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: February 9, 2012

(b) Name of system: Electronic Visa Application Form

(c) System acronym: EVAF

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

(e) System description (Briefly describe scope, purpose, and major functions):

The Electronic Visa Application Form (EVAF) enables non-immigrant visa (NIV) applicants worldwide who have access to the internet to apply for a NIV online via the DS-156 form, "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 U.S, embassy or consulate ("post"). The post scans the barcode containing the applicant's information which is entered into the Bureau of Consular Affair's (CA) NIV system. EVAF also provides an online calendar that allows applicants applying for a non-immigrant visa to schedule their NIV interview online, in turn providing NIV applicants with a more efficient and effective service. U.S. citizens may also schedule appointments for American Citizen Services (ACS) services such as passport, Consular Report of Birth Abroad (CRBA), and notarial services using EVAF.

(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):

(h) Date of previous PIA (if applicable): August 29, 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.

The EVAF primarily collects and maintains information on foreign nationals as part of the U.S. nonimmigrant visa (NIV) application process. As such, the information provided by the NIV applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). Because the visa

applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the E-Government Act of 2002, OMB 03-22, and Privacy Act of 1974.

However, an NIV application may include personally identifiable information (PII) about persons associated with the nonimmigrant visa applicant who are U.S. citizens or legal permanent residents.

This PII on U.S. persons may include the following: U.S. sponsor's name, address and phone number; U.S. contact name, address and phone numbers; and employer name, address and phone numbers. The source of information is the visa applicant, petitions, and visa applications.

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

The elements of data of foreign nationals collected by EVAF for NIV applications are obtained directly from the Nonimmigrant Visa (NIV) applicants when they fill out the DS-156 form (note: EVAF does not store or maintain this data). Those elements are as follows:

- Passport number (foreign)
- Last name
- First and middle names
- Date of birth
- Home address
- Home telephone number
- Business telephone number
- Mobile/cell telephone number
- Email address
- Passport issuance (City, Country, State/Province)
- Passport issuing country
- Passport date of issuance
- Passport expiration date
- Alias (other) names
- Place of birth (city, country, state/province)
- Nationality
- Gender
- National ID (if applicable)
- Marital status
- Spouse's full name
- Spouse's DOB
- Name & address of present employer or school
- Occupation
- Address (in US)
- Name & telephone number of point of contact in US
- Who will pay for trip
- Persons traveling with you

The EVAF system includes both an NIV and American Citizen Services (ACS) appointment capability. The information required to schedule an NIV interview

appointment is provided directly by the applicant. Information collected from the applicant includes the following:

- Last name
- First Name
- Passport Number (foreign)
- Confirmation ID (only required to change or cancel an NIV appointment).

The information required of U.S. citizens to schedule an ACS services-related appointment is provided directly by the applicant. Information collected from the applicant includes the following:

- Last name
- First Name
- E-mail Address
- Contact Phone Number
- Date of Birth

b. How is the information collected?

The information for the NIV application is collected directly from the nonimmigrant visa applicant through a secure web form application. The applicant manually inputs his or her data onto the online DS-156 form, "Nonimmigrant Visa Application," via the EVAF website at http://evisaforms.state.gov/.

The applicant is able to print the DS-156 form 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.

This website can also be used by NIV applicants and U.S. citizens to schedule NIV and passport service appointments respectively. The applicant manually inputs his or her data into the online appointment form via the EVAF website at http://evisaforms.state.gov/.

c. Why is the information collected and maintained?

No visa application, visa appointment, or ACS services appointment information is retained by the EVAF website. The EVAF online form DS-156 allows NIV applicants to complete and print an NIV application without having to come to post to obtain the form. The unique electronic barcode assigned to each printed form allows a post to scan the form into the NIV system without having to do separate data entry, thus increasing the efficiency of the NIV application process for both the applicant and post.

Each element of PII indicated in Section 3(a) above collected on the online form DS-156 is collected because it is required to process an NIV application. It is needed to schedule an ACS appointment and is subsequently used for identity verification purposes.

d. How will the information be checked for accuracy?

Accuracy of the information on the NIV application is the responsibility of the applicant. 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 the DS-156 form.

The system also ensures that the data items entered on the 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 (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)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

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

The personal data collected by EVAF is the minimum necessary to carry out the function of EVAF as identified in Section 3(c) above.

Due to the strict security controls required by all Department of State systems before system operation commences, privacy risks are generally limited to three categories. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft are:

- **Device theft or loss.** Lost or stolen laptops and other devices such as removable drives may contain PII.
- **Portable devices.** PII is at the fingertips of every staff member who has email, database and Web access at work. The growing use of removable media such as USB drives, CDs/DVDs and portable MP3 players creates risk by making PII easily transportable on devices that aren’t always properly secured.
- **Insider threat.** Disgruntled employees seeking revenge or inadvertent human error to send PII over the internet.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety

- Civil or criminal violation

In accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST), there are management, operational, and technical security controls implemented to protect the data. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), training, and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

Information collected by EVAF on the DS-156 form is used to determine whether an NIV applicant qualifies for a non-immigrant visa. The information collected for NIV and ACS appointments is used to identify the applicant and may be used by personnel at post to contact the applicant if necessary prior to the appointment.

