no need to ask for a copy.

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.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

GSA employees and contractors who use 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. These trainings help users identify and report potential incidents and decrease the risk that authorized users will access or use the applicants' data for unauthorized purposes.

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?

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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

- Designated app owner has control over approving/denying stakeholder user access requests (via ServiceNow). App owners are required to conduct annual reviews of all users granted access to ensure continued/proper access it required.
- 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. App owners are required to conduct annual reviews of all users granted access to ensure continued/proper access is required

- Salesforce system administrators operating within the Salesforce CEO org are required to have Tier 2S clearance and use their designated SNA account.

---

[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.