1. Contact Information

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

2. System Information

(a) Date PIA was completed: August 29, 2008

(b) Name of system: Electronic Visa Application Form

(c) System acronym: EVAF

(d) IT Asset Baseline (ITAB) number: 723

(e) System description:

The Electronic Visa Application Form (EVAF) enables Nonimmigrant Visa (NIV) applicants world-wide who have access to the internet to apply for a NIV via Form DS-156, "Nonimmigrant Visa Application" and to schedule appointments for consular services. The output from the system is a printed application form including a barcode containing the applicant's data that is then taken to a post. The post scans the barcode containing the applicant's information during data entry into CA's NIV system. EVAF also provides an on-line calendar that allows applicants applying for NIVs to schedule their non-immigrant visa interviews online, in turn providing NIV applicants with a more efficient and effective service. American citizens may also schedule appointments (see 3a below).

(f) Reason for performing PIA:

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

(g) Explanation of modification: Not applicable.

(h) Date of previous PIA: September 2007

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?

Information on EVAF is obtained directly from the Nonimmigrant Visa (NIV) applicants. This personal information provided by the applicant is stored in a 2D barcode on Form DS-156.

The types of personal information collected from the NIV applicant on Form DS-156 is as follows:

- Passport Number (foreign);
- Surname;
- First and Middle names;
- Date and Place of Birth;
- Home address;
- Home telephone number;
- Business/Mobile/cell number; and
- Contact information.

The EVAF system includes both an NIV and American Citizen Service (ACS) appointment capability. The information required to schedule a NIV interview appointment is provided directly by the applicant. Information collected from the applicant includes the following:

- Surname;
- Given Name;
- Passport Number (foreign); and
- Confirmation ID (only required to change or cancel an NIV appointment).

Regarding the ACS appointment capability, the information required to schedule an interview appointment is provided directly by the applicant. Information collected form the applicant includes the following:

- Surname;
- Given Name;
- E-mail Address;
- Contact Phone Number; and
- Date of Birth.

b. How is the information collected?

The information is collected directly from the nonimmigrant visa applicant through a secure web form application. The applicant manually inputs his or her data onto Form DS-156, “Nonimmigrant Visa Application,” via the EVAF online website at http://evisaforms.state.gov/. (See 6b below.)

The applicant is able to print the Form DS-156 with a barcode containing the applicant data that he or she then takes to post. The consular staff at post scans the barcode containing the applicant information during data entry into CA’s NIV system.

c. Why is the information collected and maintained?

No visa application information is retained. Information is collected to:

- Reduce the data entry burden at overseas posts;
- Allow a non-immigrant applicant to apply for a visa;
- Establish consistency in data collection;
- Improve data integrity;
- Allow for the processing and analysis of all application data; and
- Provide more efficient and effective services.

d. How will the information be checked for accuracy?

EVAF employs data integrity verification checks designed to ensure that end-users are allowed to only enter data that meets specific parameters. The adjudication process at post verifies the data contained on Form DS-156.

The system also ensures that the data items entered on Form DS-156 form by the applicant are consistent with validation rules stated on the NIV application.

Within the appointment system, applicants must enter data on the "Complete Appointment Details" page, which provides fields for appointment information to be supplied by the user. Only after all fields are completed will the applicant be able to submit the data in order to view an Appointment Confirmation Page that provides confirmation that an appointment has been scheduled and lists appointment details and instructions.

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

- Immigration and Nationality Act of 1965 (INA) as amended (P. L. 89-236), 8 U.S.C. 1202; and
- Immigration Act of 1990 (P. L. 101-649).

4. Uses of the Information

a. Describe all uses of the information.

Information in the system is used to apply for a NIV and to schedule, change or delete an appointment for a visa or an American Citizen Service.

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

The information contained in the Electronic Visa Application Form will be available in the NIV system once the barcode on the printed Form DS-156 is scanned during the NIV data entry process. If the barcode on the printed DS-156 form is scanned using the Remote Data Entry System (RDS) during the data entry process, applicant data is transferred from RDS to the NIV system.

