

# FSOT PIA

## 1. Contact Information

<p><b>A/GIS Deputy Assistant Secretary</b> Bureau of Administration Global Information Services</p>
---

## 2. System Information

- (a) Name of system: Foreign Service Officer Test
- (b) Bureau: Human Resources (HR)
- (c) System acronym: FSOT
- (d) iMatrix Asset ID Number: 1074
- (e) Reason for performing PIA: For security reauthorization of the system. Some information has changed since the last PIA conducted in January 2015.
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): Since the last authorization there has been an update to the HR Points of Contact. Additionally, it has been about three years since the last PIA was done.

## 3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
  - Yes
  - No - Contact IRM/IA at [IASolutionCenter@state.gov](mailto:IASolutionCenter@state.gov) for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?  
Authorization to Operate (ATO) expires February 28, 2018.
- (c) Describe the purpose of the system:  
The FSOT system supports the Department of State Bureau of Human Resources mission requirements for recruiting Foreign Service Officers for the United States government. The FSOT application is composed of several components to process information during various parts of the recruiting process. These include: registering candidates to take the FSOT, scheduling and administering the FSOT, maintaining the candidate's registration

profile, scoring the FSOT, forwarding scores and candidate information to the Department of State (DOS) for further selection processing, and scheduling the oral examination for selected candidates.

The process starts with the web and application servers, which take the initial registration information from the candidate and schedule a time/place to take the test. At the arranged time/place, the candidate is prompted to enter their biographical information and answer other questions relevant to the position of Foreign Service Officer. The questions for the test are generated using Pearson VUE proprietary software and systems called the VUE Testing System (VTS). The responses are scored and stored in an SQL database.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

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.

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

- 22 U.S.C. 2581 (General Authority of Secretary of State)
- 22 U.S.C 2651a (Organization of the Department of State)
- 22 U.S.C 2901 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, as amended (Numbering System for Federal Accounts Relating to Individual Persons)
- Executive Order 9830 (Amending the Civil Service Rules and Providing for Federal Personnel Administration)
- Executive Order 12107 (Relating to the Civil Service Commission and Labor-Management in the Federal Service)

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

Yes, provide:

- SORN Name and Number:

Human Resources Records, State-31, July 19, 2013

- SORN publication date (found under the Volume Number and above the Public

Notice Number on the published SORN): Volume 78, Number 139, July 19th 2013.

No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?  Yes  No

If yes, please notify the Privacy Division at [Privacy@state.gov](mailto:Privacy@state.gov).

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?  Yes  No

(If uncertain about this question, please contact the Department's Records Officer at [records@state.gov](mailto:records@state.gov) .)

If yes provide:

Schedule Number: A-04-004-03b

Length of time information retained in system – TEMPORARY. Destroy when active agency use ceases. (NC1-59-83-4, item 25b)

Type of information retained in system - Personnel Records

The records in FSOT are subject to specific records disposition schedules published by the Records Management Division (A/GIS/IPS/RA) and OPM. The schedule for record disposition varies with record type. Retention and disposal of FSOT record types are specified in Domestic Records Disposition Schedule, Chapter A-04 and in Personnel and Foreign Records Disposition Schedule, Chapter B-07, Personnel.

The Department also follows the National Archives and Records Administration (NARA) General Records Schedule 1 (GRS-1) for Civilian personnel records supplemented as necessary to meet the specialized records management needs of the Department.

#### 4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes  No

- If yes, under what authorization?

Authorization for the Department to perform SSN collection comes from the following:

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

(c) How is the information collected?

Information is collected directly from applicants through the FSOT system. The process starts with the web and application servers, which take the initial registration information from the candidate and schedule a time/place to take the test. At the arranged time/place, the candidate is prompted to enter their biographical information and answer other questions relevant to the position of Foreign Service Officer.

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

- If you did not select "Department-owned equipment," please specify.

The information is housed in SQL Server Database managed by Pearson VUE located at Pearson Datacenter in Iowa City, IA.

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

The applicant is responsible for 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).

