GSAJOBS

Privacy Impact Assessment (PIA)

March 26, 2021

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):

- Richard Banach - ISTF

Name of Program Manager/System Owner:

- Monica Shackelford - ICS

Signature Page

Signed:

DocuSigned by:
Richard Banach
21B998D30FCE4B6...

Information System Security Manager (ISSM)

DocuSigned by:
Monica Shackelford
0C9D8301687C4C8...

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 #
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation.	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
3/5/2020	Updated the PII BOT related responses	3.1
2/5/2021	Removed email field from signature page	3.2
3/26/2021	Updated - New ISSM and BOT Entry Removed - PIA Approved	3.3

Table of contents

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

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 (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 *[system, application, or project]*. To accomplish its mission *[GSA office]* must, in the course of *[program name]*, 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:

GSAJOBS – FISMA System: IC-GSAJOBS

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

Applicants applying to GSA Federal Government job positions.

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

850,000 unique records about applicants for GSA employment as of 2020.

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

- 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 identifier
- 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 on boarded 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 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate 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.

1.2 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?

System of Records Notice (SORN) - OPM-GOVT-5, 71-FR-35351 June 19, 2006

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 ICR has been submitted.

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.

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.

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, 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

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 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.

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

3.3 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.

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

GSAJOBS does not monitor job applicants.

3.5 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.

3.6 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?

GSAJOBS does not de-identify data for reporting.

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?

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)?

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

The GSA implementation of the GSAjobs application is a web-based SaaS interface. The boundary between the GSAjobs application and the FedRAMP authorized Monster Hiring Management Enterprise System (HMES).

The GSAJOBS system resides on the Monster's Hiring Management Enterprise System (MHME) platform, which interacts with USAJOBS. GSAJOBS is also connected to the GSA Enterprise Service Bus. Formal agreements are in place for both connections.

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?

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

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 (SSP) for the information system(s) or application?

The GSAJOBS ATO was issued on 01-31-2019.

(Note a new SSP will be developed on customer responsible controls, assessed and ATO will be issued).

6.3 How will the system or application be secured from a physical, technical, 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 and respond to 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.

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.

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 (Enterprise Access Request System) EARS and the account information/changes would be processed through EARS.

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 conduct annual refresher training.

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?

GSAJOBS has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a 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.

[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.