



Privacy Impact Assessment (PIA)

For: Front End Processor (FEP)

Version 07.00.02

Last Updated: April 18, 2014

1. Contact Information

Department of State Privacy Coordinator

Department of State Privacy Coordinator
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** April 18, 2014
- b. **Name of system:** Front End Processor
- c. **System acronym:** FEP
- d. **IT Asset Baseline (ITAB) number:** # 344
- e. **System description (Briefly describe scope, purpose, and major functions):**

The FEP system consists of four application servers and two Structured Query Language (SQL) Server databases located on the State Department unclassified intranet. FEP provides mission-critical support for timely and accurate translation of data requests between 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 and to interface with Department of Homeland Security Customs and Border Protection (DHS/CBP) via Microsoft BizTalk. BizTalk enables companies to integrate and manage automated processes by exchanging business documents between disparate applications. With one request, FEP can query multiple applications and return a consolidated response. FEP does not generate or save any new data. Its only function is to perform accurate data translation. For every data request and translation, there is a transaction record entered into the FEP database server.

The FEP Automated Information System (AIS) performs the following functions:

- Namecheck Service (CLASS, In-Process Database, and Multiple Issuance Verification queries)
- Social Security Administration (SSA) Service (checks the validity of the Social Security numbers and the Death Master File)
- Consular Lost and Stolen Passport System (CLASP) and CLASS (adds, updates, and queries)
- Signature Delivery Service (Passport book chip)

- CA XML (Extensible Markup Language) Translation
- Image Retrieval – sent to DHS/CBP
- Load balancing and failover support across client systems

An additional component to the FEP is the ESB (Enterprise Service Bus) Re-director. The ESB Re-director is a temporary initiative by the Department of State's Office of Consular Systems and Technology (CST) to facilitate the migration of the FEP Services to the ESB. The ESB Re-director is a proxy service that routes incoming queries from systems (Travel Document Issuance System, American Citizen Services, and Passport Lookout Tracking System) to the ESB for namecheck service as they become available for use on the ESB.

f. Reason for performing PIA:

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

g. Explanation of modification (if applicable):

FEP has been modified to run on SQL 2008 (instead of SQL 2000)

h. Date of previous PIA (if applicable): September 8, 2011

3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

FEP processes the following personally identifiable information (PII) elements when Passport Agencies and Department of State employees use the FEP system for executing queries and other transactions: names of individuals, birthdates of individuals, Social Security Numbers (SSN) or other identifying numbers, individual ID numbers from other sources, addresses/phone numbers or similar information, email addresses of individuals, images or biometrics ID, and other individually identifying items. The PII is maintained on-line in transaction logs for a period of two weeks. After that, the logs are permanently archived off-line by State Department Enterprise Operations.

b. How is the information collected?

FEP receives/transmits transactions containing PII to/from several systems. FEP does not originate PII data, collect PII data, nor does it maintain any PII data in long term storage.

c. Why is the information collected and maintained?

The FEP does not collect any PII data. The information is routed to and from several systems. The PII is maintained on-line in transaction logs for a period of two weeks. After that, the logs are permanently archived off-line by State Department Enterprise Operations. Information in the logs is helpful during any investigations involving breach of security or misuse of government systems.

d. How will the information be checked for accuracy?

Data processed by FEP is sourced from several systems. FEP is totally dependent upon the validity, safeguards, and accuracy of the PII security controls of the sourcing data systems.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The following authorities provide for the administration of the program supported by FEP:

- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- 22 U.S.C. 211a-218, 2651a, 2705 (2007); Executive Order 11295, August 5, 1966(Department of State Authority to Issue, Deny, Limit Passports);
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1401-1504(2013) (Nationality and Naturalization)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 8 U.S.C. 911, 1001, 1541-1546 (2013) (Citizenship and Passport related Crimes and Criminal Procedure)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- Section 236 of the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001
- 22 C.F.R. parts 50 and 51, Citizenship and Naturalization and Passports
- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

FEP collects the minimum amount of PII necessary to process and forward transactions. Since FEP receives and transmits PII data, FEP is designated as a moderate risk system. The primary risk is misuse by an authorized FEP System Administrator tampering with the system to extract PII from the FEP transaction stream. Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised, and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

These risk factors are mitigated through the use of Technical, Management, and Operational security controls. The FEP application data is protected by multiple layers of security controls including OpenNet security, FEP application security, Department site physical security and management security.

4. Uses of the Information

a. Describe all uses of the information.

