Front End Processor (FEP)
Privacy Impact Assessment

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: March 16, 2012

(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):

FEP 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 is the master control mechanism of the Passport Systems software (e.g., Travel Document Issuance System (TDIS)) and consists of an engine that matches data queries to a variety of databases. With one request, FEP is able to query multiple applications and return a consolidated response. It operates on the Department of State's OpenNet. A public key infrastructure (PKI) is deployed to provide enhanced security services to the new generation of machine-readable travel documents (MRTD) such as U.S. passports. To provide assurance that passport applications are processed in a secure manner, FEP serves as a broker/controller, and allows the Passport Systems to "communicate" with the MRTD PKI system to obtain these enhanced security services. These controls are all tested and proven technologies, and they pose no additional privacy risks.

(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):

N/A

(h) Date of previous PIA (if applicable): December 5, 2008

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 collects and distributesthe following personally identifiable information (PII) elements when Passport Agencies and other Department of State employees use the FEP system for executing queries and other transactions: names of individuals, birthdates of individuals, SSN or other identifying numbers, individual ID numbers from other sources such as passport books, cards, and applications, address/phone numbers or similar information, email addresses of individuals, and images or biometrics IDs. The sources of information are the various systems that FEP serves as a controller/translator for, listed in 3(b). The information is passed from the source system to the destination system. Once the transaction is complete FEP deletes the data object.

b. How is the information collected?

FEP brokers the connection among the following front-end client applications: Travel Document Issuance System (TDIS), Passport Information Electronic Records System (PIERS), Consular Lookout and Support System (CLASS), Consular Lost and Stolen Passport System (CLASP), Consular Consolidated Database (CCD), Passport Data Information Transfer System (PDITS), Passport Lookout Tracking System (PLOTS), and American Citizen Services (ACS). PII in these front-end client applications is collected by FEP when FEP interfaces with the front-end client applications for executing queries and other transactions with back-end systems and/or databases. Information about how PII is collected by these front-end client applications listed here can be found in their respective privacy impact assessments (PIAs).

c. Why is the information collected and maintained?

FEP 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). The PII it collects from front-end client applications is immediately transmitted to back-end systems and/or databases, and the PII is not maintained by FEP once the transmission is complete.

d. How will the information be checked for accuracy?

Data from FEP is from various other Department of States systems identified in Section 3(b) above. FEP is totally dependent upon the safeguards of other systems for checking validity and accuracy. Information about how information is checked for accuracy by these front-end client applications can be found in their respective PIAs.

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. 1401-1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality use of U.S. Passports)
- 8 U.S.C. 911, 1001, 1541-1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, 2651a, 2705 (2007) (Executive Order 11295, Rules Governing the Granting, Issuing, and Verifying of United States Passports,August 5, 1996)
- 8 U.S.C. 1101-1503 (Immigration and Nationality Act of 1952, as amended)
- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- 18 U.S.C. Chapter 43, False Personation
- 18 U.S.C. Chapter 47, Fraud and False Statements
- 18 U.S.C. Chapter 75, Passports and Visas
- 22 U.S.C. Chapter 4, Passports
- 22 U.S.C. Section 2651a, Organization of Department of State
- 22 U.S.C. Section 2705, Documentation of Citizenship
- 22 USC Sec. 211a-218 (“The Secretary of State may grant and issue passports, and cause passports to be granted , issued, and verified in foreign countries by diplomatic and consular officers of the United States, and by such other employees of the Department of State who are citizens of the United States as the Secretary of State may designate, and by the chief or other executive officer of the insular possessions of the United States, under such rules as the President shall designate and prescribe for and on behalf of the United States, and no other person shall grant, issue, or verify such passports.”)
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705
- 8 U.S.C. 1185 (Travel Control of Citizens)

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 personally identifiable information necessary to function as a reporting tool that tracks predefined productivity statistics of U.S. passport agencies. With the collection of passport data, FEP has a high data element sensitivity and high data subject distinguishability. The primary risk is misuse by Department employees and contractors. Misuse could result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised, in addition to 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. Details on these mechanisms are provided in the FEP System Security Plan (SSP). The FEP application data is protected by multi-level systems security that includes OpenNet security, FEP application security, Department Site Physical security and management security.

4. Uses of the Information

a. Describe all uses of the information.

FEP is used as a controller/translator where data requested from a source system is redistributed to a target system and vice versa in support of the issuance of passports. Upon receiving a request from a target system, FEP queries other databases and returns a consolidated response. FEP provides a needed assurance that passport applications are processed in a secure manner. FEP maintains a log of all transactions. However, there is only one reporting mechanism in place which is for certain super sensitive passport data. When a user requests access to such data via the FEP, it logs the data to a reporting database. This data is reported using the Management Information System (MIS).

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

The data is not analyzed because this is a communications interface.

The only new information that FEP produces is statistical in nature and does not contain PII. It is used to study the performance of FEP.

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, public information or information from other Federal agency databases.

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

FEP is a Department of State system that is developed and maintained by contractor employees, some on whom are located at contractor-owned facilities.. The system is hosted at Beltsville Information Management Center (BIMC) in Beltsville, Maryland, with a disaster recovery site located in Charleston, South Carolina. Contractors are involved with the design, development, and maintenance of the system. All employees and contractors are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

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.

As FEP is a communications interface, data is not analyzed, meaning the privacy risk from collecting PII is minimal. Contractors involved in the design, development and maintenance of FEP are required to have a Moderate Risk Public Trust access authorization. There are technical system controls in place as described in 3(f) above.

