Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, 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]

[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.

General Information

PIA Identifier: 421
System Name: GSAJOBS
CPO Approval Date: 3/15/2023
PIA Expiration Date: 3/14/2026

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
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?
900,000 unique records about applicants for GSA employment as of 2022.

D: System, application, or project includes these data elements:
a. Name and other biographic information (e.g., date of birth)

b. Contact Information (e.g., address, telephone number, email address)

c. Social Security Number, Driver's License Number or other government-issued identifier

d. Financial Information

Overview:

The GSAJobs Hiring Management System is a web-based application used by the General Services Administration (GSA) Office of Human Resources Management (OHRM) as a tool for electronic automation of staffing and HR management related functions. Monster Government Solutions (MGS) is the FedRAMP authorized Software as a Service Provider that has a leasing agreement with GSA to provide the Monster Hiring Management Enterprise suite (MHME) online services. GSA HR users access the MHME suite 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 MHME includes employment-related data such as job vacancies, position descriptions, position requirements and necessary qualifications, applicant questions, and various other factual data. MHME also stores applicant information such as professional resumes, contact information, and social security numbers.

The overall purpose of MHME is to improve the hiring management process for customers by the automation of the process from the vacancy creation through applicant selection processes. MHME does this through several functions, including posting and managing vacancies, displaying those vacancies to potential employees via the Internet, collecting and processing employment application and applicant personal data (i.e. contact information), and ranking applicants' qualifications based on such data. In addition, the system provides email correspondence functionality that employ candidates. Once enrolled, the candidate could be notified of the respective hiring decisions. Interested parties can be notified of future job vacancies.

Monster Government Solutions (MGS) is utilized by automated tools (Bot), executed by TTS to retrieve resumes to enhance the user experience.

1.0 Purpose of Collection

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), and 26 CFR 31.610.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): 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

1.2b: Explain why a SORN is not required.
.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.
No ICR has been submitted.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
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.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
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). GSAJOBS system resides on Monster 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?
No

3.2 Explained: If so, how will this data be maintained and used?

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 anappropriately 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?
None

3.4 Explain: Please elaborate as needed.
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?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
GSAJOBS does not de-identify data for reporting.

3.6 Why Not: Why will the data not be de-identified?
N/A. No data will be de-identified

4.0 Limits on Using and Sharing Information

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?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Federal Agencies

4.2How: If so, how will GSA share the 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

4.3Other Source: 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?
Yes

4.4WhoHow: If so, who and how?
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 Monsters 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.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?
N/A

5.0 Data Quality and Integrity

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.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

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.

6.1b: What is the authorization process to gain access?
Monster may access applicant data when working to resolve reported system issues or to support GSAJOBS inquiries or run reports.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
3/25/2023

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?
Yes

6.4What: 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.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
The opportunities are defined with in the SORN that covers GSAJOBS: OPM-GOVT-5, 71-FR- 35351 June 19, 2006

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that 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 GSA 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?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

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.

9.0 Accountability and Auditing

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.