

Foreign Service Officer Test (FSOT) PIA

1. Contact Information

A/GIS/IPS Director

Bureau of Administration

Global Information Services

Office of Information Programs and Services

2. System Information

- (a) Name of system: Foreign Service Officer Test
- (b) Bureau: HR/EX
- (c) System acronym: FSOT
- (d) iMatrix Asset ID Number: 1074
- (e) Reason for performing PIA:
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): FSOT has recently completed its Annual Assessment towards gaining its Approval to Operate (ATO). The ATO decision memorandum is within IRM/IA domain. Additionally, over three years has passed since the previous PIA; Dated May 12th 2010. A new commercial contractor now maintains the Foreign Service Officer Test Application that is used to administer the online Foreign Service Written Exam.

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 for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?

The FSOT ATO decision memorandum was signed on March 12th, 2015.
- (c) Describe the purpose of the system:

The Foreign Service Officer Test (FSOT) supports the Department of State Bureau of Human Resources mission requirements for recruiting Foreign Service Officers for the United States government. The FSOT registration and delivery system is used to administer the exam for officer (“Generalist”) candidates that are referenced in the Foreign Service Act. The FSOT computer-based exam now serves as the only initial exam for selecting Foreign Service candidates for Generalist appointments. 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 proprietary software and systems. The responses are scored and stored in a 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
- 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. 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) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number: Human Resources Record, State-31
- 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.

(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).

If yes provide:

- Schedule number: A-04-003-01a through A-04-003-20
- Length of time the information is retained in the system: When records have reached their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration
- Type of information retained in the system: 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

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?

- 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 through an interactive user session through the contractor hosted web site. The candidate user creates an account in a web form process providing name, date of birth, SSN, residential address, telephone number, and e-mail address.

(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.

Contractor Headquarters, Bloomington, MN and their Data Center, Iowa City, IA.

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

Information accuracy is the responsibility of the candidate who entered it to check when created and logged into their FSOT user account.

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

FSOT users must check their personal information and update if it is not current.

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

FSOT does not use information from commercial sources. FSOT information does not use publicly available.

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

Yes. The FSOT account creation web page posts a privacy popup window with a link to a document containing the complete Department of State Privacy statement.

(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?

The FSOT user must check the box in the Privacy Policy Acceptance popup box and click the "Yes, I agree to the policies" button

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

Individuals must provide consent before continuing.

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

Privacy concerns were considered. However information collected are requirements of the business processes for the system.

5. Use of information

(a) What is/are the intended use(s) for 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: An “applicant” is a person who applies for the examination. A “candidate” is a person who achieved a FSOT passing score required to continue in the Foreign Service Officer Selection process.

An applicant’s Social Security number is used to uniquely identify their record because other people may have the same name and birth date. Information collected from an applicant, including their SSN. 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, national origin, and disability status are effectively de-identified and only used to analyze the effectiveness of the Department of State hiring process.

The Social Security number is used as the candidate identification number, thus ensuring proper identification of candidates throughout the selection and employment process.

Following the exam, those applicants who pass the multiple choice and essay portions of the exam become candidates and their PII and exam score is provided to the Department of State for use by the Qualification Evaluation Panel (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 invited to an oral assessment, the next step of the selection process. The information about candidates chosen for an oral assessment is delivered by the contractor via encrypted file transfer. Oral Assessment results and candidate information is loaded into the Recruitment, Examination, and Employment Tracking Application (REETA). Candidate information that resides within REETA is not further transmitted or disclosed.

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

Yes No

FSOT information is used to satisfy the Department of State Bureau's HR mission for recruiting Foreign Services officers to the U.S. Government

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

The information collected may be used to prepare statistical reports and analyses at the Department of State. Such reports and analyses do not reveal identities. The information is maintained and used by the Human Resources Recruitment, Examination, and Employment office (HR/REE). No candidate information is shared with any other organizations internal to the Department of State.

