GSA IT Hire

[Enterprise Application Services (EAS) -, Salesforce - Employee Engagement Organization (EEO) Minor App]

Privacy Impact Assessment (PIA)

July 13, 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:

- Rachel Surick

Signature Page

Signed:

DocuSigned by:
Matthew Regan
92526A8616CB470...
Information System Security Manager (ISSM)

DocuSigned by:
Rachel Surick
03461628D4E84CB...
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

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 *GSA IT Hire.* To accomplish its mission GSA Information Technology (IT) must, in the course of *GSA IT Hire* 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:

Enterprise Application Services (EAS) - Salesforce - Employee Engagement Organization (EEO) - GSA Information Technology (IT) Hire (EAS-Salesforce-EEO-GSA IT Hire)

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

Members of the public

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

To date, 17,067 records have been generated within the minor app.

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

A listing of all fields and descriptions can be found below:

- Applicant Email Address
- Applicant Name
- Best Contact Number
- phone number of the applicant
- City and State, or Zip Code
- Current Employer (optional)
- Link #1 (optional)
- Links 1-3 are optionally required fields where a submitter may share links to GitHub, LinkedIn, or other professional social media platforms.
- Link #2 (optional)
- Link #3 (optional)
- Resume
- Plain text resume for the applicant
- U.S. Citizen
- Simple yes/no asking if the individual is a US Citizen. Some federal jobs require US Citizenship as a prerequisite.
- Veterans' Preference Claim (optional)

- Allows an applicant to designate the veterans' preference claim that is applicable to them
- Veteran Status (US Armed Forces) (optional)
- Simple yes/no asking if the individual is a veteran of the US Armed Forces

Overview

GSA Information Technology (IT) used to collect resumes from a distribution email address, and all applications were stored in a single inbox. That method of data intake makes it very difficult for hiring managers to keep track of all resumes and whether or not those potential candidate applications have been reviewed by other GSA IT Hiring Managers. Due to the lack of visibility and collaboration, hiring managers were unable to effectively report on data, as well as filter applications based on functional area, and profile information.

GSA IT has developed a web based form that collects data of potential IT Professionals interested in working for GSA IT. The web based form collects basic contact information of the candidates, their plain text resume, their functional skills, their professional or technical associations (Linkedin, GitHub etc.), Veteran status and other relevant information.

This web based application helps GSA meet the following objectives:

- Real time statistics of user traffic, reporting based on Customer flow for on demand reporting and analytics
- Effectively and efficiently utilize data to target potential candidates
- Leverage interested candidates data reports for current and future job opportunities within GSA IT and easily track potential candidate information without duplicating manual team efforts to ensure quality and up to date information

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?

Federal agencies rate applicants for Federal jobs under the authority of sections 1104, 1302, 3301, 3304, 3320, 3361, 3393, and 3394 of title 5 of the United States Code

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?

Data can be searched by name or by unique resume ID numbers. Resumes can be browsed by skills and other qualified content. SORN GSA-CIO-3 at 79 FR 47138 covers all data used within the Salesforce GSA boundaries.

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 IT Hire 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.

a. GRS 02.1/050 Job Vacancy Case Files -Records Of Onetime Competitive And Senior Executive Service (SES) Announcements/Selections.

Description: Job vacancy case files. Case files an agency creates when posting and filling competitive job vacancies. Also known as case examining, competitive examination, or merit case files.

Retention Instructions: Temporary. Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later.

b. GRS 02.1/051 Job Vacancy Case Files - Records Of Standing Register Competitive Files For Multiple Positions Filled Over A Period Of Time.

Description: Job vacancy case files. Case files an agency creates when posting and filling competitive job vacancies. Also known as case examining, competitive examination, or merit case files.

Retention Instructions: Temporary. Destroy 2 years after termination of register.

c. GRS 02.1/060 Job Application Packages.

Description: Application packages for competitive positions, in USAJobs or its successors, and other systems, whether electronic or analog.

Retention Instructions: Temporary. Destroy 1 year after the date of submission.

d. GRS 02.1/090 Interview Records.

Description: Case files related to filling job vacancies, held by hiring official and interview panel members.

Retention Instructions: Temporary. Destroy 2 years after the case is closed by hire or non-selection, expiration of right to appeal a non-selection, or final settlement of any associated litigation, whichever is later.

e. GRS 02.1/120 Special Hiring Authority Program Records.

Description: Records an agency creates and receives that document its administration of special hiring authority programs such as summer, student, intern, and other temporary hiring authorized by OPM.

Retention Instructions: Temporary. Destroy 2 years after hiring authority closes but longer retention is authorized if required for business use.

f. GRS 02.1/130 Records Related To Individual Employees Hired Under Special Temporary Authority.

Description: Includes participant agreement, records of mentoring, documentation that employee fulfilled educational and other requirements, and conversion to a permanent position.

