TTS Applicant Tracker

Privacy Impact Assessment

10/1/2018

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

richard.speidel@gsa.gov

Instructions for GSA employees and contractors:

This template is designed to assist GSA employees and contractors in complying with the E-Government Act of 2002, Section 208, which requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses processes; and can cover all of the systems, applications or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application or project's life cycle. The completed PIA demonstrates how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are made available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts 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. For example:

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

An example of a completed PIA is available at: https://www.gsa.gov/portal/getMediaData?mediaId=167954

If you have any questions, send them to gsa.privacyact@gsa.gov.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Revised to include questions about third party services on websites and robotics process automation (RPA).	2.0
6/26/2018	New question added to Section 1 regarding "Information Collection Requests"	2.1
7/25/2018	Created for Salesforce minor app (TTS Applicant Tracker)	3.0

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 TTS Applicant Tracker, a Salesforce application. Technology Transformation Services (TTS), Office of Operations does collect personally identifiable information ("PII") about the people who express interest in and/or apply for positions using this Salesforce application. 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, 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

TTS Applicant Tracker (Salesforce minor app)

System, application or project includes information about

Application may collect data from Government Employees, Contractors and/or the General Public

System, application or project includes

System will intake user information provided by prospective applicants interested in applying for a position within the Technology Transformation Services (TTS):

- Name and other biographic information (e.g., employment eligibility)
- Contact Information (e.g., address, telephone number, email address)

Note that users are instructed NOT to include Social Security Number or other sensitive government-issued identifiers on any forms they submit. However, due to the nature of the application, users cannot be stopped from uploading documents containing potentially sensitive information.

Overview

This application is designed to capture prospective job applicants' information for those individuals interested in and/or applying for a non-competitive position within the Technology Transformation Services (TTS) division of GSA. Job announcements for TTS are posted online at: https://join.tts.gsa.gov/. The new applicant tracking Salesforce App will capture potential applicant data; provide a defined workflow following GSA OHRM requirements; and creates a secure environment for TTS to process applicants through the various stages of hiring review. The data collected are covered under Office of Personnel Management SORN OPM-GOVT-5. OPM is authorized to rate applicants for Federal jobs under sections 1302, 3301, and 3304 of title 5 of the U.S. code. Section 1104 of title 5 allows the Office of Personnel Management to authorize other Federal Agencies to rate applicants for Federal Jobs.

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 applicant tracking Salesforce App captures potential applicant data, provides a defined workflow, and guides TTS hiring stakeholders and applicants through the various stages of hiring review. Applicants are required to submit certain required information in order to be considered for job candidacy. Relevant PII data is collected to provide hiring stakeholders information on applicants that allows them to remain in contact when applicable job announcements are posted.

1. The application owner will have the ability to easily import a list of new applicants and jobs data in comma separated value (.csv) format into the TTS applicant tracker application (via the Salesforce Data Import Wizard)
    a. Support all new job applicants as they begin the process
2. TTS Hiring Managers are easily able to see the hiring status for the various job postings, and the status associated to subsequent applicants
3. TTS Hiring Personnel are easily able to collaborate and rate applicants for job postings in a centralized location
    a. TTS Hiring Personnel can be assigned to fill a role (phone screen, interview, SME) for a particular job posting or for a group of job applicants
    b. A systematic workflow is in place which requires the input from various

hiring personnel in order to move an applicant through the hiring process

4. Veterans preference can be assigned to applicants who have veteran status.
    a. Visibility of an applicant's veteran status will only be visible to individuals with a need to know
    b. When Jobs have Applications with Veteran's Preference, these applications must be dispositioned prior to any Applications without a Veteran's Preference.

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

Office of Personnel Management is authorized to rate applicants for Federal jobs under sections 1302, 3301, and 3304 of title 5 of the U.S. code. Section 1104 of title 5 allows the Office of Personnel Management to authorize other Federal Agencies to rate applicants for Federal Jobs.

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?

There are two type of internal GSA users of the TTS Applicant Tracker app:

- 'Admin' access can view all Applicants' Name, Phone, Email, city, state, zip code. This level of access is only available to TTS recruiters.
- 'Reviewer' access can view an individual applicant's Name, Phone, Email, city, state, zip) that they have been assigned to review. This level of access is only assigned to interviewers for specific positions.

Upon submitting interest in a position, the applicant has a contact record created, that may be searched by applicant name. Once the applicant has completed the submission, they are no longer able to track any progress. All applicant information that is gathered is stored in the system, and only accessible by individuals as noted above. All requests for status must be submitted via email.

