PRIVACY IMPACT ASSESSMENT

Gateway to State

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: July 2022
(b) Name of system: Gateway to State
(c) System acronym: GTS (Gateway to State)
(d) Bureau: Global Talent Management (GTM)
(e) iMatrix Asset ID Number: 843
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:
   □ New system
   □ Significant modification to an existing system
   ☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
   ☒Yes □No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
   ☒Yes □No

   If yes, has the privacy questionnaire in Xacta been completed?
   ☒Yes □No

(c) Describe the purpose of the system:

Gateway to State (GTS) is the Department of State (Department) system name for the
Monster Hiring Management Enterprise system (MHME), which is a commercial off the
shelf hiring service to automate the staff acquisition process. MHME, created and
operated by Monster Government Solutions (MGS), is a web-based job candidate
assessment tool that is accessible via the Internet through the USAJOBS website.
USAJOBS is the application used for posting and managing vacancies, displaying those
vакancies to potential employees (via the Internet), collecting and processing employment application and applicant personal data (i.e., contact information), and ranking applicants’ qualification based on such data.

In addition, the GTS provides email correspondence functionality so that once enrolled, employment candidates can be notified of the respective hiring decisions and interested parties can be notified of future job vacancies. The USAJOBS website is owned and operated by the Office of Personnel Management (OPM), which is responsible for the privacy and security aspects of applicant information up to the point where the application data in USAJOBS is moved into the applicant record under GTS. GTS’s primary function is to improve and streamline hiring management processes/efforts by automating recruitment activities.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Full Name
- Social Security Number (SSN)
- Applicant Identifier Number
- Date of Birth
- Gender
- Nationality
- Citizenship Status
- Mailing Address
- Personal E-mail Address
- Personal Phone Number
- Race and National Origin
- Educational Information
- Employment History
- Military Service Information and Status
- Disability Status

Persons who are applying for employment to the Department’s vacancy announcements are the sources of information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 CFR part 337
- 22 U.S.C. 2651a (Organization of the Department of State)
- Foreign Service Act of 1980, as amended (22 U.S.C. 3901 et seq.)
- Presidential Memorandum on Improving the Federal Recruitment and Hiring Process (May 11, 2010)
- Executive Order 12293, as amended
- Executive Order 9397, as amended (Numbering System for Federal Accounts Relating to Individual Persons)
- Executive Order 12968, Access to classified information
- Executive Order 13467, Reforming processes related to suitability for Government employment

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒ Yes, provide:
  - SORN Name and Number: Human Resources Record, State-31
  - SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): July 19, 2013

☐ No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

☐ Yes  ☒ No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

☒ Yes  ☐ No

(If uncertain about this question, please contact the Department’s Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):
- Schedule number (e.g., (XX-587-XX-XXX)): N/A
- Disposition Authority Number: DAA-GRS-2017-0011-0002 (GRS 2.1, item 051)
- Length of time the information is retained in the system:
  Job application packages are destroyed one year after date of submission. Job vacancy case files are destroyed two years after selection certificate is closed or final settlement of any associated litigation; whichever is later. When records have reached their retention period, they are immediately retired or destroyed in accordance with the NARA guidelines.
- Type of information retained in the system:
  Case files an agency creates when posting and filling competitive job vacancies. Also known as case examining, competitive examination, or merit case files. Includes:
  - request for lists of eligible candidates
  - job announcement
  - examination announcement
- job analysis, assessment criteria, and crediting plan
- basis for certification
- applications, resumes, supplemental forms, other attachments
- list of eligible candidates or applicants screened, ranking or ratings assigned, and basis for certification
- certificates, registers, or lists of eligible candidates issued to selecting officials
- job-related test records
- mandatory applicant drug test records
- annotated certificates of eligible candidates returned by selecting officials
- job offers
- records of job offer being accepted or declined
- correspondence/documentation of announcement or recruiting operation

PII records will be maintained until they become inactive at which time they will be retired or destroyed in accordance with published Department records schedules and as approved by NARA and governed by the OPM guidance in the Delegated Examining Operations Handbook, Appendix C, Records, Retention and Disposition Schedule

4. Characterization of the Information
   (a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒ Yes  ☐ No  ☐ N/A

- If yes, under what authorization?

- Executive Order 12293, as amended
- Executive Order 12968, Access to classified information
- Executive Order 13467, Reforming processes related to suitability for Government employment
(d) How is the PII collected?

Information is collected directly from an applicant when applying for a position on the USAJOBS website (http://www.usajobs.gov). The applicant must first create an account and populate the account with pertinent information to include resume(s) and contact information. When the applicant creates an online resume, they are required to submit some types of PII including name, mailing address, phone number, e-mail, citizenship status, and educational information. This PII is transferred from USAJOBS into GTS using the Hypertext Transfer Protocol Secure (HTTPS) encrypted web protocol.