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The applicant is responsible for making sure their information remains current. The applicant may change contact information (i.e., phone numbers, mailing address, and email address) by going into their profile and editing the information.

- (g) Does the system use information from commercial sources? Is the information publicly available?

The system does not use information from commercial sources or publicly available information.

- (h) Is notice provided to the individual prior to the collection of his or her information?

Individuals are made aware of the uses of the information prior to collection. Examination applicants can view the Department of State'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 the web application is launched, prior to login. In addition, a copy of the Department of State's website Privacy Notice can also be found at <https://www.state.gov/privacy>. The purpose, use, and authority for collection of information submitted are described in the System of Records Notice, STATE-31.

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

- If yes, how do individuals grant consent?

Information requested including an applicant's Social Security number is voluntary. However, the failure to provide all information requested may prevent timely processing of an applicant's submission, or may prevent Pearson VUE from registering an applicant for the examination.

- If no, why were individuals not allowed to provide consent?

- (j) How did privacy concerns influence the determination of what information would be collected by the system?

Privacy concerns were considerations. However information collected is a requirement of the business processes for the system. As such only the minimum amount of information required to perform these functions is collected.

## **5. Use of information**

- (a) What is/are the intended use(s) for the information?

To collect information to test candidates for the position of Foreign Service Officers.

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

The use of information is relevant to the purpose for which FSOT applications were designed.

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

There is no analysis other than the standard reporting requirements.

If yes:

- (1) What types of methods are used to analyze the information?
- (2) Does the analysis result in new information?
- (3) Will the new information be placed in the individual's record?  Yes  No
- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?  
 Yes  No

## **6. Sharing of Information**

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

Information collected in FSOT is used for registering candidates to take the FSOT, scheduling and administering the FSOT and maintaining the candidate's registration profile and scores. This information is shared with the Department of State (DoS) for further selection processing and scheduling the oral examination for selected candidates.

- (b) What information will be shared?

Information transferred to DoS includes personal data (full name, social security number (SSN), date of birth, nationality, mailing address, personal email address, phone number, race, national origin, salary, education, military status, disability status) related to examination scores and employment qualifications.

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

The purpose of FSOT information sharing with DoS is for further selection processing, and scheduling of oral examination for selected candidates.

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

Information is shared by secure network transmission methods permitted under Department policy for the handling and transmission of SBU information including Transport Layer Security (TLS) v1.2. Data is exchanged with HumRro, Department of State and Pearson VUE by SFTP hosted by Pearson VUE. HumRro provides the test questions to be utilized for the FSOT and Pearson VUE provides the candidate data related to the delivery of the FSOT exam.

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

Candidate examination and personal data are shared with DoS through Secure File Transfer Protocol (SFTP).

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

Privacy concerns identified include: access to PII data including full name, social security number (SSN), date of birth, nationality, mailing address, personal email address, phone number, race, national origin, salary, education, military status, disability status by persons without a need to know. The FSOT System Security Plan delineates responsibilities and expected behavior of all individuals who access the FSOT application. The transfer of PII between Pearson VUE and DoS must be encrypted to protect the PII. Secure File Transfer Protocol (SFTP) is used to encrypt data transfer. Section 8 also addresses the security of PII in FSOT.

## **7. Redress and Notification**

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

To gain access to their account, a candidate must visit <http://www.pearsonvue.com/fsot/> and click on “Sign in” in the upper right hand side of the landing page. They would use the username and password that they created during initial registration to access their account. If the candidate has forgotten either the username or password, they may click on the “I forgot my username or password” link below the log in boxes. They would be able to gain access to their account by answering security questions and using the e-mail address they used to create their account. They also have the option of contacting Pearson VUE’s customer service at this link (<http://www.pearsonvue.com/fsot/contact/>) to get assistance with accessing their account.

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

Yes  No

If yes, explain the procedures.

Applicants may update their contact information on their own. If a candidate wants to change their name, SSN, or date of birth, they must submit documentation to the Pearson VUE team for review and the edits will be made for them.

If no, explain why not.

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

Applicants are informed of this if they contact Pearson VUE.

