1. Contact Information

DoS Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: April 12, 2010

(b) Name of system: Gateway-to-State

(c) System acronym: GTS

(d) IT Asset Baseline (ITAB) number: 843

(e) System description: Gateway-to-State (GTS) is the Department of State (DoS) implementation of the Hiring Management Enterprise Suite (HMES), a commercial off the shelf hiring service that is used to automate the staff acquisition process. HMES was created by Monster Government Solutions (MGS) as a web-based job candidate assessment tool that is accessible via the internet from the USA Jobs website. The USA Jobs website is owned and operated by the Office of Personnel Management (OPM) and OPM is responsible for the privacy and security aspects of applicant information up to the point where the application data in USA Jobs is moved into the applicant record under GTS.

GTS serves as the automated mechanism for applicants to apply for all DoS Civil Service and Foreign Service Specialist jobs. Applicants access GTS via the USA Jobs website, and once registered are able to perform key activities that include but are not limited to posting up to five online resumes, searching for and applying to Federal government jobs, and receiving automated job alerts. GTS is part of the HMES that is hosted, managed, and serviced by MGS. HMES is classified as a Major Application. GTS enables DoS to use the Internet to build and post job vacancies and gather information needed to evaluate and hire qualified candidates.

DoS has a contract with MGS to manage and operate GTS. DoS does not own HMES but pays for the rights to use it. However, DoS does own all applicant data collected via the GTS system, including the file of vacancy announcements and the question library.

(f) Reason for performing PIA:

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

(g) Explanation of modification: Not applicable

(h) Date of previous PIA: April 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII.

☒ does contain PII.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The following elements of PII are collected and maintained:

- Full Name;
- Social Security number (SSN);
- Nationality;
- Mailing address;
- Personal email address;
- Phone number;
- Race and National Origin;
- Education;
- Employment history;
- Military status; and
- 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.

b. How is the information collected?

Information is collected when an applicant applies for a position using a web browser on the USA Jobs website (http://www.usajobs.gov/). Before an applicant begins the job search, 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) to include their SSN. Such information is securely transmitted by the applicant through the https://my.usajobs.gov/ site using the Hypertext Transfer Protocol Secure (HTTPS) encrypted web protocol. If the applicant decides to use a Job Search Agent(s) for automated searches, then such search information is securely entered.

When an applicant selects a job on the USA Jobs website that came from the HMES and clicks the 'Apply Online' link, their request goes to an agency specific version of the QuickHire Business Connector (QHBCWeb) which applies logic to their request and forwards the request to the proper agency specific version. QHBCWeb is an application that provides integration services between the HMES and the USA Jobs website. Thus GTS has an indirect interface with OPM's USA Jobs recruitment tool. QHBCWeb accesses the client's transactional database and adds applicant data as needed. Applicants can also fax information to include transcripts, Student Aid Reports and DD-214 forms via the fax imaging module.

The process culminates with MGS submitting applicant data on an encrypted CD-ROM for uploading into the DoS Recruitment, Examination, and Employment Tracking Application (REETA). REETA is maintained by The HR Bureau's Office of Recruitment (HR/REE). The key to decrypt the CD-ROM information is transmitted to DoS via a secure out-of-band method. Only authorized individuals designated by HR/REE may receive the media and key.

c. Why is the information collected and maintained?

Applicant personal information is collected, processed, and maintained to determine employee eligibility and, as part of the hiring process, to rank applicants' qualifications based on such data. In addition, the system provides mailing list functionality so that enrolled employment candidates can be notified of the respective hiring decisions and interested parties can be notified of future job vacancies.

Race and National Origin and Disability Information, which is disassociated from the applicant, are used to analyze the effectiveness of the DoS hiring process.

d. How will the information be checked for accuracy?

During the registration process, each applicant has the opportunity to verify his/her personal and demographic information. If after registering the applicant discovers they have entered incorrect information, they have the option of logging into GTS to make the necessary corrections to their profile. It is the applicant's responsibility to ensure the accuracy and completeness of their information. If a DoS 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 or make arrangements to mail in the necessary information.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 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. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The most sensitive unique identifier in GTS is the record subject's SSN. After the applicant's SSN is captured through the USA Jobs profile and copied into the GTS record, the SSN is not displayed in any interactive applicant interface. Marginal risk exists that routine authorized uses of GTS, or data inaccuracies in the GTS, might

render an adverse determination against the record subject, or deny the individual a right, benefit, or privilege of the government, or otherwise cause them harm.

Privacy risks are mitigated through adherence to information assurance policy and guidelines (e.g., National Institute of Standards & Technology 800 series). This system collects the absolute minimum amount of PII required to satisfy the statutory purposes of this system and the mission of the Bureau of Human Resources. Access, authorizations and permissions are only granted to systems administrators, helpdesk agents, HR specialists and hiring managers at a level commensurate with their need-to-know and database management responsibilities.

4. Uses of the Information

a. Describe all uses of the information.