If yes:

(1) What types of methods are used to analyze the information?

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.

- (2) Does the analysis result in new information?

Analysis produces reports. Analysis does not result in new information containing PII.

- (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.

The information is maintained and used by the Human Resources Recruitment, Examination, and Employment office (HR/REE). No candidate information is shared with any other organizations internal or external to the Department of State.

The information collected may be used to prepare statistical reports and analyses at the Department of State. Such reports and analyses do not reveal identities, and may be shared outside the Department of State.

- (b) What information will be shared?

FSOT candidate information is not shared outside HR/REE.

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

FSOT candidate information is not shared outside HR/REE.

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

FSOT candidate information is not shared outside HR/REE.

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

FSOT candidate information is not shared outside HR/REE.

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

FSOT candidate information is not shared outside HR/REE.

7. Redress and Notification

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

The applicant user may edit inaccurate or erroneous information address, phone and email address by logging into their account and correcting the information under their “profile.”

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

Yes No

If yes, explain the procedures.

The applicant user may edit inaccurate or erroneous address, phone and email address by logging into their account and updating their “profile.” To change name, SSN or birth date, the user must contact the contractor’s call center numbers for live customer service assistance.

- (c) By what means are individuals notified of the procedures to correct their information?
Notification of procedures to correct applicant user information are provided to registered candidates in an e-mail response from the FSOT call center which includes direction to use the profile or voice telephone contact numbers for further assistance. Candidates can also edit the information (physical/email address) themselves anytime they log into their accounts. The profile link is in a column on the right side of the screen and is available to the candidate from any place in the application.

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 used in FSOT meet the requirements found in the National Institute of Standards and Technology’s (NIST) Special Publication 800-53 (NIST SP 800-53) which provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. Access to the application from an end user or a user with elevated privileges are controlled by the application administrators. Application identifiers and authenticators are provisioned based on the NIST SP 800-53 and DoS requirements. The server operating system, web servers, applications, and databases are configured according to the contractor’s secure configuration standards which meet, at a minimum, DoS standards. 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.

The Separation of Duties in the FSOT System Security Plan (SSP) refers to the contract company’s Corporate Security Policy which states, "Separations of duties are to be implemented to separate roles for developers from those that promote and run operational applications." The SSP indicates that when access rights are allocated to an employee, the authorizing manager must review the totality of the employee's access rights to ensure a

segregation of duties control weakness will not be created; the contractor applies the aforementioned corporate security policy to separation of duties with privileged, non-privileged, functional roles and user roles in FSOT. FSOT SSP refers to the contract company's policy on Least Privilege which states, "The level of access granted is appropriate for the business purpose and does not compromise segregation of duties". Further, their Access Rights policy requires that all their personnel are given access to only those internal applications and data required to perform their day to day job functions, and removed immediately if they are involuntarily terminated, or removed at the end of contract in all other cases. The policy applies to all environments including and supporting FSOT: Production, Client Testing and Training, and Quality Assurance systems.

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

The Auditable events in the FSOT System Security Plan(SSP), refers to the contract company's Corporate Security Policy which states, "Auditing of events are to be implemented within FSOT to define the audit trail process, the types of logs to be maintained – both manual and automated, and who may delete, modify, or dispose of FSOT event logs and audit trails. The SSP indicated which events need to be auditable in FSOT. FSOT SSP refers to the contract company's policy on auditable events which states "auditable events include logon success and failures, policy changes, privileged use, system events, account creation, account deletion, and change password attempts, remote dial-up access, web browsing and file transfer activity. The policy applies to all environments including and supporting FSOT: Production, Client Testing and Training, and Quality Assurance systems.