SSNs are not required to be submitted at any time during expression of interest in any job posting. However, as there is a form submission which is specifically for uploading the applicants resume, the potential exists that SSNs may be submitted. Applicants are encouraged to NOT include SSNs on resume.

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.

Not applicable because this is not an information collection request.

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.

Applicant records will be maintained in accordance with General Records Schedule 2.1, Item 50 which specifies a two year retention policy. For example, any applicant who has not applied to a TTS position during the previous two fiscal year periods will be subject to a removal of records. This removal of records process will occur in tandem with each fiscal year change. However, the system will allow the flexibility for the Application Owner to request that entire records are deleted by a Salesforce administrator, or that a subset of certain fields within the applicant's records are deleted by a Salesforce administrator.

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

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

1.) Practice least privilege permissions, where any user of the Applicant Tracking Salesforce app will have only the bare minimum privileges necessary to perform their particular job function. For example, "Recruiters" as defined in Salesforce may view an applicant's Veteran derived preference as they have a need-to-know. However, a "Subject Matter Expert" (SME) as defined in Salesforce conducting an interview of an applicant may not view an applicant's Veteran derived preference.

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 (including adding users to access the application);
- attend Security de-briefs, to review and then digitally sign updated security pkgs as appropriate and outlined by your respective Security team;
- work with Release Managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes; and

- ensure NO sensitive information is sent into the Helpdesk ticket requests in text form or via attached documents/snapshots.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

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

Yes. The application provides a link to a privacy notice on the application form, so that potential job applicants can review prior to submission. The aforementioned privacy notice link is presented before the submit button on the job application form. Job announcements for TTS are posted online at, https://join.tts.gsa.gov/ this site highlights an email address where individuals can contact the talent team with any questions, including, the request that their data be removed.

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

N/A

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?

Application will collect information from prospective employees who are interested in employment with GSA TTS. Those individuals may be general public, current government employees and/or contractors.

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

Eligibility Requirements: “All United States citizens and nationals (residents of American Samoa and Swains Islands) are eligible to apply.” Do you meet the eligibility requirements? (Y/N)

Preferred Name, Email, Best Phone Number, City, State, ZIP Code, Ability to work full-time (Y/N), Preferred Work location (Picklist), Where did you learn about this opportunity (Picklist), Up to 3 URL links to resume, portfolios or other online presence, Resume (Text Box), Why do you want to join this organization (Text Box), Tell us why you're interested in the role you're applying for (Text Box).

"Are you a Veteran of the U.S. Armed Forces or are you eligible for derived preference?" (Picklist below)

- No, I do not claim Veterans' Preference.
- 0-point Sole Survivorship Preference (SSP).
- 5-point preference based on active duty in the U.S. Armed Forces (TP).
- 10-point preference based on a compensable service connected disability of at least 10% but less than 30% (CP).
- 10-point preference based on a compensable service connected disability of 30% or more (CPS).
- 10-point preference for non-compensable disability or Purple Heart (XP).
- 10-point preference based on widow/widower or mother of a deceased veteran, or spouse or mother of a disabled veteran (XP).

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

The collection of PII is necessary for TTS to recruit and hire The information is utilized to contact the applicant and validation of the applicant's eligibility.

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?

No aggregate data is created as a result of any system actions.

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

1.) Practice least privilege permissions, where any user of the Applicant Tracking Salesforce app will have only the bare minimum privileges necessary to perform their particular job function. For example, "Recruiters" as defined in Salesforce may view an applicant's Veteran derived preference as they have a need-to-know. Whereas a "Subject Matter Expert" (SME) as defined in Salesforce conducting an interview of an applicant, may not view an applicant's Veteran derived preference.

2.) Assign a designated application owner. App 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 (including adding users to access the application);
- attend Security de-briefs, to review and then digitally sign updated security pkgs as appropriate and outlined by your respective Security team;
- work with Release Managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes; and
- ensure NO sensitive information is sent into the Helpdesk ticket requests in text form or via attached documents/snapshots.

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

There are no logs generated when a prospective hire submits the information other than the data that has been submitted. 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?

The reports that the tool supplies are at the Summary level of Job and Application Status.
'Admin' users can create reports Admins, may create query to find a users contact record, which is tied to the summary of job and application status.
'Reviewer' users have no reporting access.

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?

N/A

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

All data captured is relevant to the hiring process. Data that is not required is optional and users are instructed NOT to include Social Security Number or other sensitive government-issued identifiers on any forms they submit.

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?

All data captured is relevant to the hiring process. Data that is not required is optional.

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 is generally not shared with any other agencies, applications or systems. Dashboard reporting is contained within the Salesforce ORG, and is not shared outside of the ORG or with any other applications, agencies or systems. However, with the applicant's permission, TTS recruiters may refer an applicant to State and local governments, congressional offices, international organizations, and other public offices for employment consideration.