When an applicant selects a job on the USAJOBS website and clicks the “Apply Online” link, the authenticated session of the applicant user is then passed through to GTS. At this point the applicant submits their date of birth and Social Security Number (SSN) to GTS in order to proceed in the application process. Applicants can also fax or upload support documents such as resumes, transcripts, performance evaluations, Student Aid Reports, SF-50 (Notice of Personnel Action) and DD-214 (Certificate of Release or Discharge from Active Duty) forms once within GTS.

(e) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select “Department-owned equipment,” please specify.
  GTS is owned and housed by Monster. GTS is FEDRAMP approved as of 4/7/2022.

(f) What process is used to determine if the PII is accurate?

It is the applicant’s responsibility to ensure the accuracy and completeness of their information. During the registration process with USAJOBS, each applicant enters his/her personal and demographic information. After registering the applicant can correct, update, and modify their information by logging into USAJOBS to make the necessary changes to their profile. Any changes made by an applicant of a Department-related job vacancy is then transferred to GTS while the vacancy announcement is still open and accepting applications.

If a Human Resources (HR) specialist identifies a problem with the application, the applicant may be notified of the error by an e-mail generated in GTS. At that point, the applicant can go back and make the necessary corrections to their profile in USAJOBS.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Information is current as of the time it was submitted by the applicant. Any changes made by an applicant of a Department-related job vacancy are then transferred to GTS while the vacancy announcement is still open and accepting applications.

(h) Does the system use information from commercial sources? Is the information publicly available?

No. GTS does not use information from commercial sources or publicly available information.

(i) How was the minimization of PII in the system considered?

Privacy concerns abound due to the sensitive PII data in GTS. However, all of the information is required to authenticate applicants and review qualifications in meeting the requirements of a given position.

5. Use of information

(a) What is/are the intended use(s) for the PII?

The information is used to screen applicant qualifications for employment with the Department and track if an applicant withdraws, is referred, interviewed, and/or chosen by the selecting official to fill a vacant position.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, GTS’s primary function is to improve and streamline hiring management processes/efforts by automating recruitment activities. The PII collected assist in completion of this effort.

(c) Does the system analyze the PII stored in it? ☐ Yes ☒ No

If yes:

1. What types of methods are used to analyze the PII?

2. Does the analysis result in new information?

3. Will the new information be placed in the individual’s record? ☐ Yes ☐ No

4. With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐ Yes ☐ No

(d) If the system will use test data, will it include real PII?

☐ Yes ☒ No ☐ N/A
If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal: The information is shared internally with the GTM owned Integrated Personnel Management System (IPMS) via Monster Government Solutions Data Processor (MDP), which is a child of IPMS.

External: No information will be shared outside of the Department of State.

(b) What information will be shared?

Internal:

- Applicant’s personal information (Full Name, Date of Birth, Social Security Number, Citizenship, Gender)
- Applicant’s contact information (Mailing Address, Personal Email Address, and Phone Number)
- Military service information (i.e. Veteran preference)
- Applicant’s resume
- Diversity data is also shared (race and disability)

External: N/A

(c) What is the purpose for sharing the information?

Internal:

- To support the Foreign Service medical clearance process
- To support the security clearance process
- To support hiring managers and HR specialists when posting and filling each respective position as part of the hiring process
- To provide applicable information in grievance and litigation cases
- To report on diversity, inclusion, equity, and accessibility trends

External: N/A

(d) The information to be shared is transmitted or disclosed by what methods?

Internal: Applicant data is transferred from GTS to Integrated Personnel Management System (IPMS) using a secure file transfer protocol (SFTP) using the Monster Government Solutions Data Processor (MDP), which is a child of IPMS. Based on the type of candidate data (FS Specialist, Civil Service, student, and various other
hiring programs), the MDP application is then able to route data to either the Recruitment, Examination, and Employment Tracking Application (REETA), Specialist Tracking and Reporting (STAR) or Global Employment Management System (GEMS) which are also systems under IPMS.

External: No PII will be shared outside of the Department of State.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal: All applicant’s data are packaged as XML file. The XML files are pulled via Secure File Transfer Protocol (SFTP) from the Monster site to IPMS by system administrators utilizing public and private security keys. The files that were transferred to IMPS are only accessible by the system administrator via MDP application. All data is encrypted in transit and at rest. Vulnerability scanning is performed on the files before they are transferred to prevent intrusion for the interface from GTS to IPMS via MDP.

Also, OpenNet is the principal data network supporting all Department Sensitive but Unclassified (SBU) IT services. OpenNet is also a dedicated agency network for the secure transmission of SBU information among Department component offices, domestically and overseas. Access to OpenNet system is restricted to Department employees only. Two factor authentication is implemented.

External: No PII will be shared outside of the Department of State.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

USAJOBS utilizes Login.gov’s Privacy Act Statement (PAS) which provides notification. This PAS provides the applicant with notice of what authorizes the Federal Government to collect this information, why the information is being collected, with whom the information will be shared, and whether the information is mandatory. USAJOBS is a branded version of GTS for the United States Government.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒ Yes ☐ No

If yes, how do record subjects grant consent?

