DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

Gateway-To- State (GTS)

(Updated April 2008)

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Email: pia@state.gov

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public?**

YES X NO___

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail addresses pia@state.gov

2) **Does a Privacy Act system of records already exist?**

YES X **NO**

If yes, please provide the following:
System Name: Human Resources Records **Number:** State-31

If no, a Privacy system of records description will need to be created for this data.

3) **What is the purpose of the system/application?**
Gateway To State (GTS) is the Department's implementation of the QuickHire commercial off the shelf (COTS) hiring service that will be used to automate the staff acquisition process. GTS enables the Department to use the Internet to build and post job vacancies and gather the information needed to evaluate and hire qualified candidates. GTS also serves as the Web presence and front end for the Recruitment, Examination, and Employment Tracking Application (REETA) in support of the Bureau of Human Resources (HR).

4) **What legal authority authorizes the purchase or development of this system/application?**

22 U.S.C. 2581 (General Authority of the Secretary of State)

B. DATA IN THE SYSTEM:

1) **What categories of individuals are covered in the system?**
GTS will collect information on individuals who are seeking employment with the Department of State (DoS). This includes individuals who are current employees of the federal government and the Department as well as individuals who are neither current employees of the Department nor are they employees of the federal government.

2) **What are the sources of the information in the system?**

a. **Who/what is the source of the information?**
The individuals who are applying to the Department's vacancy announcements will provide this information. In the case of non-DoS employees, this information will be transferred to GTS database from

outside DoS. In the case of current DoS employees, this information may or may not originate from within DoS.

b. **What type of information is collected from the source of the information?**
The individuals applying for jobs using GTS will provide personal information about themselves to include name, address and social security number among other pieces of personal information. In addition, the applicants will provide information about their employment history, including their resume and detailed information about current and previous employers and educational background, among other pieces of employment history, educational information, and RNO and disability information. Applicants will also fax in information such as transcripts, Student Aid Reports and Forms DD-214s via the fax imaging module.

3) Accuracy, Timeliness, and Reliability

a. **How will data collected from sources other than DoS records be verified for accuracy?**

The applicant will have the opportunity to verify his/her personal and demographic information in the application process. If, after the applicant leaves GTS and needs to make changes to his or her profile, they can log back into the system and make changes. It is the applicant's responsibility to ensure the accuracy and completeness of their own data.

b. **How will data be checked for completeness?**
The GTS database requires that certain fields be answered before the applicant can move on to another part of the application process. The DoS HR Specialist's identifies these fields as they build a vacancy in the system. If these mandatory fill fields have not been completed, the system will stop the applicant at certain points in the application process and force them to go back and complete the fields. GTS informs the applicant of the fields that have not been completed. 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.

c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

All data is as current as the applicant wants it to be. If any information needs to be changed by the applicant, it can be saved and revisited later. The applicant is responsible for insuring that their personal data is correct and up-to-date. Student intern programs and civil service vacancies have cut-off dates. Data outside the open vacancy interval are not accepted. An applicant can reuse their profile data and core question responses they previously entered. Other than that, there are no procedures to notify DoS personnel if an applicant's information is not current.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

The information the applicant provides through the GTS Web based application is used for the purpose of determining eligibility and qualifications of an individual for the position being advertised and for which they are applying. The data is used for the hiring process. The RNO and disability data, which is disassociated from the applicant, is used to analyze the effectiveness of the hiring programs. The following Privacy Act statement is accessible from the front page of the Web site and on every subsequent page:

Gateway to State Privacy Statement

Thank you for visiting the U.S. Department of State's website and reviewing our privacy statement. The Gateway to State is an Internet-based Human Resource vacancy announcement, application, and certification system for both internal and external recruitment. This system is authorized by 5 U.S.C. 3301. This system is used by the public to apply for positions in the Department of State (DOS) and by the DOS Bureau of Human Resources as a means of publishing vacancy announcements and soliciting and processing on-line applications. DOS will protect the collected information pursuant to the Privacy Act of 1974, as amended and the Freedom of Information Act, as applicable. For additional information on the Privacy Act of 1974 and the Freedom of Information Act go to http://foia.state.gov/refer.asp.

If a request is made, we may share non-personally-identifiable information with others in aggregated form (for instance, a count of the number of total registered users, or the average number of applications received for Gateway to State vacancy announcements). With respect to personally-identifiable information, the Office of Personnel Management is authorized to rate Civil Service applicants for Federal jobs under sections 1302, 3301, 3304, 3320, 3361 and 3394 of title 5 of the U.S. Code. Section 1104 of title 5 of the U.S. Code allows the Office of Personnel Management to authorize other Federal Agencies to rate applicants for Federal jobs. With respect to personally-identifiable information, the Department of State is authorized to rate Foreign Service applicants for Federal jobs under sections 3926 and 3941 of the U.S Code.