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

The information entered to the online NIV forms through the EVAF system is not retained online. The data is encoded into the bar code that is electronically imposed on the completed form once that form is completed and printed. The applicant then takes the form to post where the bar code is scanned to obtain the data encoded therein. When the barcode on the printed DS-156 form is scanned into the Remote Data Entry System (RDS) during the data entry process, applicant data is transferred from RDS to the NIV system. Further information about the NIV system is available in the NIV privacy impact assessment.

Authorized visa adjudicators review this information to determine the purpose of the travel, the identity of the applicant and whether he/she qualifies 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.

EVAF does not use commercial information, publicly available information, or information from other Federal agency databases.

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

EVAF is a government owned system. Contractors are involved with the design and development of the system. Direct hire U.S. government employees have the sole responsibility for adjudicating NIV applications to determine if applicants are entitled to non-immigrant visa issuance. 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.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

All users are screened prior to their employment with the Department of State. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before they are given access to the authenticating OpenNet (the Department of State intranet) users and any CA/CST system, including EVAF, are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

Consular post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard PII from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites for the proper disposal of paper that contains PII.

5. Retention

a. How long is information retained?

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

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 EVAF throughout the lifetime of the data. The information is only retained for the amount of time that is required to perform the system's purpose.

All physical records containing PII are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. 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?

EVAF will share information with the Consular Consolidated Database (CCD) for the purpose of authenticating OpenNet (the Department of State intranet) users and allowing Post/Foreign Service users access to the administrative features of the appointment system. End-user appointment information is also replicated from EVAF to CCD. EVAF shares data stored in the barcode created on the printable PDF version of the DS-156 form with the NIV and Remote Data Entry System (RDS) systems.

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

Once the applicant completes the DS-156 form 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 his/her data and barcode displayed on it. Once the visa applicant prints out this form, he/she may then present it at a visa unit at a U.S. mission abroad to support his/her application for a visa. The information from the barcode will be scanned into the CA NIV via the RDS system at post.

Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Security Officers determine the access level an application user (including managers) may require depending on the user's particular job function and level of clearance. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted by EVAF.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Access to electronic files is protected by passwords, and is under the supervision of system managers. 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 is 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, numerous management, operational and technical controls are 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?

No information from EVAF is shared with external organizations.

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

No information from EVAF is shared outside the Department.

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

No information from EVAF is shared with external organizations.

8. Notice

The system:

☒ contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records:
- Visa Records. STATE-39

☐ does NOT contain information covered by the Privacy Act.

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

The information provided by the nonimmigrant visa applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

End-users accessing the non-immigrant visa application form are provided a statement that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

Also, notice is provided in the System of Records Notice (SORN) Visa Records, State-39.

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

Yes, but failure to supply the requested information may result in the denial of the NIV application.

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?

Applicants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

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.

Notice is given to individuals as described in Section 8(a) above. The notice offered to individuals is reasonable and adequate in relation to the purpose and uses of EVAF. The information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). The information provided on the online forms accessible through EVAF and in the SORN regarding visa records fully explains how the information may be used by the Department and how it is protected.

EVAF DS-156 application data is not accessible by the applicant (once submitted). Access to the appointment information in EVAF is restricted to cleared, authorized Department of State direct hires and contractor personnel. EVAF enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

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?

U.S. citizens who have scheduled an appointment for an ACS service can cancel their appointment. The EVAF system will grant an applicant access to cancel an appointment for an ACS service based on his/her surname, given name, contact telephone number and a system generated password. The applicant can submit a new appointment request to (re)schedule a new appointment for an ACS service.

Applicants who have scheduled an NIV appointment can change or cancel their appointment. The EVAF system will grant the applicant access to change or cancel an NIV appointment based on his/her surname, given name, and appointment confirmation number. Applicants do not have the ability to change any appointment data other than the date and time.

Visa applicants completing an online application (DS-156 application form) may change their information at any time prior to submission of the application in the EVAF system. Once the application data is submitted in the system, the applicant must print the confirmation page with barcode number and hand-carry the printed confirmation page to the Consulate or Embassy. Once that is done, an applicant may make changes only by filing a new application with the Department or providing the correct information during the course of a visa interview. The Department will release the following information to a visa applicant upon request, and this guidance is available to the public in 9 FAM 40.4:

(1) Correspondence previously sent to or given to the applicant by the post;

(2) Civil documents presented by the applicant; and

(3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

NIV information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about

the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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

To the extent information in EVAF may be Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore, this category of privacy risk is appropriately mitigated in EVAF.

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?

Internal access to EVAF is limited to authorized Department of State users, including contractors that have a justified need for the information in order to perform official duties. To access the system, a user must be an authorized user of the Department of State's unclassified network. Access to the EVAF administrative module requires a unique user account assigned by a supervisor, as well as a CCD logon. Users access the EVAF admin module via the CCD portal. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. 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 level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users in the EVAF appointment module is monitored, logged, and audited as needed to address support tickets.

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

Internal access to the system is limited to authorized Department employees who require access in order to perform their official duties. All authorized users must pass computer cyber security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain access.

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.

Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.)

11. Technologies

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

EVAF does not employ any technology known to elevate 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 EVAF does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum satisfactory in this application.

12. Security

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

The Department operates EVAF in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department will conduct a risk assessment of the system to identify appropriate security controls to protect against risk. The Department will perform routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, EVAF was certified and accredited for 36 months to expire on February 29, 2012. It is anticipated that the current C&A process will be completed by March 2012 resulting in a projected authorization to operate (ATO) date of March 2015.