Citizenship and military service information are used to determine federal employment eligibility requirements. An applicant's SSN is used to uniquely identify their records because other people may have the same name and birth date. Information collected from an application to include a person's SSN may be used in conducting an investigation to determine the applicant's suitability for employment, or the applicant's ability to hold a security clearance. The e-mail address and phone numbers provided by each applicant are used to contact each respective applicant for the purpose of follow on actions after an applicant's response to a vacancy is received either online or via fax.

b. What types of methods are used to analyze the data? What new information may be produced?

From the responses received to each respective vacancy announcement, GTS automatically generates a list of the most qualified candidates. Based on the overall score accumulated by the client and pre-positioned cut-off scores, DoS will make a hiring decision based on the "Best Qualified" candidate. The accumulated passing or failing score is derived data based on the way the candidate answered the questions and the weighted score given to that answer. A method used is to use qualification questions with associated multiple choice or written responses. A second method used by GTS, is an analysis methodology called the "weighted scoring method." Weighted scoring is used to produce a weighted score derived from using multiple choice questions. Each question is allocated a weight value that reflects its relative importance. The allocation of a score to each question subsequently reflects how it will perform in relation to other questions. The result is a single weighted score for each applicant, which is then used to indicate and compare the overall performance among multiple applicants. Based on the overall score accumulated by the client and pre-positioned cut-off scores, DoS will make a hiring decision based on the "Best Qualified" candidate. The accumulated passing or failing score is derived from answers provided by each candidate to questions, and the associated weighted score given to that answer.

GTS users have the ability to generate statistical reports by vacancy announcement and applicant demographics. GTS users may also pull individual or select groups of applicant profiles for use by the various offices and bureaus in DoS in hiring the best qualified personnel to fill vacancies. The ability to access these reports directly in GTS is based on user permissions that are defined and controlled by DoS internal system administrators. The system users are HR Specialists specifically authorized to access the applicant data. The data feed via encrypted CD- ROM will be integrated into the

internal Recruitment, Examination, Employment, and Tracking Application (REETA) data structure, the Knowledge Center (KC) universe and GEMS. At that time the applicant data is available for audit trails for operations and maintenance purposes, ad hoc reporting and finite and extensive statistical analysis by authorized HR Specialists. These types of reports may include, but are not limited to demographic data and diversity initiative data. The purpose of the extracts and analysis is to select the best qualified personnel, fill the best fit jobs and to test the effectiveness of the various hiring programs.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

GTS does not use commercial, publicly available or information from other Federal agency databases. In making applicant qualification decisions GTS functionality itself does not use information from credit agencies or background checking agencies. Further along in the hiring process, applicant information collected by GTS is used, by DoS analysts to verify clearance, to conduct credit and background checks on new applicants and on people who transfer from other agencies.

d. Are contractors involved in the use of PII?

The HMES software is owned and operated by the contractor, Monster Government Solutions. All contracts contain approved Federal Acquisition Regulation Privacy Act clauses. MGS ensures that all their personnel and authorized contractors working in the GTS environment comply with the security policies and procedures outlined in their security plan. However the applicant data collected via the system, the file of vacancy announcements and the question library are all owned by DoS.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Access, authorizations and permissions are granted only to systems administrators, helpdesk agents, HR specialists and hiring managers at a level commensurate with their need-to-know and database management responsibilities.

The HMES (GTS) system security plan delineates responsibilities and expected behavior of all individuals, by referencing the MGS Rules of Behavior 2.0 document. In addition, DoS has implemented a separate “Rules of Behavior for Protecting Personally Identifiable Information” policy, dated October 6, 2008. The privacy rules of behavior are applicable to all employees and contractors, and cover all DoS records, regardless of format that include PII.

5. Retention

a. How long is information retained?

As an HR application, GTS adheres to the guidance provided in System of Records Notice, STATE-31, titled *Human Resources Records*. PII is maintained until it becomes inactive, at which time it will be retired or destroyed in accordance with published DoS record disposition schedules and as approved by the National Archives and Records Administration.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Regular backups are performed and recovery procedures are in place for GTS. All records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. Per the System of Records Notice, STATE-31, titled *Human Resources Records*, when records have reached their retention period they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA).

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Information is available only to authorized users within DoS for the purpose of executing their official duties related to Human Resource services. When received by HR, the PII is manually uploaded into the Integrated Personnel Management System (IPMS). Memorandums of Understanding (MOUs) governing information sharing, what information is shared and information protection requirements are in place between HR and each bureau or office listed below:

- Office of Medical Services: IPMS shares employee and dependent medical information. The expected use of the information is to support the Foreign Service medical clearance process.
- Bureau of Diplomatic Security: IPMS shares employee and applicant information. The expected use of the information is to support the security clearance process.
- All Domestic and Regional DoS Bureaus: Bureaus share applicant information. As part of the hiring process the expected use of the information is to support DoS hiring managers and HR specialists when posting and filling each respective position.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Once applicant information is received by the HMES system from QHBCWeb, MGS hand delivers an encrypted CD-ROM containing applicant data to DoS for uploading into REETA. The personnel responsible for protecting the privacy rights of the public and employees are the system administrators, and HR specialists with the authorization and permissions based on their need-to-know and job function.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

