GSAJOBS

Privacy Impact Assessment

12/04/2018

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

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
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
9/25/2018	**Updated PIA as it pertains to GSAJOBS**	**2.2**

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 GSAJOBS. GSA IT may, in the course of GSAJOBS, 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, 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

GSAJOBS

System, application or project includes information about

Applicants applying to GSA Federal Government job positions.

System, application or project includes

- Name and other biographic information (e.g., date of birth)
- Contact Information (e.g., address, telephone number, email address)
- Social Security Number, Driver's License Number or other government-issued identifiers
- Financial Information

Overview

The GSA Hiring Management System (GSAJOBS) is a web-based application used by the General Services Administration (GSA) as a tool for electronic automation of staffing and HR management related functions used by the Office of Human Resources Management (OHRM). GSA's GSAJOBS system resides on Monster's Hiring Management Enterprise System (MHME) that has a leasing agreement with GSA to provide the application's online services. GSA HR users access the GSAJOBS application via the Internet and use the tool for creating and managing vacancies, notifying potential applicants of those vacancies via the Internet, collecting and

processing applicant data, ranking applicant qualifications based on such data, and allowing managers to view qualified applicants via an online certificate of eligible applicants. Information stored and processed by the MHME includes vacancy data such as job descriptions, questions, and criteria; as well as applicant data such as resumes, contact information, and social security numbers.

GSA HR uses GSAJOBS to build and post vacancies directly to USAJOBS to collect applications. Applicants create profiles in USAJOBS with basic, personal, and document information, and when they apply to a vacancy, are directed to the GSAJOBS Seeker with that information to complete and submit their application. While most applicants log into GSAJOBS to access the Seeker site, some applicants who are onboarded directly through GSAJOBS can log directly into the GSAjobs system.

PII Collected shown below. All PII collected is for the purpose of applying for employment at GSA from all job applicants.

- Name
- Email Address
- Home Address
- Social Security Number (SSN) (Only last four digits are visible)
- Date of Birth
- Home address and telephone number
- Resume / Employment history
- Race and National Origin data (optional**)

System of Records Notices (SORNs) -

- OPM-GOVT-5, 71-FR-35351 June 19, 2006

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 GSA Hiring Management System (GSAJOBS) is a web-based application used by the General Services Administration (GSA) as a tool for electronic automation of staffing and HR management related functions used by the Office of

Human Resources Management (OHRM). GSA's GSAJOBS system resides on Monster's Hiring Management Enterprise System (MHME) that has a leasing agreement with GSA to provide the application's online services. GSA HR users access the GSAJOBS application via the Internet and use the tool for creating and managing vacancies, notifying potential applicants of those vacancies via the Internet, collecting and processing applicant data, ranking applicant qualifications based on such data, and allowing managers to view qualified applicants via an online certificate of eligible applicants. Information stored and processed by Monster's MHME includes vacancy data such as job descriptions, questions, and criteria; as well as applicant data such as resumes, contact information, and social security numbers. Job applicants use the MHME system to apply for GSA positions via USAjobs.

GSA's GSAJOBS Software as a Service (SaaS) provided by Monster relies on Monster's MHME hardware and software. The system has been designed to comply with the following laws, regulations, policies and legal authorities:

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

The nature of the system requires it. The Privacy Act of 1974 is a federal law that governs our collection and use of records we maintain on you in a system of records. In addition 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are the authorities for maintaining personnel information. Authorities for recording Social Security Numbers are E.O. 9397, 26 CFR 31.6011(b)–2, and 26 CFR 31.6109–1.

1.3 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?

System of Records Notice (SORN) -

- OPM-GOVT-5, 71-FR-35351 June 19, 2006

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 ICR has been submitted.

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.

GSAJOBS complies with all GSA retention and disposal procedures specified by 1820.1 CIO P GSA Records Maintenance and Disposition System. Records contained in the HR Links system will be retained consistent with section 2.2 of NARA General Records Schedule, "Employee Management Records". See https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf. Disposition Authority Number: DAA-GRS-2016-0014-0001 - Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.

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

No, GSAJOBS is a back-end management tool for creating and managing vacancies, notifying potential applicants of those vacancies via the Internet, collecting and processing applicant data, ranking applicant qualifications based on such data, and allowing managers to view qualified applicants via an online certificate of eligible applicants.

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, notice is provided via System of Records Notice (SORN) OPM-GOVT-5, 71-FR-35351 June 19, 2006, the Privacy Act Notice on USAjobs.gov and this PIA which is available at gsa.gov/PIA

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, this PIA and notices provided during the application process address notice, consent and transparency requirements.