We are authorized to solicit your Social Security number by Executive Order 9397. We need the information collected to determine how well your knowledge, skills and abilities qualify you for a Federal job. We also need information on matters such as citizenship and military service to determine whether you are affected by laws that we must follow in deciding who may be employed by the Federal Government. We need your Social Security Number (SSN) to identify your records because other people may have the same name and birth date. If necessary, and usually in conjunction with another form or forms, the information collected in an application (including your Social Security number) may be used in conducting an investigation to determine your suitability for employment or your ability to hold a security clearance. The information may be disclosed to authorized officials making similar, subsequent determinations. Disclosure of the information requested in an application (including your Social Security number) is voluntary; however, your application will not be processed if you fail to disclose any such information (including your Social Security number). Information we have about you may also be given to Federal, State, and local agencies for checking on law violations or other lawful purposes. We may send your name and address to State and local Government agencies, Congressional and other public offices, and public international organizations, if they request names of people to consider for employment. We may also notify your school placement office if you are selected for a Federal job.

E-mail address information in your user profile and resume is being solicited to expedite the process of contacting you in conjunction with your application submitted via Gateway to State. E-mails may also be sent for the purpose of requesting information from the Gateway to State Help Desk. If your e-mail message includes personally identifiable information, as for example an e-mail containing an inquiry or request for information, we will use that information to respond to your inquiry. Also, incomplete and/or incorrect addresses and/or email addresses may result in our inability to contact you should you be selected for an interview and/or as the selected candidate for a position for which you have applied.

Public Burden Statement
Public reporting burden for this collection of information is estimated to average 30 minutes per response, including time for reviewing instructions, searching existing data sources, gathering data, and completing and reviewing the information. The OMB number, 1405-0139, is currently valid. The U.S. Department of State Bureau of Human Resources may not collect this information, and you are not required to respond, unless this number is displayed. Send comments regarding this burden statement or any other aspect of the collection of information, including suggestions for reducing the burden to: A/ISS/DIR, U.S. Department of State, Washington, DC 20520.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

GTS consists of a collection weighted and qualification questions with associated multiple choice or completion type answers. 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.

The applicants have access to their own data for update via an ID and password. The applicant may view, add, update, change and delete information in their personal profile only. The QH and DoS help desk personnel if requested may assist the applicant in completing their application. The system administrators grant the help desk personnel the privileges to access, maintain databases or make changes to applicant data. The applicant data will be stored outside DoS. GTS database servers located in the vendor's controlled access data center will provide storage for the applicant's data, HR's vacancy announcements and questionnaires.

3) **Will the system make determinations about DoS employees or members of the public that would not be possible without the new data?**
Yes, GTS is able to provide an automated list of the most qualified candidates in a very short amount of time. This is a function that until now was done manually and performed by the HR Specialist through many steps of preparation and data entry over a long period of time. GTS facilitates the selection of "Best Qualified" candidate in an automated, timely manor, thus reducing the long interval experienced with the manual system. It is less prone to keying errors by an HR specialist as the responsibility for data entry and subsequent data quality is transferred to the applicant.

4) **Will the new data be placed in the individual's record?**
The data entered by the applicant into GTS eventually becomes the individual's record. While the candidate is in the hiring cycle and being considered for employment, the candidate can correct errors in his or her data and enter missing data. The HR specialist will have the ability to generate e-mail notification to the applicant automatically via the email function in GTS. The candidate will be able to use the fax-imaging function of GTS to fax resumes, transcripts, Forms DD-214s, et.al. The fax image becomes part of the individuals GTS record.

