Gateway to State

1. Contact Information

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

2. System Information

(a) Name of system: Gateway to State

(b) Bureau: HR

(c) System acronym: GTS

(d) iMatrix Asset ID Number: 843

(e) Reason for performing PIA: Click here to enter text.

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

Gateway to State was previously authorized as part of the HR IPMS Authorization to Operate (ATO) in accordance with federal law on July 22, 2009. GTS is presently going through reauthorization. The documentation package for reauthorization is presently under review by the Bureau of Information Resource Management (IRM) and Chief Information Officer (CIO), who serves as the authorization official for the Department of State (DoS).

(c) Describe the purpose of the system:

Gateway to State (GTS) is the DoS application 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. The application is used for

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' qualification based on such data. In addition, the system provides email correspondence functionality so that employment candidates once enrolled 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 or 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
- Nationality
- Mailing address
- Personal email address
- Phone number
- Race and National Origin
- Education
- Employment history
- Military service information and status
- Disability status

Persons who are applying for employment to DoS vacancy announcements are the sources of information. Such persons may include current DoS employees, employees from other federal agencies, or members of the public.

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

- 22 U.S.C. 2581 (General Authority of Secretary of State)
- 22 U.S.C. 2651a (Organization of the DoS)
- 22 U.S.C. 3901 et seq. (Foreign Service Act of 1980)
- 22 U.S.C. 3921 (Management of the Foreign Service)
- 22 U.S.C. 4041 (Administration of the Foreign Service Retirement and Disability System)
- 5 U.S.C. 301-302 (Management of the DoS)
- Executive Order 9397 (Numbering System for Federal Accounts Relating to Individual Persons)
- Executive Order 9830 (Amending the Civil Service Rules and Providing for Federal Personnel Administration)

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

☒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): Volume 78, Number 139, July 19th 2013

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

(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 Division 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:

- Schedule number (e.g., (XX-587-XX-XXX)): DAA-GRS-2017-0011-0002 (GRS 2.1, item 051)
- Length of time the information is retained in the system: Job application packages are destroy 1 year after date of submission. Job vacancy case files are destroy 2 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:
  PII records will be maintained until they become inactive at which time they will be retired or destroyed in accordance with published records schedules of DoS 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) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?

•26 CFR 301.6109, Taxpayer identification;
•Executive Order 9397, Federal employment; and
•20 CFR 10.100, Federal Workers' Compensation allow the Department to collect SSN for employment, payroll, tax identification and benefit purposes

(c) How is the information collected?

Information is collected directly from an applicant when applying for a position during an authenticated session initiated on the USAJOBS website (http://www.usajobs.gov). The applicant must first create an account and populate the account with pertinent information to include a resume(s) and contact information. When the applicant creates an online resume, they are required to submit various forms of personally identifiable information (PII). Through the applicant's USAJOBS account some types of PII including name, address, telephone, e-mail, citizenship status, and educational information are collected by applicant entry or resume documentation. This PII is transferred from USA JOBS 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 and DD-214 forms once within GTS.

(d) 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.

It is owned and housed by Monster

(e) What process is used to determine if the information is accurate?

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. USAJOBS provides authentication services and applicant profile management during the job application process. Any changes made by an applicant to a Department-related job vacancy are then transferred to GTS while the vacancy announcement is still open and accepting applications. It is the applicant's responsibility to ensure the accuracy and completeness of their information. If a DoS Human Resources (HR) Specialist identifies a problem with the application information, 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.

(f) 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 to a Department-related job vacancy are then transferred to GTS while the vacancy announcement is still open and accepting applications.

(g) Does the system use information from commercial sources? Is the information publicly available?
No. GTS does not use commercial, publicly available or information from other Federal agency databases.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes. Individuals are made aware of the uses of the information prior to collection. Applicants can view the Office of Personnel Management's Privacy Act Statement immediately before account creation and are required to agree to the terms and conditions during the account creation and registration process.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
Information requested in an employment application including a person's SSN is voluntary; however, the employment application may not be processed if a person fails to disclose any requested information. Individuals grant consent by creating a profile on USA JOBS, providing the information, and submitting their application for employment after notification of its use,

- If no, why are individuals not allowed to provide consent?
Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
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 information?
The information is used to screen applicant qualifications for employment with DoS and track if an applicant withdraws, is referred, interviewed, and/or chosen by the selecting official to fill a vacant position. Applicant data is transferred from GTS to 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).

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

Yes. GTS allows the DoS Human Resources Executive Office (HR/EX) to manage its workforce hiring processes.

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

If yes:

(1) What types of methods are used to analyze the information?

A hiring office creates a self-assessment questionnaire to be completed by applicants in order to screen for knowledge, skills, and accomplishments that are applicable to the job description. Responses to each question have a weighted score that is assigned by the hiring office. This scoring identifies the overall score that can be accumulated for the questionnaire. The hiring office establishes pre-positioned cut-off scores to identify desired qualifications. GTS automatically uses this information to score and rank responses to self-assessments included with completed job applications. GTS generates a list of candidates, ranked by their score; followed by candidates who fall below the minimum cut-off score then by candidates who withdrew from consideration. Based on the cut-off scores defined by the hiring office HR will refer "Best Qualified" candidates to the hiring/selecting official for further consideration. PII is stored only in connection to the analyzed non-PII information (these are skill questions).

(2) Does the analysis result in new information?

No new data is created on job applicants within GTS.