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).

The internal users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the premises for the proper disposal of paper that is SBU.

5. Retention

a. How long is information retained?

The established retention period for electronic records in FEP is presently 100 years in accordance with published record schedules as approved by the National Archives and Records Administration (NARA). The following record schedule specifies that these records are to be destroyed when they are 100 years old: Chapter 13 Passport Records A-13-001-01c(2)(a) DisAuth No: NCI-59-79-12 item 1b – Transfer to WNRC monthly.

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

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the user of FEP throughout the lifetime of the data. Accuracy of the data is dependent on the individuals providing self-identifying information. The information is only retained for the amount of time that is required to perform the system’s purpose.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

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?

FEP 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). The statistical information that is maintained or produced by FEP is for operational purposes.

- FEP acts as a broker controller to the following internal organizations: Passport Record Imaging System Management (PRISM) scans and stores images of documents, FEP retrieves those images for requesting systems;
- 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 main purpose of the FEP application is to provide mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications running on systems connected to the State Department OpenNet Intranet. Availability is the key trait of the FEP system which ensures all the major Passports applications are operational by getting the requested data from FEP servers. FEP's 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 performs the following:

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

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

Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

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

The risks associated with sharing privacy information internally and the disclosure of privacy information are generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. To combat the misuse of information by personnel, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel 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 acts as a data broker/controller with the Social Security Administration (SSA). FEP prepares and drops batches of Social Security Number (SSN) checks for delivery to SSA through Consular Data Information Transfer System (CDITS) and periodically checks for completed responses from SSA via CDITS. The SSN check is performed by the Social Security Administration (SSA). The FEP submits a query to SSA with applicants name and SSN, the SSA responds back with a match or no match for the query.

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

The FEP has an asynchronus link with the Social Security Administration (SSA). The FEP routinely performs a file drop to a server in the DMZ which the SSA has access to. The SSA performs the namechecks and drops off the results on the same server which is later picked up by the FEP.

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

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and use not secure connections are also a serious threat to external sharing. FEP does not encrypt the data as none of the client systems it connects to performs encryption. The FEP relies on the underlying network infrastructure to encrypt the data. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with external sharing and disclosure including, but not limited to formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements (SLA), annual security training, separation of duties, least privilege and personnel screening.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

Passport Records – STATE-26

Overseas Citizens 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?

Notice is provided in the System of Records Notices for Passport Records – STATE-26 and Overseas Citizens Services Records – STATE-05. The main purpose of the FEP application is to provide mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications running on systems connected to the State Department OpenNet. Availability is the key trait of the FEP system which ensures all the major Passports applications are operational by getting the requested data from FEP servers. FEP's 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. Information about how notice is provided by the front-end systems identified in Section 3(b). for which FEP translates data can be found in their respective PIAs.

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

No. The main purpose of the FEP application is to provide mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications running on systems connected to the State Department OpenNet. Availability is the key trait of the FEP system which ensures all the major Passports applications are operational by getting the requested data from FEP servers. FEP's 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. Information about the right to decline to provide PII to be used by the front-end systems identified in Section 3(b) for which FEP translates data can be found in their respective PIAs.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. The main purpose of the FEP application is to provide mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications running on systems connected to the State Department OpenNet. Availability is the key trait of the FEP system which ensures all the major Passports applications are operational by getting the requested data from FEP servers. FEP's 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. Information about the right to limit the uses of PII collected by the front-end systems identified in Section 3(b) for which FEP translates data can be found in their respective PIAs.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The main purpose of the FEP application is to provide mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications running on systems connected to the State Department OpenNet. Availability is the key trait of the FEP system which ensures all the major Passports applications are operational by getting the requested data from FEP servers. FEP's 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. Information about how notice is provided to individuals and how the risks of them being unaware of the collection of PII collected by the front-end systems identified in Section 3(b) for which FEP translates data can be found in their respective PIAs.

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?

The data on individuals collected by FEP comes from other Department of State databases identified in Section 3(b) Information about how individuals may gain access to and amend their information contained in these systems can be found in their respective PIAs.

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. Therefore, this category of privacy risk is appropriately mitigated in FEP.

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 direct-hire or contractor personnel via OpenNet. To access the system, users must be an authorized user of the Department of State's unclassified network. Each authorized user must sign a user access agreement before being given a user account. 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. The FEP application enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties. 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/password to access FEP information. User access to FEP information is based on roles.

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?

Users internal to the Department must attend a security briefing and pass the computer cyber security and privacy awareness training prior to receiving access to the system. In order to retain the access users much complete annual refresher training.

Internal users 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. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and 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 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 is the master control mechanism of the Passport Systems software (e.g., Travel Document Issuance System (TDIS)) and consists of an engine that matches data queries to a variety of databases. With one request, FEP is able to query multiple applications and return a consolidated response. It operates on the Department of States OpenNet. A public key infrastructure (PKI) is deployed to provide enhanced security services to the new generation of machine-readable travel documents (MRTD) such as U.S. passports. To provide assurance that passport applications are processed in a secure manner, FEP serves as a broker/controller, and allows the Passport Systems to “communicate” with the MRTD PKI system to obtain these enhanced security services. These controls are all tested proven technologies, and they pose no additional privacy risks.

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

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, its 36 month authorization to operate expires May 31, 2012.