## **8. Security Controls**

(a) How is the information in the system secured?

The information in FSOT is secured through implementation of the minimum baseline of controls for a Moderate impact system for confidentiality, integrity, and availability. Security controls are specific to FSOT control descriptions in NIST SP 800-53. Access to the application from an end user and user with elevated privileges are controlled by the application administrators. Application identifiers and authenticators are provisioned based on the NIST SP 800-53 and State requirements. The server operating system, web servers, applications, and databases are configured to meet security standards and best practices. Account privileges are based on roles with the concept of least-privilege and need-to-know.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

Full information on assignment of users to roles is documented in the FSOT System Security Plan. Role assignment is controlled based on application.

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

Access to data is determined by roles as defined in the FSOT SSP. Privileged system administration and database administration roles are assigned in line with job function. System Administration access is limited to authorized Pearson personnel and access to the Pearson VUE servers are reviewed on a monthly basis to ensure access is restricted to authorized personnel. Database Administration access is limited to authorized Pearson personnel and it is reviewed on a quarterly basis. Application user access is limited to authorized Pearson personnel and are provisioned and de-provisioned through a formal and documented process. Application access is reviewed and validated on a bi-annual basis. General users are potential employees of the Foreign Service and are only permitted access to their test and profile data.

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

The Department of State’s appropriate use policy and rules of behavior are the general terms under which federal employees and contractors use FSOT. The Department of State requires all new employees and contractors to complete a Cyber Security Awareness Course (PS 800) provided by DS/SI, before or immediately after the employment start date and prior to being granted access to the system. In addition, the OpenNet account request form signed by all employees and contractors who will have access to FSOT contains a “Computer Security Awareness Form” that includes privacy orientation. All Department of State personnel must complete a Cyber Security

Awareness Course yearly. Additionally all Department employees are required to take PA459-Protecting Personally Identifiable Information.

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

If yes, please explain.

Transmission of data from the Internet for web (https) sessions uses encryption through TLS protocols.

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

The security measures above were influenced by the baseline requirements for a system with moderate impact rating for confidentiality, integrity, and availability. FSOT followed the data categorization procedures for confidentiality, integrity, and availability based on Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. Additionally, the DoS IRM/IA Security Categorization Form (SCF) and eAuthentication Risk Assessment guides were used to determine the overall impact and eAuthentication levels of each FSOT application. NIST SP 800-53 security controls for a moderate system were included in the design and operation of FSOT. In particular, the PII influenced the application of the controls from the following families: access control, audit and accountability, identification and authentication, system and communications protection, and system and information integrity control families.

## **9. Data Access**

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

The following system user definitions describe the roles and access.

- System administrators are limited to authorized Pearson personnel. Administrative access to the Pearson VUE servers are reviewed on a monthly basis to ensure access is restricted to authorized personnel.
- Database administrators are limited to authorized Pearson personnel. Access to key databases (DBA and direct access) is reviewed on a quarterly basis.
- Firewall administrators are limited to authorized Pearson personnel. Firewall administrator access to the firewall is reviewed twice a year by the IT Security team.
- Application users are limited to authorized Pearson personnel. Application users are provisioned and de-provisioned access through a formal and documented process. Application access is reviewed and validated on a bi-annual basis.
- General users of the FSOT system are potential employees of the Foreign Service. This includes people located domestically and abroad who wish to apply for a Foreign

Services position. They are not permitted access to anything except the test and their profile data.

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

Access to data in the system is determined by the individual's role and authorized responsibility.

- Access to data is determined by roles as defined in the FSOT SSP. Privileged system administration and database administration roles are assigned in line with job function. Application access is reviewed and validated on a bi-annual basis.

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

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

Users have restricted data access based on their individual role and privileges granted. See section 9a above for full breakdown of access restrictions based on roles.

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

Access is restricted by application and roles within each application. Full description of roles and permissions for FSOT application with end user access is provided in Section 9a above. Data access is limited by a least privileged and need-to-know restriction for each role. End users are limited to viewing their own personal information.