(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

6. Sharing of Information

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

GTS information, through established Memorandum of Understandings and Agreements (MOU/MOA) is shared internally with Integrated Personnel Management System (IPMS)

(b) What information will be shared?

- Applicant personal information (Last Name, First name, Middle Initial, Date of Birth, Social Security Number, US Citizen, Gender type)
- Applicant contact information (Street Address, City, State, Zip code, Country, Email address, Phone number)
- Employee and dependent medical information
- Veteran preference
- Applicant resume
- Documentation received

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

- 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

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

GTS is transmitted via the DoS intranet, OpenNet.

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

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

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Unauthorized access to GTS, data leakage, and information exposure were concerns identified by HR and Monster team. This is one of the reasons why SSN is not collected at the initial stage, it is only collected when an applicant has advanced to a point in the hiring process when it becomes necessary. These risks are mitigated through adherence to and implementation of security controls in the system design and operation. Procedural and technical security controls, including permission and access controls, are in place to protect data in transit and at rest. Use of data encryption, audit log review, data masking and separation of duties are some of the controls in place to mitigate the risk of data exposure. Access to data is granted to systems administrators, and hiring managers at a level commensurate with their need-to-know and database management responsibilities. The sharing of data is limited to carry out mission critical activities.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals have the ability to contact the Director, Office of Information Programs and Services (A/GIS/IPS) Department of State, 515 22nd street NW DC 20522-8100. For more information see System of Records Notice State-31, Human Resources Record, provides guidance for record access to individual's information in GTS and amendment procedures. In addition, individuals may log in to their USAJOBS account to view information they provided to a given vacancy announcement but cannot amend it once the announcement is closed.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals have the ability to contact the Director, Office of Information Programs and Services (A/GIS/IPS) Department of State, 515 22nd street NW DC 20522-8100.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

STATE-31, Human Resource Records, along with the other SORNs provides guidance for record amendment procedures. Individuals who wish to amend records pertaining to them may do so through Information Programs and Services (A/GIS/IPS).

8. Security Controls

(a) How is 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 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.

(b) Describe the procedures established to limit 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 (HR Administrator, Monster Government Solution Administrator, and System Operator) with the concept of least-privilege and need-to-know. GTS is hosted, managed and serviced by the off-the-shelf vendor. 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.

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

The vendor conducts continuous monitoring, including monthly vulnerability scanning by an outside third party on selected subnets accessible from the Internet. Systems owned by the contractor are checked periodically by its staff. Audit logs are maintained to record system and user activity including invalid logon attempts and access to data. The HR Information System Security Officer monitors audit logs monthly received from the contractor for unusual activity. System managers, key security, and user personnel work cooperatively to implement access controls.

(d) Explain the privacy training provided to authorized users of the system.

The Department's user policy and rules of behavior are the general terms under which federal employees and contractors use the system. The Department requires all new employees and contractors to complete the Department's Cyber Security Awareness training Protecting Personally Identifiable Information course (PA-459) before or immediately after the employment start date and prior to being granted access to the system. In addition, the OpenNet account request form signed by all employees and contractors. To retain access, all Department personnel must complete annual refresher Cyber Security Awareness Training. Access to data is limited to cleared U.S. Government employees.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

Access to all systems is conducted over an AES TLSv1.2 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.

(f) How were the security measures above influenced by the type of information collected?

The security measures above were influenced by the baseline requirements for a system with moderate impact rating for confidentiality, integrity, and availability. GTS followed the data categorization procedures for confidentiality, integrity, and availability based on Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-60

Rev 1, Guide for Mapping Types of Information and Information Systems to Security Categories. Additionally, the DoS IRM/IA Security Categorization Form (SCF) and eAuthentication Risk Assessment guides were used to determine the overall impact and eAuthentication levels of KC. NIST SP 800-53 Rev 4 security controls for a moderate system were included in the design and operation of GTS. In particular, the PII data influenced the application of the controls from the following families: access control, audit and accountability, identification and authentication, system and communications protection, and system and information integrity control families.

9. Data Access

(a) Who has access to data in the system?

GTS users fall in one of the three following privileged and general user definitions. General user accounts are provided only to government employees.

- **System administrators** are limited to authorized contractor company personnel. Administrative accesses to the servers are reviewed on a monthly basis to ensure access is restricted to authorized personnel.
- **Database administrators** are limited to authorized contractor company personnel. Access to key databases (DBA and direct access) is reviewed on a quarterly basis.
- **Application users** are limited to authorized contractor company personnel. Application users are provisioned and de-provisioned access through a formal and documented process. Application access is reviewed and validated on a bi-annual basis.

(b) How is access to data in the system determined?

Access to GTS is conducted over an AES TLSv1.2 or Higher encrypted connection via the Internet and via an AES Virtual Private Network (VPN) tunnel from the vendor's office for administration.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

No. User access is restricted to only those roles for which their position is authorized. Individual record information is available only to the user with appropriate privileges and their supervisor when applicable.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

All contract personnel must sign a company policy acceptance agreement, which covers data confidentiality, use of computing resources, and Internet use. The ultimate responsibility for

granting access, authorizations and permissions is determined by the DoS and is based on the need of the individual requesting the privileges after verification of proper credentials. Contractors that design, develop and maintain the system are required to adhere to Privacy Act clauses present in the contracts and in the Statements of Work. Only the individuals with need-to-know are allow access to the system, and privileges are assigned based on the roles of the individuals.