DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

Foreign Service Officer Test (FSOT)

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

The Department of the State
FY 2008 Privacy Impact Assessment for IT Projects

Introduction

Section 208 of the E-Government Act requires that agencies now conduct a Privacy Impact Assessment (PIA) for all new and significantly modified Information Technology (IT) projects. This includes projects that are requesting funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally and those undergoing DOS IT Security Certification and Accreditation (C&A) process. The Privacy Impact Assessment (PIA) is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA will help DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified systems that contain personally information about members of the public. OMB, which has oversight of all federal agency implementation of the Privacy Act of 1974, as amended, will be particularly scrutinizing IT project budget requests on the Exhibit 300 based on the PIA in addition to the other requirements that are already in place. The score obtained on the PIA among other criteria will determine the funding of the IT project. IT projects scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests as well as systems undergoing the C&A process. Consequently, it is imperative that the attached PIA be fully **completed, certified and submitted** as indicated below.

The Office of Information Programs and Services (IPS) is responsible for conducting the PIA as part of its Department-wide implementation of the Privacy Act. The PIA will be reviewed and scored by IPS and will be provided with the Exhibit 300 to OMB. This score will reflect how well your system protects personal information and will be integrated with the score for security. This combined score will then be incorporated in your Exhibit 300 submission to OMB. The document will also be provided to the Office of Information Assurance for purposes of C&A. For non-majors, IPS will retain PIAs on file for future needs. A guide and a handbook are being provided along with the PIA questionnaire. Please refer to the PIA handbook while completing the questionnaire. For more detailed information you may refer to the guide. In addition, this Office will assist you in completing the PIA questionnaire should you have any questions not covered in the guide.

Department of State
FY 2008 Privacy Impact Assessment

Once completed copies of the PIA may be provided to the following:

- Bureau/office IT Security Manager (when a C&A is required);
- Office of Information Programs and Services (A/ISS/IPS) Privacy Act Program Staff must be provided a copy of the PIA in all cases;
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also please complete the certification page at the end of this document. Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

A. CONTACT INFORMATION

Who is the Agency Privacy Coordinator who is conducting this assessment? (Name, organization, and contact information).

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

(1) Does this system collect, maintain or disseminate personally identifiable information (PII) 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 the above answer is YES, please complete the survey in its entirety. If NO, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.

1) **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.

2) **What is the purpose of the system/application?**

The purpose of the Foreign Service Officer Test systems (FSOT) is to provide an electronic registration and test mechanism for American citizens interested in a Foreign Service career. It will also be used as a data source for the Qualifications Evaluation Panel (QEP) module/process.

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

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

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?
FSOT will collect information on individuals who are seeking Foreign Service Officer positions with the Department of State (DoS). The individuals can be U.S. citizens from the general public or current federal government employees.

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 for Department of State (DOS) Foreign Service Officer positions will be providing this information. In the case of non-DOS employees, this information will be transferred to the Qualifications Evaluation Panel (QEP) database from outside the Department. In the case of current Department employees, this information may or may not originate from within the Department.

b. What type of information is collected from the source of the information?

The individuals applying for Foreign Service Officer positions will provide personal information about themselves such as name, address, social security number, educational background, employment history to include current and previous employers, RNO and disability information, if any, etc.

3) Accuracy, Timeliness, and Reliability

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

It is the candidate's responsibility to ensure the accuracy and completeness of their own data. The applicant will have the opportunity to verify his/her personal and demographic information in the application process. If the applicant, after he or she successfully completes the initial testing and prior to the qualifications examination panel, needs to make changes to their profile, they can contact the outside testing vendor, ACT, and make the changes. After the panel, the successful candidate will be issued a conditional offer with a Department of State point of contact who he or she will be instructed to contact with changes.

b. How will data be checked for completeness?