Authorized visa adjudicators review this information for the purpose of the travel, the identity of the applicant and whether they qualify for a visa.

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

Not applicable.

d. Is the system a contractor used and owned system?

Contractors are the primary designers and developers of this system. All contractors involved with this system have appropriate security clearances up to Secret level and have undergone an annual security briefing. All contractors have approved Federal Acquisition Regulation Privacy Act clause and have signed the established rules of behavior.

5. Retention

How long is information retained?

Data retained by the EVAF scheduling and appointment system is currently retained for approximately one month past the appointment date in the scheduling system until it is archived. No visa information is retained.

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?

EVAF will share information with the Consular Consolidated Database (CCD) for the purpose of authenticating OpenNet (DoS intranet) users and allowing Post/Foreign Service users access to the admin features of the appointment system. EVAF shares data stored in the barcode created on the end-user printed DS-156 form with CA's NIV and RDS systems.

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

Once the applicant completes Form DS-156 and submits the data, the EVAF system will generate a PDF version with a barcode that contains selected applicant biographical data. The user then has a printable PDF version of the DS-156 Form with their data and barcode displayed on it. Once the visa applicant prints out this form, he may then present it at a visa unit at a US mission abroad to support his/her application for a visa. The information from the barcode will be scanned into the CA NIV or RDS system at post. Once the data is entered into the NIV system, an NIV applicant case is initiated. All connections between the applicant and the Department of State equipment is established with a Secure Sockets Layer (SSL) protocol,

This information is known only by the Internet based applicant user applicant and the risk associated with gaining access is minimal. User access is restricted only by the end user's ability to access the Internet and have the appropriate version of an

Internet browser that can support 128 bit encryption. Once an applicant has successfully scheduled an appointment, the EVAF system will generate and provide the user with a unique confirmation ID as a safeguard.

7. External Sharing and Disclosure

With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

No external organizations share information in the system.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

The information in this system is covered by STATE-39, Visa Records, which was last amended August 2, 1995, at 60 FR 39473-39474.

☐ does not constitute a system of records covered by the Privacy Act.

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

End-users accessing the EVAF web site will be presented with a certification statement that states:

I certify that I have read and understood all the questions set forth in this application and the answers I have furnished on this form are true and correct to the best of my knowledge and belief. I understand that any false or misleading statement may result in the permanent refusal of a visa or denial of entry into the United States.

Additionally, EVAF end users are presented with the Privacy and Computer Fraud and Abuse Acts Notice that identifies additional rules of behavior required of EVAF end users.

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

Yes, but they cannot apply for a visa without supplying this information.

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?

See (a) and (b) above.

9. Notification and Redress

What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

U.S. citizens making appointments may cancel their request and resubmit it.

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?

Authorized DoS users include the System Administrators, the Database Administrators and Web Administrators. All authorized users maintain a security clearance level at least commensurate with public trust positions. DoS users access lists are constantly updated and periodically reviewed for accuracy. Each prospective authorized user must sign a user access agreement. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes rules of behavior where the individual's responsibility to safeguard EVAF information is described.

EVAF is evaluated for security compliance to ensure that the deployment of an application does not effectively introduce any vulnerability into OpenNet. This is accomplished through the C&A process.

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

Access to the system is limited to authorize DoS employees who require access in order to perform their official duties. All authorized users maintain a security clearance level at least commensurate with public trust positions. To access EVAF, the staff member must first be an authorized user of the Department's unclassified computer network. Access to the network requires a unique user name and password assigned by Diplomatic Security. Apart from network access, the EVAF application requires a separate user account with unique user name and password. Each prospective authorized user must sign a user access agreement. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes rules of behavior where the individual's responsibility to safeguard EVAF information is described.

11. Technologies

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

No technologies commonly considered to elevate risk are employed.

12. Security

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

In accordance with FISMA provision for the certification of this system, EVAF received a full 36 months approval to operate (ATO) on 4/12/2006.