5) **How will the new data be verified for relevance and accuracy?**
The Department's HR Bureau checks the data keyed in by the applicant and faxed in through the fax-imaging module. If there are problems with an application, HR can contact the applicant via the system messaging function to request that they correct their record. The applicant is able to update their profile data in their file directly on-line and the changes are communicated instantaneously to the HR specialist. The automated memos and on-line functionality have virtually eliminated delays in data collection and correction. Relevance and accuracy are quickly addressed.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**
Access to the applicant data is protected and controlled by a user ID and password function. There are various levels of authorization in order to access the data and the application functionality depending on the job function of the authorized user and applicant themselves. The list is controlled and administered by designated system administrators and Help Desk Personnel representing both the Department and the vendor. All data is primarily retrieved via the vacancy to which the applicant applied. Each applicant's record can be retrieved by the applicant's name or social security number or by a numerical key internal to the system (e.g. vacancy number of the position to which they applied) . GTS administrators will extract data from GTS's database and transmit it to the Department via CD-ROM or electronic data pull for integration into the REETA database, KC universe and GEMS.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
GTS users may run 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 the Department in hiring the best qualified personnel to fill vacancies. The ability to access these reports directly in GTS is based on user permissions defined and controlled by DoS's internal system administrators. The system users are HR specialists specifically authorized to access the applicant data. The data feed, initially via CD-ROM and eventually an electronic data pull, will be integrated into the internal REETA data structure, the KC universe and GEMS. At that time, the applicant data is available for audit trails for O&M 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, among others. 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.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**
GTS is designated as the front end to the internal REETA data structure. Once the data is imported and integrated to the REETA database, the KC universe and GEMS the vacancy data on GTS is considered historical and achieved. The exception is the profile data remains active allowing the applicant to continue to apply to other vacancy announcements and to update

data in their profiles as changes occur. Subsequent changes to the applicant's profile only, will be transferred down to the REETA database with the next data feed and subsequently update the applicant's profile. When an applicant is selected for consideration for employment or hired, maintenance of the record passes to the internal DoS systems and databases. With regard to the external systems hardware and software, GTS's servers are located in secure facilities outside the Department. GTS's employees maintain these servers. Maintenance of certain components (i.e. software/hardware maintenance and performance management) of GTS is managed by GTS's Development and IT staff.

2) What are the retention periods of data in this system?

Record data retention is governed by the guidelines provided in 5 FAM 400 and 5 FAH-4 for inactive and obsolete Student/Intern, Summer Clerical, and Civil Service applicant records. GTS will retain data at the direction of DoS in accordance with those guidelines. Otherwise, applicants'data are retained indefinitely. DoS will create a specific purge schedule, which will be executed annually at the discretion of DoS. The function of purging or deleting data resides with the HR specialist responsible for personnel records retention and is based on user permissions managed by DoS's systems administrator. When an applicant is selected for employment by the Department of State, the individual's personnel file is electronically transferred to our internal database, becomes inactive on GTS and is subject to records disposition rules.

The following excerpt from the 5 FAH-4 H-312 Responsibility For Records Disposition is provided here for reference purposes:

a. The records disposition function for the Department is directed by the Office of Information Services, Records Management Branch (OIS/RA/RD) in the Bureau of Administration. OIS/RA/RD's responsibilities include establishing Department-wide policies and procedures in compliance with Federal laws and governmental regulations, and providing support, training, technical guidance, and records storage services as needed.

b. Each office or post is responsible for carrying out an active records disposition program in accordance with policy and procedures set forth in this handbook and 5 FAM 400. This includes assigning a responsible person to manage the disposition of records by applying the appropriate records disposition schedules for their organization or section.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
The standard procedures for disposition of data are at the discretion of DoS. Please refer to the excerpt of the 5 FAH and 5FAM in question #4 above. Data retention and reports generated from that data are governed by those documents.

4) **Is the system using technologies in ways that the DoS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
GTS is a technology in its own right that has not been previously employed by DoS. It is unique in that GTS is managed outside and is hosted by an outside vendor for collecting, screening, generating reports, editing candidate data, auto-generation of correspondence to candidates, and providing status to the candidate on the progress of their application. DoS has never used the fax-imaging module before, which is a part of GTS. This functionality allows the applicant to fax documents such as resumes, transcripts and Forms DD214s directly to GTS and made immediately available online for review by HR specialists and hiring managers. The documents are stored in electronic format thereby eliminating the need for paper. Also, the bio-access technology employed at the vendor's server sites for security is a technology that is just beginning to emerge in DoS.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**
GTS and its technology facilitate public/employee privacy in both the electronic and physical security sense. The user ID and password access to GTS and the various levels of authorization and permissions granted the applicant and HR specialist user group provide several layers of electronic access restrictions. The guarded controlled access and bio-access technology employed at GTS's server sites severely restricts physical access to the system by providing several layers of physical security for DoS's information while it resides within GTS. DoS's system administrator manages access, authorizations and permissions. All RNO information is encrypted.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**
This is an automated hiring system that collects personal information voluntarily provided by the applicant. It is not classified but is sensitive information such as name, address, SSN, DOB, sex, race and national origin, work history, education, disability information, among other sets of sensitive

data. This information is available for review and analysis by the hiring managers and HR specialists. The level of access, authorization and permissions granted by the systems administrator governs the level of monitoring by the user group. GTS utilizes the functionality described in paragraph 5 above as controls to prevent unauthorized monitoring. The data transfer from GTS on the outside to the REETA application inside DoS is initially an air gap via CD-ROM hand delivered. The future data transfer will be via secure FTP.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Yes, GTS will be revised when system modifications affect employee information protected by the Privacy Act of 1974.

