PRIVACY IMPACT ASSESSMENT

FRONT END PROCESSOR

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: August 2022
(b) Name of system: Front End Processor
(c) System acronym: FEP
(d) Bureau: Consular Affairs
(e) iMatrix Asset ID Number: 344
(f) Child systems (if applicable) iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

☐ New system
☐ Significant modification to an existing system
☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The FEP provides mission-critical support for timely and accurate translation of data requests between the Passport Systems' major applications. FEP is a multi-threaded application that provides the Travel Document Issuance System (TDIS), Passport Record Imaging System Management (PRISM), American Citizen Services (ACS), Consular Lookout and Support System (CLASS), Passport Information Electronic Records System

(PIERS) and Passport Lookout Tracking System (PLOTS) applications the ability to communicate with several database systems.

With one request, FEP can query multiple applications of these systems and return a consolidated response. FEP capabilities assist Consular Affairs in processes requested services while reducing the issuance of passports or other services to those who may pose a national security threat and/or who may be using a false identity.

FEP does not generate or save any data. Its only function is to perform accurate data translation and delivery. For every data request and translation, there is a transaction record entered into the FEP database server. FEP prepares and drops batches of data for transfer to outside agencies via Consular Data Information Transfer System (CDITS). CDITS is a separate system outside of the FEP boundary.

The FEP performs the following:

- Accepts the client system request
- Places the request in the appropriate format for each database
- Sends the reformatted request
- Collects a response from each of the various system databases
- Consolidates the responses
- Reformats the responses
- Sends a single consolidated reply to the requester

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

The Following PII elements apply:

- Names
- Date of Birth
- Place of Birth
- Social Security Numbers
- Phone Numbers
- Passport Number
- Personal Address
- Personal E-mail Address
- Photos/ Biometrics
- Citizenship

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

- 8 U.S.C. 1101-1104, 1401-1503 (Immigration and Nationality Act of 1952, as amended)
- 22 U.S.C 2651(a) (Organization of Department of State)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)

- 22 U.S.C. 211a-218 (Passports)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 C.F.R. Subchapter F, Nationality and Passports

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

☒Yes, provide:

SORN Name and Number: Passport Records, STATE-26
SORN publication date: March 24, 2015

SORN Name and Number: Overseas Citizen Services Records and Other Overseas Records, STATE-05
SORN publication date: September 8, 2016

☐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 Office 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 (Consolidate as much as possible):

Schedule number: A-13-001-16, Passport Lookout Master
Disposition Authority Number: N1-059-04-2, item 16 A-13-001-16 Passport Lookout Master
Length of time information is retained in the system: Destroy when active agency uses ceases. (ref. N1-059-96-5, item 16)
Type of information retained in the system: This on-line information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have been denied passports, or those who are not entitled to the issuance of full validity passport a and those whose existing files must be reviewed prior to issuance

Schedule Number: A-13-001-17 Passport Lookout Index
Disposition Authority Number: N1-059-04-2, item 17
Length of time information is retained in the system: Destroy when active agency uses ceases. (ref. N1-059-96-5, item 27

Type of information retained in the system: This on-line information system provides rapid access to names in the Passport Lookout Master.

Schedule Number: A-13-001-18, Name Check System
Disposition Authority Number: N1-059-04-2, item 18
Length of time information is retained in the system: Destroy when active agency uses ceases.
Type of information retained in the system: Name Check History Master. This series contains a yearly listing of requests by Passport Services and Visa Services personnel to query the Passport and Visa Lookout systems (see schedules for A-13-001-16 and 17). The listing provides statistical data for the Bureau of Consular Affairs.

Schedule Number: A-15-001-02, American Citizens Services (ACS) system
Disposition Authority Number: N1-059-09-40, item 1
Length of time information is retained in the system: TEMPORARY. Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is later. NOTE: ACS case records are replicated to the Consular Consolidated Database each day for long-term recordkeeping.
Type of information retained in the system: The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts. ACS records include case level data on the following types of citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases; lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Record level data includes· biographic information, case information, and case activity log.

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) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No ☐N/A

- If yes, under what authorization?

Executive Order 9397, November 22, 1943
Executive Order 13478, November 18, 2008
26 U.S.C. 6039E (Information Concerning Residence Status)

(d) How is the PII collected?

FEP receives and transmits electronic transactions containing PII to and from Consular Affairs systems addressed in paragraph 3c, via the State Department intranet, with the exception of PRISM. FEP only receives information from PRISM and does not transmit information to PRISM. FEP does not originate PII or collect PII from the public.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Accuracy is the responsibility of the processes incorporated in the CA source system that originally collects the information. The original PII submitted is validated for accuracy via the source system processes in which the applicant requests and apply for the CA service. External agencies providing information to the Department via CA source systems are responsible for the accuracy of the information in the records that the agency submits to the Department.

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

FEP receives current information containing PII from Consular Affairs systems listed in paragraph 3c. The source systems that provide CA services have processes in place to ensure information is current such as face-to-face interviews and follow-ups via mail; in addition to checking information against other CA databases for discrepancies.

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

No, FEP does not use information from commercial sources. The information in FEP is not publicly available.

(i) How was the minimization of PII in the system considered?

The PII listed in 3d are the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered and assessed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function of conducting queries and providing information to Consular personnel to adjudicate consular service requests of applicants.