The Content of Audit Records in the FSOT System Security Plan (SSP), refers to the contract company's Corporate Security Policy which states " Content of Audit Records retained within FSOT contains sufficient information to, at a minimum, include the type of event, when the event occurred, where the event occurred, source of event, the outcome of the event, and the identity of individuals or subjects associated with the event. Refer to 5(C) for Contract Company's policy on auditable events. The policy applies to all environments including and supporting FSOT: Production, Client Testing and Training, and Quality Assurance systems."

The Audit Review, Analysis, and Reporting in the FSOT System Security Plan (SSP), refers to the contract company's corporate Security Policy which states "Reviews and Analysis of system audit records is conducted for indications of inappropriate or unusual activity. The SSP indicated the frequency of the review and analysis of audit records. FSOT SSP refers to the contract company's policy on Audit Review, Analysis and reporting, which states "Contract Company monitors audit records on a daily basis and

performs a formally documented review on a monthly basis". The policy applies to all environments including and supporting FSOT: Production, Client Testing and Training, and Quality Assurance systems.

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

The contracting companies Security Training policy requires that all contractor personnel must complete privacy training before they can perform job duties that involve access to Company Confidential and Strictly Company Confidential data. Contractor personnel who violate this policy shall face disciplinary action, up to and including termination of employment. The contracting Security and Privacy Officer are each responsible for ensuring that all applicable personnel are made aware of company policy and acknowledge receipt and review.

- (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 Integrity & Transmission Confidentiality, Protection of Information at Rest, & Identification and Authentication in the FSOT System Security Plan(SSP), refers to the contract company's corporate Security Policy which states "confidentiality and integrity of the information system is to be protected, protected at rest, and uniquely identified and authenticates privileged users" The SSP indicates how the confidentiality and integrity of the information system is achieved which states "Contract company's Virtual University Enterprises (VUE) testing systems (VTS) protects the integrity of web services and test center communications through Secure Socket layer (SSL), implements the use of strong encryption on all Production and client testing databases, and uses 2 factor authentication for accessing FSOT Production, Client Testing and Training, and Quality Assurance systems.

- (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 FSOT. NIST SP 800-53 security controls for a moderate system were included in the design and operation of FSOT. In particular, the PII data 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?

- **System administrators** are limited to authorized contractor company personnel. Administrative accesses to the servers are reviewed on a monthly basis to ensure access is restricted to authorized personnel.
- **Database administrators** are limited to authorized contractor company personnel. Access to key databases (DBA and direct access) is reviewed on a quarterly basis.
- **Firewall administrators** are limited to authorized contractor company personnel. Firewall administrator access to the firewall is reviewed twice a year by the IT Security team.
- **Application users** are limited to authorized contractor company 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 FSOT data is determined by the user role. Contractor company personnel assigned to administrator and security responsibilities have required levels of access necessary for processing registrations of applicant users, contacting applicant users, proctoring the FSOT exam, compilation and transmittal of completed exam applicant records for HR/REE.

(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.

Access is restricted based on the assigned user role. All privileged users listed in section 9a are commercial contractor employees vetted under terms of HR/REE's contract. General users, who are applicants and FSOT exam test takers, are restricted to only the personal information in their own account.

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

The Separation of Duties in the FSOT System Security Plan (SSP) refers to the contract company's Corporate Security Policy which states, "Separations of duties are to be implemented to separate roles for developers from those that promote and run operational applications." The SSP indicates that when access rights are allocated to an employee, the authorizing manager must review the totality of the employee's access rights to ensure a segregation of duties control weakness will not be created; the contractor applies the aforementioned corporate security policy to separation of duties with privileged, non-

privileged, functional roles and user roles in FSOT. FSOT SSP refers to the contract company's policy on Least Privilege which states, "The level of access granted is appropriate for the business purpose and does not compromise segregation of duties". Further, their Access Rights policy requires that all their personnel are given access to only those internal applications and data required to perform their day to day job functions, and removed immediately if they are involuntarily terminated, or removed at the end of contract in all other cases. The policy applies to all environments including and supporting FSOT: Production, Client Testing and Training, and Quality Assurance systems.