Retention Instructions: Temporary. Destroy 2 years after the employee is converted to a permanent position or leaves a program but longer retention is authorized if required for business use.

g. GRS 02.1/141 Pre-Appointment Files - Records Appropriate For Inclusion In The OPF - Prospective Employees Who Enter On Duty.

Description: Records created when vetting a prospective employee between the time a job offer is accepted and the time employee enters on duty. Such as designation of beneficiary, life insurance election, and health benefits registration.

Retention Instructions: Forward to appropriate human resources office to include in OPF after employee enters on duty.

h. GRS 02.1/142 Pre-Appointment Files - Records Appropriate For Inclusion In The OPF - Prospective Employees Who Do Not Enter On Duty.

Description: Records created when vetting a prospective employee between the time a job offer is accepted and the time employee enters on duty. Such as designation of beneficiary, life insurance election, and health benefits registration.

Retention Instructions: Temporary. Destroy 1 year after the prospective employee is no longer a candidate. DAA-GRS-2014-0002-0009 (GRS 02.1/142)

i. GRS 02.1/143 Pre-Appointment Files - Copies Of Records Included In Job Vacancy Case Files (Items 50-51).

Description: Records created when vetting a prospective employee between the time a job offer is accepted and the time employee enters on duty.

Retention Instructions: Temporary. Destroy after the prospective employee enters on duty, declines appointment, or is no longer a candidate.

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.

Yes, an individual is notified by a Privacy Notice displayed on the first page of the application and prior to the applicant "Submit" button for sharing their data. The Privacy Notice displayed follows:

Privacy Act Statement. Federal agencies rate applicants for Federal jobs under the authority of sections 1104, 1302, 3301, 3304, 3320, 3361, 3393, and 3394 of title 5 of the United States Code. We need the information requested and in any associated vacancy announcements to evaluate your qualifications. Other laws require us to ask about citizenship, military service, etc. Failure to furnish the requested information may delay or prevent action on your application. Incomplete addresses and ZIP Codes, personal email addresses, social networking profiles, or other information may slow processing. We may confirm information from your records with prospective nonfederal employers concerning tenure of employment, civil service status, length of service, and date and nature of action for separation as shown on personnel action forms of specifically identified individuals. For routine uses and other relevant information, please see GSA-CIO-3 for the system of records notice (79 F.R. 47138). https://www.federalregister.gov/documents/2014/08/12/2014-19071/privacy-act-of-1974-notice-of-an-updated-system-of-records

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?

The PII data requested is the minimal amount needed for the GSA IT managers to contact an individual.

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?

No, we are not collecting or aggregating any new data outside of what is requested on the form. If an individual submits the form multiple times, the data would be stored as separate records in the system. Multiple submissions of the form would not enhance an individual's standing or competitiveness within the organization.

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 Administration Setup Permission Sets & Public Groups.
1.) Practice least privilege permissions, where any user of the GSA IT Hire 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 IT Service Desk (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 debriefs, 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?

While reporting is a capability within this application, much of the data to be consumed is longform text which is not conducive to reports.

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?

Users have the ability to de-identify records when producing ad-hoc reports. This is accomplished by choosing to not include any identifying information when pulling a report.

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?

Data will not be shared with any external entities.

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. It is the responsibility of the individual 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, there are 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. It is the responsibility of the individual to assure the data provided is correct. Applicant entries are one time entries of contact information and resumes. There is not a direct means for an individual to update their information. In the event that someone moves to a new address or would like to update the content of their resume, there are two options available.

1) The submitter creates a new submission via the form. Upon receipt, the program office will consider the new submission and no longer use the old submission.

2) The submitter can contact the GSA IT Hire team via e-mail and request an update to their information.

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?

● 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 the CEO as well as one of the custom GSA IT Hire Permission Sets in order to have access to this application.
● Designated app owners have control over approving/denying user access requests (via ServiceNow).
● Practice least privilege permissions, where any user of the GSA IT Hire 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.
● 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 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?

GSA IT Hire is a Salesforce Minor application in the CEO ORG which falls under EAS (Enterprise Application Services); EAS SSP authorization expires March 31, 2021.

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

Salesforce is a cloud-based product, the minor application is protected by a multi tiered security process. The cloud platform along with GSA’s implementation of security controls provide 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 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.

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.

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

In the event that the submitter would like to change or correct information that was submitted, they can contact the GSA IT Hire team via e-mail. The e-mail address is shared on the form, the post-submission thank you page, and in a confirmation e-mail. Additionally, the submitter may submit the form again and create a new record.

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.

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?

GSA IT Hire is identified as a Minor Application within Salesforce. Salesforce event monitoring is available for activity audits. Designated app owners have control over approving/denying stakeholder user access requests (via ServiceNow). Salesforce system administrators operating within the Salesforce EEO org are required to have Tier 2S clearance and use their designated SNA account. Access controls are monitored in accordance with GSA IT Policy. Admins are also required to complete annual privacy training and security awareness training for users with elevated privileges.

---

[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.