There are no risks to privacy from internal sharing. The HMES system security plan delineates responsibilities and expected behavior of all individuals who access it. The use of the information is in accordance with the stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons with a need-to-know. The HMES system security plan delineates responsibilities and expected behavior of all individuals. In addition, DoS has implemented a “Rules of Behavior for Protecting

Personally Identifiable Information" applicable to all employees and contractors and covering all DoS records that include PII, regardless of format.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Information gathered by GTS is not shared with any external organizations.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information gathered by GTS is not shared with any external organizations.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The contract with MGS contains approved Federal Acquisition Regulation Privacy Act clauses. MGS ensures that all their personnel and authorized contractors working in the GTS environment comply with the security policies and procedures outlined in their security plan. Because information gathered by GTS is not shared with any external organizations the risk to privacy resulting from external sharing is non-existent.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

System of Records Notice STATE-31, *Human Resources Records.*

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

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. An approved government use Warning Banner is displayed each time prior to login. In addition, a copy of the Office of Personnel Management's *Privacy Act Statement* can also be found at *http://www.usajobs.gov/privacy.asp*. The purpose, use, and authority for collection of information submitted are described in the System of Records Notice, STATE-31.

b. Do individuals have the opportunity and/or right to decline to provide information?

Information requested in an employment application including a person's SSN is voluntary; however, the employment application will not be processed if a person fails to disclose any information including their SSN.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No, the system would not be able to process the large volume of applications. Allowing individuals the right to consent to limited, special, and/or specific uses of the information would result in the negation of the systems intended use. No other special uses of the information are permitted. Users are advised on the use of the information being collected.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purposes and uses. Additional notice of authority for collecting PII data is also in the System of Records Notice, STATE-31, titled *Human Resources Records* available in the Federal Register. The notice is specific to the system's purpose and sensitivity of the PII collected.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

An applicant can access the system once they enter their username or e-mail and password and make necessary corrections or make arrangements to mail in the necessary information. Once an applicant is logged in, then they may view, add, update, change and delete information in their personal profile only. If requested MGS and DoS help desk personnel may assist the applicant in completing their application. In addition, procedures for notification and redress are published in the System of Record Notice STATE-31, titled *Human Resources Records.*

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Individuals can update their accounts as needed or follow the notification and redress procedures stated in the System of Record Notice STATE-31, titled *Human Resources Records* published in the Federal Register. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

GTS is part of the HMES that is hosted, managed and serviced by Monster Government Solutions (MGS). MGS designates only certain personnel to have access to HMES information and systems housed in MGS facilities. All MGS staff 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.

MGS 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. In addition, to comply with the security policies and procedures outlined in the GTS security plan, MGS' personnel security guidelines adhere to the following:

- P.L. 107-347, Title III, Federal Information Security Management Act (FISMA) of 2002;
- Ethics in Government Act of 1978;
- OMB Circular A-130; and
- Privacy Act of 1974.

MGS 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 MGS staff. Only authorized DoS current employees and contractors are provided access to HMES at MGS facilities. A system use notification ("warning banner") is presented on the HMES log-on screen. The notification complies with the content criteria prescribed by NIST Special Publication 800-53 for a system having a security categorization of Moderate, as defined by the Federal Information Processing Standards Publication 199.

b. What privacy orientation or training for the system is provided to authorized users?

The appropriate use policy and Rules of Behavior are the general terms under which federal employees and contractors use the system. The DoS requires all new employees and contractors to attend Cyber Security Awareness training before or immediately after the employment start date and prior to being granted access to the system. In addition, the account request form signed by all employees and contractors to access the Department SBU network includes a requirement for the individual to successfully complete a security awareness distance learning course. To retain access, all DoS employees and contractors must complete refresher training annually. Access to data is limited to cleared U.S. Government employees and contractors administering the system who meet "official" need-to-know criteria. The GTS System Security Plan and the Department Rules of Behavior delineate the responsibilities and expected behavior of all individuals who access the system.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Safeguards for access are commensurate with the confidentiality level of PII in GTS and reduce related privacy risk to a negligible level. The Bureau of Human Resources places great emphasis on the security of the data under its purview by adhering to best security practices (i.e., National Institute of Standards and Technology guidance) and complying with DoS directives and federal laws. The NIST security controls required by FISMA include continuous monitoring of account access and least privilege, monitoring of event log activities related to object access and transactions, and appropriate internal user training to include "Rules of Behavior" and security awareness. These controls are certified and reassessed annually to maintain security standards.

11. Technologies

a. What technologies are used in the system that involves privacy risk?

Although the DoS does not own the HMES software and, pays for the rights to use the software, it does own the applicant data collected via the GTS system, the file of vacancy announcements and the question library. The HMES relies on web forms and relational database technology to gather applicant data for GTS.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

With the exception of free form Knowledge, Skill, and Ability (KSA) questions, all web form fields are designed with read-only predefined lists. The relational database within GTS is annually tested for secure configuration and vulnerability per FISMA required continuous monitoring activities.

12. Security

What is the security certification and accreditation (C&A) status of the system?

GTS was granted an Approval to Operate on 7/22/09. The Approval to Operate expires on 7/22/2012.