USAJOBS utilizes Login.gov’s PAS. When logging into USAJOBS, the user has opportunity to review the PAS and accept/decline to provide the PII or to consent particular uses of the PII before accessing the system.

If no, why are record subjects not allowed to provide consent?
(c) What procedures allow record subjects to gain access to their information?

Individuals may login to USAJOBS to gain access to their information they provided to a given vacancy announcement. USAJOBS is a branded version of GTS for the United States Government. Accounts can be recovered using email address that was originally used to create the account.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒ Yes ☐ No

If yes, explain the procedures.

After registering on USAJOBS, the applicant can login to correct, update, and modify their information. Any changes made by an applicant of a Department-related job vacancy is then transferred to GTS while the vacancy announcement is still open and accepting applications.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

If a Human Resources (HR) Specialist identifies a problem with the application, the applicant may be notified of the error by an e-mail generated in GTS. At that point, the applicant can go back and make the necessary corrections to their profile in USAJOBS. Additionally, users may correct their information independently.

8. Security Controls

(a) How is all of the information in the system secured?

The information in GTS is secured through implementation of the minimum baseline of controls for a Moderate impact system for confidentiality, integrity, and availability. Security controls used in GTS meet the requirements found in the NIST (National Institute of Standards) Special Publication 800-53 Rev 4 (NIST SP 800-53 Rev 4) which provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. Access to the application from an end user or a user with elevated privileges is controlled by the application administrators. Application identifiers and authenticators are provisioned based on the NIST SP 800-53 Rev 4 and DoS requirements. GTS Server operating system, web servers, applications, and databases are configured according to the Diplomatic Security (DS) Security configuration standards such as data at rest encryption, data in transit encryption, multifactor authentication and least privilege.
(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

GTS user account privileges are based on roles (GTS – Administrator, Hiring Manager, HR Specialist, and GTS Support) with the concept of least-privilege and need-to-know. GTS is hosted, managed, and serviced by the off-the-shelf vendor (Monster). All technical components are currently located in a secure data center, where access is strictly limited to authorized personnel. Only certain personnel have access to information and systems housed at the vendor’s facilities. GTS operates behind a firewall, which only allows access from the Internet via HTTPS, is restricted by an Access List and is not open to the public. Administrator can see everything; a Hiring Manager can see only applicants certified for their open positions; and a HR specialist can see all applicants for positions in their Bureaus. RNO (diversity) data is in a separate table and is not directly tied to an applicant. Hiring Managers do not have access to RNO data. GTS Support has full administrative privileges.

(c) Describe the procedures established to limit system and data access to only those individuals who have an “official” need to access the information in their work capacity.

GTS user account privileges are based on roles (GTS – Administrator, Hiring Manager, HR Specialist, and GTS Support) with the concept of least-privilege and need-to-know. Audit logs are maintained to record system and user activity including invalid logon attempts and access to data. System managers, key security, and user personnel work cooperatively to implement access controls along with other systems. These are not specific roles to GTS and do not have access to any data in GTS.

(d) How is access to data in the system determined for each role identified above?

Access to data in the system is governed by one’s role. Based on one’s role, an individual will have access to data based on specific tables, rows and column fields in the database. Access for each of the roles - GTS – Administrator, Hiring Manager, HR Specialist, and GTS Support are governed by the data table, rows and columns permissions. Administrator can see everything; a Hiring Manager can see only applicants certified for their open positions; and a HR specialist can see all applicants for positions in their Bureaus. RNO (diversity) data is in a separate table and is not directly tied to an applicant. Hiring Managers do not have access to RNO data. GTS Support has full administrative privileges.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

Access to all systems is conducted over an Advanced Encryption Standard (AES) Transport Layer Security (TLS) v1.2 or Higher encrypted connection via the Internet and via an AES Virtual Private Network (VPN) tunnel from the MGS office for administration. Remote access is not permitted except for a limited number of contractor
personnel for administrator purposes. The GTM Information System Security Officer (ISSO) monitors audit logs monthly received from the contractor for unusual activity.

(f) **Are procedures, controls, or responsibilities regarding access to data in the system documented?**

☒ Yes ☐ No

(g) **Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.**

The State Department’s user policy and rules of behavior are the general terms under which federal employees and contractors use the system. The State Department requires all new employees and contractors to complete the Department’s Cyber Security Awareness training (PS800) and Protecting Personally Identifiable Information course (PA318) before or immediately after the employment start date and prior to being granted access to the system. To retain access, all State Department personnel must complete annual refresher Cyber Security Awareness Training. The Personally Identifiable Information course is required every two years. Access to data is limited to cleared U.S. Government employees. The vendor, Monster, also provides privacy training (Information Security Awareness Training) to its staff and safeguards against dissemination of PII.