The FEP system is an application that provides a communications interface to various front-end client applications for executing queries and other transactions with back-end systems and/or databases. It serves as a controller/translator where data requests from one application (client) are redistributed to various application systems (clients/servers). It consists of an engine that matches data front-end queries to the backend databases. The PII is maintained on-line in transaction logs for a period of two weeks. After that, the logs are permanently archived off-line by State Department Enterprise Operations. PII is retained for reference during any investigations involving breach of security or misuse of government systems.

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

The FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems major applications. FEP does not generate or save any new data; its only function is to perform accurate data translation. FEP does not perform any content analysis of PII.

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

FEP does not use any commercial information or public information. FEP does process PII from other Federal agencies including the Justice Department and the Social Security Administration. The FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems major applications. With one request, FEP can query multiple applications and return a consolidated response. FEP does not generate or save any new data; its only function is to perform accurate data translation. For every data request and translation, there is a transaction record entered into the FEP database server.

The FEP AIS performs the following functions:

- Namecheck Service (CLASS, In-Process Database, and Multiple Issuance Verification queries)
- Social Security Administration (SSA) Service (checks the validity of the Social Security numbers and the Death Master File)
- CLASP and CLASS (adds, updates, and queries)
- Signature Delivery Service (Passport book chip)
- CA XML Translation

- Image Retrieval – sent to CPB
- Load balancing and failover support across client systems

d. Are contractors involved in the uses of the PII?

Contractors are involved with the design, development, and maintenance of the system. Privacy Act information clauses have been inserted into all statement of work and become part of the signed contract. Each contractor employee is required to attend mandatory briefings that cover the handling of PII information prior to working on the task.

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.

The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, report's findings to appropriate officials, and takes necessary actions.

Database audit logs and Listener Logs are reviewed daily by the FEP DBA and any suspicious activity is immediately reported to the ISSO. The ISSO has an account on the database server and can access the audit log and other security related items that have been placed in designated folders/files for review. The FEP database audit logs are maintained indefinitely and are protected from unauthorized modification, destruction, and access by the limited rights assigned by the hand full of authorized database administrators.

DBA's use Windows OS authentication; NetIQ Security Manager sends automatic alerts of multiple logon failures and logons at after hours or unusual times. NetIQ Application Manager monitors the Listener Log for unusual activities and sends a pop up screen alert to DBA workstations.

The content of the FEP Audit records contain sufficient information to establish: event type, date, time, location, source, outcome (success or failure), and the identity of any user/ subject associated with the event.

In general, audit logs for FEP are retained indefinitely to provide support for after-the-fact investigations of security incidents and to meet regulatory and Bureau of Diplomatic Security (DS) information retention requirements in accordance with 12 FAM 622.5, 12 FAM 623, 12 FAM 629, 12 FAM 642 and 12 FAM 643 and as implemented and followed by Bureau of Diplomatic Security (DS) administrators.

FEP collects and maintains PII information in its logs for purposes of accountability. At any given time there are up to two weeks of logs online and available. These audit logs

help investigators determine if there has been a breach of security or misuse of government systems. Database logs are archived indefinitely by CST Enterprise Operations.

System audit logs are managed and maintained by EOS for a minimum of 6 months or when no longer needed to support reconstruction of audit log data.

The hardcopy applications and softcopy images of applications and supporting documents are retained for 99 years.

Contractors involved in the design, development, and maintenance of FEP are required to have a Moderate Risk Public Trust access authorization. This includes a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of FEP hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

5. Retention

a. How long is information retained?

The PII is maintained on-line in transaction logs for a period of two weeks. After that, the logs are permanently archived off-line by State Department Enterprise Operations.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The archived logs do not introduce any additional risk to the FEP system since they are maintained off-line so the PII can't be accessed by FEP. The two weeks of on-line logs are stored but never accessed again by FEP in the course of normal operations so they introduce negligible additional risk to the system.

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 FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems major applications. FEP does not generate or save any new data; its only function is to perform accurate data translation. FEP does not perform any content analysis of PII. The statistical information that is produced and

maintained by FEP is for CA operational purposes only. FEP serves as a robust, timely, and accurate data broker, controller, and translator for the following organizations internal to CA:

- FEP prepares and drops batches of data to Consular Data Information Transfer System (CDITS) for transfer to outside agencies.
- For requesting systems, FEP retrieves images of passports scanned and stored by Passport Record Imaging System Management (PRISM);
- Travel Document Issuance System (TDIS) runs name checks through FEP and uses FEP to get digital signatures for ePassports:
- Passport Lookout Tracking System (PLOTS) uses FEP for image retrieval and for CLASS adds, deletes, and queries;
- American Citizen System (ACS) runs name checks through FEP; and
- Information shared between Consular Lookout and Support System (CLASS) and FEP is for the purpose of name check and confirmation.