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?

All applicants seeking employment at GSA

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

PII Collected shown below. All PII collected is for the purpose of applying for employment at GSA from all job applicants.

- Name
- Email Address
- Home Address
- Social Security Number (SSN) (Only last four digits are visible)
- Date of Birth
- Home address and telephone number
- Resume / Employment history
- Race and National Origin data (optional**)

The PII collected can be seen by GSA HR specialists and managers who have requested applicants for open positions.

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

The GSAJOBS Hiring Management System (GSAJOBS) is a web-based application used by the General Services Administration (GSA) as a tool for electronic automation of staffing and HR management related functions used by the Office of Human Resources Management (OHRM). GSA's GSAJOBS system resides on Monster's Hiring Management Enterprise System (MHME) that has a leasing agreement with GSA to provide the application's online services. GSA HR users access the GSAJOBS application via the Internet and use the tool for creating and managing vacancies, notifying potential applicants of those vacancies via the Internet, collecting and processing applicant data, ranking applicant

qualifications based on such data, and allowing managers to view qualified applicants via an online certificate of eligible applicants.

Information stored and processed by Monster's MHME includes vacancy data such as job descriptions, questions, and criteria; as well as applicant data such as resumes, contact information, and social security numbers. Monster may access applicant data when working to resolve reported system issues, or to support GSAJOBS inquiries, or run reports.

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 GSAJOBS does not create or aggregate new data about the individual.

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

GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. GSAJOBS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

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

GSAJOBS does not monitor job applicants.

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

GSAJOBS may create reports related to job applicants for a particular position, job series or similar category.

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?

GSAJOBS does not de-identify data for reporting.

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

Given the reporting capability, the security and privacy measures include access controls, awareness and training for users and auditing capability to ensure accountability.

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?

GSAJOBS limits information to only what is required to carry out employment activities.

Monster may access applicant data when working to resolve reported system issues or to support GSAJOBS inquiries or run reports.

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?

GSAJOBS shares demographic information with OPM as federally mandated. See the "Purpose and Routine Uses for Demographic Information" section of the usajobs.gov Privacy Act Notice for additional information.

Monster may access applicant data when working to resolve reported system issues or to support GSAJOBS inquiries or run reports.

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)?

The information collected from job applicants is input directly into OPM's USAjobs. USAjobs then transfers the information collected directly into GSAJOBS Seeker when an applicant applies for a GSA vacancy.

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?

The GSAJOBS system resides on the MHME platform, which only interacts with USAjobs.

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?

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

Mitigation:
GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. GSAJOBS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

SECTION 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?

Individuals/job applicants provide and self-certify the accuracy of the information in the system.

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?

GSAJOBS data is logged and audited and otherwise controlled to ensure confidentiality, integrity and availability.

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?

GSAJOBS has individual and administrative role access to the data in the system. The access authorization is covered under the SP 800-53 access controls.

Monster may access applicant data when working to resolve reported system issues or to support GSAJOBS inquiries or run reports.

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

The GSAJOBS ATO was issued on 09-28-2018.

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

GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. GSAJOBS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. GSAJOBS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

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?

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

Mitigation:
GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. GSAJOBS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

SECTION 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.

The opportunities are defined with in the SORN that covers GSAJOBS: OPM-GOVT-5, 71-FR-35351 June 19, 2006

7.2 What procedures allow individuals to access their information?

Job applicants create accounts in USAJobs where they can access and modify information as needed. The information is forwarded to GSAJOBS.

GSA hiring managers gain access through GSA's Enterprise Access Request System (EARS) and the account information/changes would be processed through EARS.

EARS is used to provision, track, and audit GSA employee/contractor access to GSA applications. EARS works in conjunction with Rational ClearQuest for account approval, account management, and re-certification and has Authority to Operate under the Ancillary Financial Applications (AFA) FISMA Moderate boundary.

EARS ensures adherence to the "IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07" ensuring personnel authorization best practices are implemented and followed when authorizing application access. The use of EARS systematically implements the general activities for authorizing personnel to access IT resources.

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

Job applicants create accounts in USAJOBS where they can access and modify information as needed. The information is forwarded to GSAJOBS.

GSA hiring managers gain access through EARS and the account information/changes would be processed through EARS.

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?

GSAJOBS is a back-end management tool. Applicants may access or amend the information in the USAJobs account up until they submit it for review.

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.

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

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?

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

Mitigation:
GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. GSAJOBS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

SECTION 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?

GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ variety of security measures defined in the System Security Plan (SSP) designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, along with system and information integrity.

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?

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

Mitigation:
GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. GSAJOBS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

[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.