5. Use of information

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

The PII enables FEP to query various databases to provide requested information. With one request, FEP can query multiple applications and return a consolidated response regarding crucial information in processing consular services requests such as: name check services, SSN checks, etc. By performing this function, the Department greatly reduces the risk of issuing passports or other services to those who may pose a national security threat and/or who may be using a false identity.

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

Yes, the PII transmitted supports the implementation of the State Department's Consular Services programs. The information is used to support passport application and other CA services submissions, processing, and the approval/denial decisions.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

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

(d) If the system will use test data, will it include real PII? ☐Yes ☐No ☒N/A
If yes, please provide additional details.

6. Sharing of PII

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

Internal: The term "internal sharing" traditionally refers to the sharing of information within the Department of State (Department) but external to the owning organization (referred to as "bureau" at the Department of State). However, since the various Bureau of Consular Affairs offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in FEP will be shared internally with CLASS, ACS, PIERS, TDIS, CDITS, PLOTS, and the CA Enterprise Service Bus (CAESB).

External: FEP does not share any information directly with external agencies. FEP prepares and drops batches of data into CDITS for transfer to outside agencies: the Department of Homeland Security Customs and Border Protection (DHS/CBP) and the Social Security Administration.

(b) What information will be shared?

Internal: The PII in paragraph 3d is shared with the CA systems listed in paragraph 6a depending on the request.

External: N/A

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

The Information in paragraph 3d is shared with CA systems in paragraph 6a to conduct queries of multiple CA databases and provide information to assist CA personnel in adjudicating and providing CA requested services.

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

Internal: Information is shared database to database by Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information. Secure transmission methods are implemented, including encryption using Hypertext Transfer Protocol Secure (HTTPS) and secure communications using Transport Layer Security and multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers. These are permitted by internal Department of State policies for handling and transmission of SBU information.

External: N/A

What safeguards are in place for each internal or external sharing arrangement?

Internal: Data transmitted to and from FEP is protected by robust encryption mechanisms inherent within OpenNet that encrypt the data from domestic and overseas posts to the database. Safeguards in place for internal sharing arrangements include secure transmission methods such as data encryption using Hypertext Transfer Protocol Secure (HTTPS) and secure communications using Transport Layer Security (TLS) and multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers. These safeguards are approved by in Department of State policies for handling and transmission of sensitive but unclassified (SBU) information. Electronic files are PIV/PIN or password protected and access is controlled by system managers. Audit trails track and monitor usage and access of systems that reside on the Department's secure intranet network, OpenNet.

External: N/A.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

FEP information is obtained from other CA source systems. When the collection of information by the source system involves potential PII collected on U.S. citizens, there is a Privacy Act Statement displayed on the form in which the applicant is seeking a consular service, such as a passport. It is the responsibility of the source system or other agency to provide notice to U.S. persons when collecting PII submitted via CA source systems.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

FEP pulls information on record subjects from other authorized Department systems. Consent is acquired via the CA source system or agency where the applicant applies for services.

(c) What procedures allow record subjects to gain access to their information?

The published SORNs STATE-26, Passport Records; and STATE-05, Overseas Citizen Services Records and Other Overseas Records, include procedures on how to contact an office to access records pertaining to the individual.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals must follow processes of the source system to request correction of information. Individuals can also follow the record access procedures in SORNs STATE-26, and STATE-05 which include procedures on how to contact an office for assistance in addressing inaccurate information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

The Department informs applicants on how to correct information during the adjudication process of the requested citizen service via the source system process. Additionally, individuals can also follow procedures outlined in SORNs STATE-26 and STATE-05, to acquire points of contact information to correct information.

8. Security Controls

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

FEP is secured within the Department of State intranet where risk factors are mitigated using defense in-depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information to perform official duties.

Access to FEP is controlled at the system level with additional access controls at the application level and requires a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN). This meets the dual authentication requirement for federal systems access that is required for logon. All accounts must be approved by the user’s supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

FEP is configured according to the Department’s Bureau of Diplomatic Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Access to FEP is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. FEP Database administrators (DBAs), and System Security administrators (SSAs) include both government and contractor personnel.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

FEP roles are defined according to the principle of least privilege. Access to FEP is role-based and restricted according to approved job responsibilities to perform official duties by the supervisor or manager. Local Information System Security Officers (ISSO) determine the access level needed by a user to ensure it correlates to the user's particular job function, manager's approval, and level of clearance.

(d) How is access to data in the system determined for each role identified above?

In accordance with Department of State policy, FEP employs the concept of least privilege for each user by allowing only authorized access to information in the system necessary to accomplish assigned job and tasks. All roles have been analyzed to determine the specific data set and corresponding functions required to accomplish assigned tasks in accordance with the person's job and level of security approved by the supervisor. This is accomplished via email/ and or a form. Accordingly, when a user or service account is added to a particular database role, access is limited to only the data and functions allotted. Accounts are deactivated upon departure of individuals in accordance with Department of State procedures.

Access to FEP is role-based and structured according to official job responsibilities and approval by the supervisor/manager. The user is granted only the role(s) required to perform officially assigned duties.

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

The FEP audit service on its servers captures logs, access attempts, and all actions, exceeding the Department of State requirements. Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information in FEP. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with

Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures
- Logons after-hours or at unusual times
- Failed attempts to execute programs or access files
- Addition, deletion, or modification of user or program access privileges
- Changes in file access restrictions

The purpose of the audit trail is to document unintended modification or unauthorized access to the system.

(f) Are procedures, controls or responsibilities regarding access to data in the system documented?

☒Yes ☐No

The FEP System Security Plan includes information and procedures regarding access to data in the system.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.