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)?

Accuracy of data is ensured since it is being collected directly from the job applicants themselves during the application process. Users will receive a confirmation message upon submission of data. It will contain "what they submitted". Message will contain contact information to report any incorrectly submitted information or to submit updated information.

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 interaction with other internal applications or 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?

The application does not share information with USAJobs or any other system. However, an applicant may opt-in to be considered for other employment opportunities within the U.S. government. In that case, TTS will track that information because other agencies sometimes alert the TTS project team that they are looking to hire someone. The project team then asks the TTS Talent group if they know of anyone who might be a fit. At that point, if it does, the Talent team reaches out to the candidate to see if the candidate would be interested in exploring that opportunity and if so, the TTS Talent group securely shares candidate's resume with that agency contact.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Accuracy of data is ensured since it is being collected directly from the job applicants themselves during the application process. Users will receive a confirmation message upon submission of data. It will contain "what they submitted". Message will contain contact information to report any incorrectly submitted information or to submit updated information.

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?

Job announcements for TTS are posted online at, https://join.tts.gsa.gov/ this site highlights an email address where individuals can contact the talent team with any questions, including, the request to update data which may have been entered incorrectly by the applicant during the application process. A talent team member will respond once the data update has been completed.

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?

TTS users who have a designated responsibility in the hiring process and have been granted access to the application, this may include recruiters, subject matter experts and managers. Salesforce administrative staff also have access to the system. All access is granted via a request 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.

- Designated app owner has control over approving/denying hiring stakeholder user access requests (via ServiceNow).
- Practice least privilege permissions, where any user of the Applicant Tracking Salesforce app will have only the bare minimum privileges necessary to perform their particular job function. For example, “Recruiters” as defined in Salesforce may view an applicant’s Veteran derived preference as they have a need-to-know. Whereas a “Subject Matter Expert” (SME) as defined in Salesforce conducting an interview of an applicant, may not view an applicant's Veteran derived preference, therefore the field will be removed from their page layout.
- Salesforce system administrators operating within the Salesforce PEO org are required to have Tier 2S clearance and use their designated SNA account.

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

Salesforce is an element in the EAS SSP with an ATO expiration date of 3/21/2019

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 multi-tiered 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, 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.

Job announcements for TTS are posted online at, https://join.tts.gsa.gov/ this site highlights an email address where individuals can contact the talent team with any questions, including:

- the request to obtain a copy of their data on record (found by the hiring team within the Salesforce App).
- the request that their data be removed.
- the request to update data which may have been entered incorrectly by the applicant during the application process.

In all cases, a talent team member will respond once the data update has been completed.

7.2 What procedures allow individuals to access their information?

Job announcements for TTS are posted online at, https://join.tts.gsa.gov/ this site highlights an email address where individuals can contact the talent team with any questions, including:

- the request to obtain a copy of their data on record (found by the hiring team within the Salesforce App).
- the request that their data be removed.
- the request to update data which may have been entered incorrectly by the applicant during the application process.

In all cases, a talent team member will respond once the data update has been completed.

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

Job announcements for TTS are posted online at, https://join.tts.gsa.gov/ this site highlights an email address where individuals can contact the talent team with any questions, including:

- the request to obtain a copy of their data on record (found by the hiring team within the Salesforce App).
- the request that their data be removed.
- the request to update data which may have been entered incorrectly by the applicant during the application process.

In all cases, a talent team member will respond once the data update has been completed.

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?

Users have no access to data once it has been submitted. Upon submission of data, users will receive an email confirmation of all data that has been submitted. Job announcements for TTS are posted online at, https://join.tts.gsa.gov/ this site highlights an email address where individuals can contact the talent team with any questions, including, the request to update data which may have been entered incorrectly by the applicant during the application process. A talent team member will respond once the data update has been completed.

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 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?

All GSA employees 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 hiring stakeholder user access requests (via ServiceNow). Salesforce system administrators operating within the Salesforce PEO org are required to have Tier 2S clearance and use their designated SNA account.

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 hiring stakeholder user access requests (via ServiceNow).
- Practice least privilege permissions, where any user of the Applicant Tracking Salesforce app will have only the bare minimum privileges necessary to perform their particular job function. For example, "Recruiters" as defined in Salesforce may view an applicant's Veteran derived preference as they have a need-to-know. Whereas a "Subject Matter Expert" (SME) as defined in Salesforce conducting an interview of an applicant, may not view an applicant's Veteran derived preference, therefore the field will be removed from their page layout.
- Salesforce system administrators operating within the Salesforce PEO 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.