The FSOT database requires that certain fields be answered before the applicant can move on to another part of the application. The testing vendor, ACT, identifies these fields. If these mandatory fill fields have not been completed, the system will stop the applicant at certain points in the application process and require them to go back and complete those fields. ACT informs the applicant of what those fields are

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 candidate wants it to be. If any information needs to be changed by the candidate who passed the initial screening, the initial data is saved and revisited later. The applicant is responsible for insuring that their personal data is correct and up-to-date. The Foreign Service Officer Test (FSOT) takes place several times a year, at which time the initial personal information is provided by the candidate. The candidate passing the initial screening will be instructed that they are responsible for keeping their information current and they are given a DoS POC to contact for changes.

D. <u>INTENDED USE OF THE DATA:</u>

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 FSOT is used for the purpose of determining eligibility and qualifications of an individual for the Foreign Service as a Foreign Service officer. The data is used for the hiring process. The RNO and disability data is used for program analysis and OPM reporting.

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?**
Based on the overall score the candidate is given and a pre-determined cut-off score determined by the Department, the Department 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 rating given to that candidate by the Department's review panel.

The candidates are responsible for keeping their data up-to-date. The candidate may add, update, change and delete information in their personal profile through ACT to the point where a conditional offer letter is issued then through their POC from that point. The candidate data will be stored outside the Department. FSOT database servers located in the vendor's controlled access data center will provide storage for the candidate's data. Records retention is in accordance with the criteria set forth by the Bureau of Administration, Office of Information Services, Records Management Branch and 5 FAH-4 H-312, *Responsibility for Records Disposition.*

3) **Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**
No, ACT will provide an automated testing functionality but selection of the "Best Qualified" candidates will be based upon derived cutoff scores and the review panel results. FSOT facilitates the selection of "Best Qualified" candidate for panel review in an automated, timely way. By shifting the responsibility for data entry and subsequent data quality to the candidate themselves instead of an HR specialist, FSOT is less prone to keying errors.

4) **Will the new data be placed in the individual's record?**
For the best qualified candidates, the data in FSOT eventually becomes their personnel record. While the candidate is in the hiring cycle and being considered for employment, the candidate can update their personal information, correct errors, and enter missing data.

5) **How will the new data be verified for relevance and accuracy?**
Review Panel personnel and the HR Specialists will check the data that is keyed in by the candidate. If there are problems, such as incomplete, inconsistent or questionable data, the Department's HR Specialist will contact the candidate via e-mail requesting they correct their record. The applicant will be able to update

their profile data in their file through ACT initially and via their Department POC through the hiring cycle. 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 candidate's data is protected and controlled by ACT. There are various levels of authorization one must go through to get to the data and the application functionality, depending on the job function and roles of the authorized user. This is controlled and administered by designated System Administrators and Help Desk Personnel representing both the Department and ACT. Each applicant's record can be retrieved by a unique ACT ID assigned by ACT at registration time (i.e., candidate's name or social security number or by a numerical key internal to Department systems such as the unique system generated person ID). ACT FSOT administrators will extract data from FSOT's database and transmit it to the Department via an encrypted CD-ROM or encrypted electronic data pull for integration into the QEP database and other internal data structures.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
The ability to access system reports directly in FSOT is based on user permissions that are defined and controlled by the Department's internal system administrators. There are no reports produced from ACT regarding individuals personnel data. ACT collects the data, evaluates the candidate essays, scores them, enters scores in the candidates' records, and collects scheduling information from those candidates selected for the oral exam. This is done electronically. The information is then passed to the Department through a data feed, initially via encrypted CD-ROM and eventually an encrypted electronic data pull. The data will be integrated into Department data structures for internal use. All reports are internal to the Department once the CD or electronic data is integrated. At that time, the applicant's data is available for audit trails for OPM and 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, fit the personnel with the jobs, and to test the effectiveness of the Foreign Service hiring program.

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?**
ACT is the front end to the internal data structure. Once all the data for a cycle is imported and integrated to the Department's internal database, the candidate's data on Act's database for that cycle is considered historical and archieved. Once an applicant is selected and scheduled for the Foreign

Service Oral Assessment (FSOA), selected for consideration for employment or hired, the record maintenance passes to the internal Department systems and databases. With regard to the external systems hardware and software, ACT's servers are located in secure facilities outside the Department. ACT's employees maintain these servers. Maintenance of certain components (i.e. software/hardware maintenance and performance management) of ACT is managed by ACT's Development and IT staff.