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

The FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems major applications. FEP does not generate or save any new data; its only function is to perform accurate data translation. FEP does not perform any content analysis of PII. FEP serves as a robust, timely, and accurate data broker, controller, and translator and only interacts directly with CA Systems over the Department OpenNet intranet. Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. For every data request processed by FEP, a full record of the data transaction is entered into the FEP database server transaction logs. The FEP performs the following:

- Receives the data request from the client system
- Logs the data request
- Formats the request as required for each database
- Sends the reformatted data request to the target database or system
- Logs the request for data
- Collects data request responses, consisting of the requested data
- Logs the data request responses
- Consolidates and reformats the data request responses
- Transmits a single consolidated reply to the client system
- Logs the transmission of data

The queries to the databases are processed in parallel, so that if a particular database is not operating, the overall process is not delayed. Regularly administered

security/privacy training ensures authorized users are aware of proper data handling procedures.

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

FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems major applications. FEP does not generate or save any new data; its only function is to perform accurate data translation. FEP does not perform any content analysis of PII. Human users are the primary threat vector associated with the risk of unauthorized disclosure of privacy information. Unauthorized disclosure of privacy information can result from social engineering, phishing, abuse of elevated privileges, or lack of appropriate and current training. Required management, operational and technical controls are verified annually to be in place to reduce and mitigate this risk, including required annual security training, separation of duties, rigorous application of least privilege, access badges, and personnel background screening.

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?

FEP information is not shared with any entities outside of the Department of State. Only authorized FEP System Administrators have access to the PII processed by the system.

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

External access to any non-Department entities is strictly prohibited.

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

FEP data is not externally shared or disclosed so there are no additional privacy risks.

8. Notice

The FEP system:

- contains information covered by the Privacy Act.
Provide number and name of each applicable system of records.
Passport Records – STATE-26
Overseas Citizen Services Records– STATE-05

- does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

FEP only processes transactions containing PII data that is collected by other CA systems. FEP does not collect PII data directly from any users.

b. Do individuals have the opportunity and/or right to decline to provide information?

FEP only processes transactions containing PII data that is collected by other CA systems. FEP does not collect PII data directly from any users.

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?

FEP only processes transactions containing PII data that is collected by other CA systems. FEP does not collect PII data directly from any users.

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.

FEP only processes transactions containing PII data that is collected by other CA systems. FEP does not collect PII data directly from any users.

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?

FEP only processes transactions containing PII data that is collected by other CA systems. The systems sourcing the data to FEP have the responsibility for meeting this requirement.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

FEP only processes transactions containing PII data that is collected by other CA systems. The systems sourcing the data to FEP have the responsibility for meeting this requirement.

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?

Access to the FEP application is restricted to cleared, authorized Department of State FEP System Administrators via the Department unclassified intranet. To access the system, administrators must be an authorized user of the Department of State's unclassified network. Each authorized administrator must sign a user access agreement before being given an account with FEP administrator privileges. The user access

agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. System administrators can access the FEP application only at the central server location to perform application maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality. External access to any non-Department entity is strictly prohibited.

Personnel accessing FEP information must be authorized by FEP management. Authorized personnel require a user ID and password to access FEP information. User access to FEP information is restricted to administrator roles only.

Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.)

b. What privacy orientation or training for the system is provided authorized users?

All FEP administrators must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access users must complete annual refresher training.

Administrators must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice that describe the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

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.

Several steps are taken to reduce residual risk related to system and information access. FEP utilizes access control lists to restrict access to only system administrators and the lists are regularly reviewed; inactive accounts are promptly terminated. Also, as mentioned earlier, the system audit trails that are automatically generated are regularly reviewed and analyzed. As a result of these actions, the residual risk is low.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

FEP does not use any technology known to introduce additional privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since FEP does not use any technology known to elevate privacy risk, the current FEP safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

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

The Department of State operates FEP in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security management Act (FISMA) of 2002 provision for the triennial recertification of this system, in September 2012, FEP received a limited Authorization to Operate (ATO), which expired April 30, 2013 because it was running on an outdated database (SQL 2000). On October 25, 2013, FEP (now on SQL 2008) completed the certification phase and is expected to receive a 3 year ATO, which will expire in late 2016 or early 2017.