1. Contact Information

Department of State 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: May 12, 2010

b) Name of system: Foreign Service Officer Test

c) System acronym: FSOT

d) IT Asset Baseline (ITAB) number: 1074

e) System description:

Foreign Service Officer Test (FSOT) is a Department of State (DoS) information system to support the proctored, computer-based Foreign Service Exam. FSOT supports electronic registration and application for American citizens interested in a Foreign Service career by providing the following services to prospective candidates: online exam registration, online exam scheduling, and computer-based completion of the written portion of the exam.

FSOT is administered in Iowa City, Iowa, by ACT, Inc., a contractor to DoS. The questions for the exam are generated using ACT proprietary software called Validus. ACT proctors the exam in the U.S. and at U.S. military bases approved by DoS. ACT also conducts the scheduling for the Foreign Service Officer Oral Assessments.

ACT also performs all backend services, including editing, analysis, scoring, and reporting of the written exam results to DoS. The exam includes multiple choice and essay questions. Applicants that achieve a passing score on the exam are then considered to be candidates for the next step in the Foreign Service Officer selection process.

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)
- Date of birth
- Nationality
- Mailing address
- Personal email address
- Phone number
- Race
- National Origin (RNO)
- Salary
- Education
- Military status
- Disability status.

The person applying for a DoS Foreign Service Officer position is the only source of PII. Such persons may include current DoS employees, employees from other federal agencies, or members of the public.

b. How is the information collected?

PII is obtained directly from the individual through online application forms completed by the applicant. Following an applicant's completion of the exam, the FSOT test system scores each test. Applicants that achieve a certain passing score on the multiple choice and essay portions of the exam will have their information submitted via encrypted CD-ROM to the DoS Qualifications Evaluation Panel (QEP) for evaluation. The key to decrypt the information is conveyed by ACT to DoS using a secure out-of-band method.

c. Why is the information collected and maintained?

Information is collected to determine an applicant's eligibility to take the exam, register each applicant for the exam, assess an applicant's qualifications for selection as a Foreign Service Officer, and to ensure the integrity of the exam process. All elements of PII including the SSN are collected to prove that an applicant is eligible to work for or with the U.S. government. Contact information is used for tracking and communication. The SSN is

used as the candidate identification number. Executive Order 9397 authorizes solicitation of the SSN for use as an identifier in personnel records management, thus ensuring proper identification of candidates throughout the selection and employment process. For record retrieval, the candidate's SSN is not used. Instead, ACT generates a 12-digit field as a primary key to uniquely identify each candidate.

d. How will the information be checked for accuracy?

The applicant is responsible for the accuracy of the information. The applicant will have the opportunity to verify and make changes to his/her personal and demographic information during the application process. Once an applicant has submitted their registration package, an applicant may not amend any part of it except to update changed contact information (i.e., phone numbers, mailing address, and email address). If an applicant achieves a passing score on the multiple choice and essay examinations, then the candidate will receive an email asking them to submit a Personal Narrative (PN) in which the candidate is to answer questions describing the knowledge, skills, and abilities they would bring to the Foreign Service. The firm deadline for submission is three weeks after the request is sent to the candidate. The PN is read carefully by each member of a Qualifications Evaluation Panel (QEP) made of up experienced Foreign Service Officers. A candidate's responses are subject to verification by a Board of Examiners before a decision is made affecting an individual.

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 Department of State)
- 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 Department of State)
- 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 FSOT is the record subject's SSN. After its first entry into FSOT, the SSN is not displayed in any interactive applicant interface. Marginal risk exists that routine authorized uses of FSOT, or data inaccuracies in FSOT, 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 DoS policy and guidelines. FSOT collects the absolute minimum amount of PII required to satisfy the statutory purposes of the system and the mission of the Bureau of Human Resources (HR). Access authorizations 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.

The principle uses of FSOT are to determine an applicant's eligibility to take the Foreign Service Officer Exam, register an applicant for the Exam, assess candidate qualifications for selection as a Foreign Service Officer, and to ensure the integrity of the process. Note the distinction between an "applicant" which is a person who applies for the examination, and a "candidate" which is a person who is selected by virtue of achieving a passing score required to continue in the Foreign Service Officer selection process.

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, including their SSN, may be used to conduct an investigation to determine the applicant's suitability for employment or ability to hold a security clearance. The email address and phone numbers provided by each applicant are used to contact each respective applicant for the purpose of follow- on actions such as exam scheduling and the reporting of exam results. Race and national origin, and disability information is effectively de-identified and is only used to analyze the effectiveness of the DoS hiring process.

The information collected may be used to prepare statistical reports and analyses at DoS. Such reports and analyses are prepared in such a way that they do not reveal identities, and may be shared outside DoS. The information collected during FSOT registration also may be made available to other federal agencies in response to a request for information about hiring or retention of an employee, to members of Congress in response to an inquiry on behalf of the applicant, or for authorized law enforcement or administrative purposes. The SSN is used as the candidate identification number. Executive Order 9397 authorizes solicitation of the candidate's SSN for use as an identifier in personnel records management, thus ensuring proper identification of candidates throughout the selection and employment process.