2) **What are the retention periods of data in this system?**
The Department of State will advise ACT regarding data retention policy as stated in 5 FAM 400 and 5 FAH-4 and when to delete the files. ACT will retain data at the direction of the Department in accordance with Records Disposition Schedules.

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 system procedures for disposition of data are at the discretion of the Department. 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)?**
ACT registration, testing and scheduling services have been used by the Department in the past but the FSOT is a new format that replaces the FSWE and adds new functionality. ACT is unique in that it is managed outside the Department and is hosted by an outside vendor for collecting, storing, screening, editing candidate data, and auto-generation of correspondence to

candidates. The documents are stored in electronic format thus eliminating the need for paper

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**
The technology employed in the FSOT system does not change the obligation to protect the private data collected from individuals. The use of web and internet technologies exposes the private data to new threats and vulnerabilities. Mandated risk assessment processes are used to insure that adequate security measures are taken to protect the data both at rest and in transit per *OMB Circular A-130 Appendix III*. Access to FSOT systems is restricted to authenticated, authorized individuals with specific roles and permissions.

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?**
FSOT is a web based Foreign Service candidate testing application, owned by the Department of State and operated and administered by ACT. All servers and the supporting technology are owned by ACT. FSOT collects personal information which is voluntarily provided by the candidate over a secure connection. 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. The information transmitted via secured FTP or CD will be reviewed and analyzed by the BEX Review Panel Members, BEX HR Specialists and BEX System Administrators. The level of access, authorization and permissions granted by the systems administrator governs the level of monitoring by the user group. ACT utilizes the functionality described in paragraph 5 above as controls to prevent unauthorized monitoring. The data transfer from ACT on the outside to the QEP application inside the Department is initially an air gap via encrypted CD-ROM. 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. The FSOT, administered outside the Department by ACT, will be revised when system modifications affect employee information protected by the Privacy Act of 1974. The Department will oversee compliance.

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 ACT, the design of the online views consists of a set of instructions, a questionnaire to collect personal information, and a set of test questions. The only data that is collected from the public is the data required to evaluate the candidate for the current FSOT cycle. The data elements are stored in a relational database structure and records are then added, updated and displayed as needed for maintenance purposes. Data is transferred from ACT to the Department and integrated into the QEP system. At that time, the information is made available for reports. All reports are generated internal to the Department. The ACT and/or the Department's Privacy Act statements may be accessed at the users' 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)
ACT's designated employees including support personnel, the development and IT teams will have access to FSOT applications and databases housed in ACT facilities. Their access is necessary to provide ongoing software and hardware O&M, new development and vendor help desk services. The candidate will have very limited access through the ACT help desk function to their own profile data for updating their personal information. The candidate will be able to assess the FSOT scheduling application once notified by ACT that their FSOT cycle is open for online scheduling. With regard to the Department, access, authorizations and permissions will be granted to BEX reviewers, BEX systems administrators, and BEX HR specialists at a level commensurate with their "need to know" and database management responsibilities.

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

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, ACT contractors design, develop and maintain the system. Privacy Act clauses are present in their contracts and in their Statements of Work (SOW). The vendor has established its 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 FSOT 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 FSOT 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 FSOT application. The training describes methods to avoid those 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, ACT will provide a data transfer initially by encrypted CD-ROM delivered to the Department of State. The imported data will be integrated within the QEP data structure and eventually transferred to other internal data structures for selection, analysis and reporting. In the near future, the encrypted CD-ROM data transfer is to be replaced by an electronic data feed via SSL tunneled VPN using 3DES encryption. In both interface scenarios, the personnel responsible for protecting the privacy rights of the public and employees are the system administrators and Human Resource 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 ACT provides similar services to other federal agencies and commercial customers, the FSOT data and database belongs exclusively to the Department of State.. Their candidates and the Department's user group consisting of BEX Panel members, BEX HR specialists and system administrators are the only users who have access to it. The exceptions are the vendor administrators and developers, designers, system administrators and helpdesk personnel in direct support of the Department and the Department's candidates.

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.

ADDITIONAL COMMENTS: *(optional)*