8) **Are there forms associated with the system? YES _X_ NO ___**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

In GTS, the design of the vacancy announcement is a narrative and the associated sets of questions are displayed as pages in a questionnaire. The only data that is collected from the public is the data required to evaluate an applicant for the position being advertised and for statistical analysis to determine the effectiveness of the hiring program and ensure compliance with The Equal Opportunity Employment Act. The data elements are stored in a relational database structure and records are then added, queried, extracted for maintenance, printed and displayed as needed. The GTS Privacy Act statement may be accessed at the user's discretion from every page in the application. Please refer to Section D.1 "Intended Use of Data" above for a verbatim extract of the Privacy Act statement as it appears in the Web pages.

F. ACCESS TO DATA:

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**

GTS's designated employees including support personnel and the development and IT teams will have access to GTS applications and databases. Their access is necessary to provide ongoing software and hardware O&M, new development and vendor help desk services. The applicant will have very limited access to their own profile data for updating, adding missing information and reviewing their file as required or desired. With regard to DoS, access, authorizations and permissions are granted to systems administrators, helpdesk agents, HR specialists and hiring managers at a level commensurate with their "need to know" and database management responsibilities. The vendor representative grants initial access to GTS and to DoS personnel designated as the system administrators. Subsequently, the administrators will limit access by reissuing credentials. DoS and vendor systems administrators will retain full access.

2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**
The vendor provides comprehensive guidelines and training to the Department on the functions and criteria for granting access, authorizations and permissions to GTS. The ultimate responsibility for granting access, authorizations and permissions is determined by the Department of State and is based on the need of the individual requesting the privileges upon presenting proper credentials. GTS's personnel with operational responsibilities and who have essential work within the system are granted access to DoS's data and the system hardware and software supporting that data.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**
Applicants will only have access to their personal information via user ID and password access. The Department user group will be granted the level of access, authorization and permissions commensurate with their need in order to perform their assigned tasks. Please refer to question #2 above for further description of the accessibility process.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials).**
Within the user group by virtue of the position they hold and their assigned duties, they are informed that accessing the system for purposes outside the scope of authorization constitutes a violation of Federal Law (18 U.S. C. & 130, et al, the Privacy Act). Auditing records and date/time stamps will control and/or identify unauthorized use.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been

established and training regarding the handling of such information under the Privacy Act of 1974, as amended?
Yes, GTS contractors design, develop and maintain the system. Privacy Act clauses are present in the contracts and in the Statements of Work (SOW). The vendor has established their personnel security guidelines through interpretation and adherence to the tenor of 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*
- *Privacy Act of 1974*
- *Computer Security Act of 1987*

The vendor 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.

Under the governance of P.L. 107-347 Title III, Federal Information Security Management Act (FISMA) of 2002, and the Computer Security Act of 1987, security and awareness training occurs at the vendor's facilities and is directly related to GTS application users. The purpose of this training is to enhance employees' and contractor personnel's knowledge of general vulnerabilities, risks, and threats specifically related to the use of the GTS application. The training describes methods to avoid vulnerabilities, risks, and threats. In addition, training provides an understanding of what to do if a user or operator suspects and/or knows of any data and/or system compromises. The training includes topics such as privacy protection, handling sensitive documents and information, incident reporting, proper password construction, and screensaver use. The vendor's training program is governed by the policies and procedures of the personnel security guidelines listed above for initial implementation as well as ongoing awareness and training.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
Yes, GTS will provide a data transfer initially by CD-ROM hand-delivered to DoS. The imported data will be integrated within the REETA data structure and in some cases transferred to GEMS upon hiring as well as shared with the Knowledge Center as a universe for ad hoc reporting. In the near future the CD-ROM data transfer is to be replaced by an electronic data feed via SSL tunneled VPN using Triple DES encryption. In both interface scenarios 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.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**
No. Although GTS is used across several agencies, the data and database belongs exclusively to the Department of State. The applicants of the Department's user group consisting of HR specialists and hiring managers are the only users that have access to it. The exceptions are the vendor developers, designers, system administrators and helpdesk personnel in direct support of the Department and the applicants.

8) **Who is responsible for assuring proper use of the SHARED data?**
Data is not shared among other departments or agencies. The Department's system administrators are tasked with the responsibility to ensure the data is used properly.