Following the ACT-administered exam, those applicants that pass the multiple choice and essay portions of the exam become candidates to have their PII and exam score delivered by ACT to DoS for use by the QEP. The QEP evaluates the candidates by career track. Panels rank candidates by career track, after which the Board of Examiners determines a cut line based on expected hiring numbers. Those above the cut line are chosen to be invited to an oral assessment. The information about candidates chosen for an oral assessment is delivered to ACT via encrypted CD-ROM. ACT issues invitations to the selected candidates for Oral Assessments. Oral Assessment results and candidate information is loaded into the Recruitment, Examination, and Employment Tracking Application (REETA). Candidate information that resides within REETA is no further transmitted or disclosed.

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

No data mining methods, pattern-based queries, searches, or matches are used to analyze candidate PII. The analytical method used to score applicant essay portion of the exam is the "T-score" statistical method, commonly used to establish norms for standardized exams.

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

Neither FSOT nor analysts that receive candidate exam information from ACT use commercial, publicly available, or any other Federal agency information as part of the exam, or as part of the final determination process in the selection of Foreign Service Officers.

d. Are contractors involved in the use of PII?

The Validus software is owned, operated, and maintained by ACT. All contractors are required to complete, and repeat when appropriate, security awareness training. All contracts contain approved Federal Acquisition Regulation Privacy Act clauses. ACT ensures that all their personnel working in the FSOT environment comply with the security policies and procedures outlined in their security plan. Applicant data collected via FSOT is the property of 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 FSOT system security plan delineates responsibilities and expected behavior of all individuals. In addition, the 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.

5. Retention

a. How long is information retained?

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 the National Archives and Records Administration. More specified information may be obtained by writing to the Director, Office of IRM Programs and Services; A/RPS/IPS;
U.S. Department of State, SA-2; Washington, DC 20522-6001.

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 FSOT. All records containing PII 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. When records have reached their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration.

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?

The information is maintained and used by the HR Recruitment, Examination, and Employment office (HR/REE). No candidate information is shared with any other organizations internal to DoS.

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

Any internal uses of the information by HR/REE employ secure methods approved for the internal transmission of sensitive but unclassified (SBU) information.

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 FSOT's 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 FSOT 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?

FSOT does not directly share information with any organization external to DoS other than with ACT.

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

With the exception of the sharing of candidate information with ACT, no information is shared outside DoS.

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

The contract with ACT contains approved Federal Acquisition Regulation Privacy Act clauses. ACT ensures that all their personnel working in the FSOT environment comply with the security policies and procedures outlined in their security plan.

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. Examination applicants can view the DoS *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 DoS *Privacy Act Statement* can also be found at *www.act.org/fsot/faq.html#paperwork*. 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 including an applicant's SSN is voluntary. However, the failure to provide all information requested may prevent timely processing of an applicant's submission, or may prevent ACT from registering an applicant for the examination.

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, and would result in the negation of the system's intended use.

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 is also in the System of Records Notice. 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?

If an applicant's name, address, or email address changes prior to the exam results notification date, the applicant may contact ACT by telephone, or submit the new contact information by email to fsot@act.org or in writing to ACT, Inc., P.O. Box 4070, Foreign Service Officer Test (82), Iowa City, Iowa 52243-4070.

Once a career track is chosen, applicants cannot change their career track choice at a later point in the selection process. Careful thought should be put into making this decision. In addition, procedures for notification and redress are published in the System of Record Notice. An applicant's registration remains active until the applicant takes the examination or up to a maximum period of 12 months from the date of submission, whichever comes first. If an applicant does not schedule a test date and take the test, or is not selected to schedule a test date within that period, the applicant must wait 11 months from the date of the original registration submission and then submit a new registration.

Applicants have limited access to their own profile data for updating their personal information. Once an applicant is notified by ACT that they are a successful candidate in the Foreign Service Officer selection process by virtue of having achieved a passing score, they are provided notice that their FSOT cycle is open for online scheduling. A candidate is then able to access the Foreign Service Oral Assessment scheduling application.

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. 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?

ACT designates only certain personnel to have access to FSOT information and systems housed in ACT facilities. All ACT 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 DoS and is based on the need of the individual requesting the privileges upon presenting proper credentials.

ACT 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 FSOT security plan, ACT's 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
- Privacy Act of 1974

Only authorized DoS current employees and contractors are provided access to FSOT at ACT facilities. A system use notification ("warning banner") is presented on the FSOT 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 authorized users?

The DoS appropriate use policy and Rules of Behavior are the general terms under which federal employees and contractors use the system. 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 DoS 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 FSOT System Security Plan and DoS 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 FIPS 199 security categorization assigned to FSOT. The safeguards reduce privacy risk related to user access to a negligible level. HR places great emphasis on the security of the data under its purview by adherence to best security practices and compliance 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 the 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 involve privacy risk?

DoS does not own the Validus software. DoS purchased the rights to use the software and owns all applicant information. FSOT utilizes web forms and relational database technology to gather test data.

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 essay questions, all web form fields are designed using defined attributes that highly constrain user inputs. The relational database within FSOT is annually tested for secure configuration and vulnerability according to DoS security policy.

12. Security

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

FSOT was granted an Approval to Operate on 1/25/2008, for continued operation for up to 36 months. The Approval to Operate expires on 1/25/2011.