PRIVACY IMPACT ASSESSMENT

Enterprise Visa Application Forms (EVAF)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: 4/21/2021
(b) Name of system: Enterprise Visa Application Forms
(c) System acronym: EVAF
(d) Bureau: CA/CST
(e) iMatrix Asset ID Number: 723
(f) Child systems (if applicable) iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?

☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?

☒Yes
☐No

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

(c) Describe the purpose of the system:

EVAF provides for online scheduling of an in-person visa or passport appointment for both American Citizen Services (ACS) and Non-Immigrant Visa (NIV) at posts. EVAF is a public-facing application (with internal non-public administrative components) for scheduling. The NIV and ACS services are separate components outside the boundary of EVAF.

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

The information provided by the non-U.S. citizen applicant is considered a visa record subject to the confidentiality provisions of section 222(f) of the Immigration and Nationality Act (INA). Because visa applicants themselves are not U.S. persons (that is, U.S. citizens or lawful permanent residents (LPRs)), they are not covered by the provisions of the Privacy Act of 1974 and the E-Government Act of 2002. However, the visa portion of records may include PII about U.S. persons associated with the applicant.

Foreign Nationals: Surname, given name, passport number, email address, and telephone number.

U.S. Citizens: Surname, given name, date of birth, telephone number, and email address. In addition, country of citizenship, country of birth, gender and passport number are also collected for ACS appointments related to notarial appointments. Visa applicant can also include U.S. citizen information regarding their relationship to applicant and if the U.S. citizen is associated with an organization.

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

- 8 U.S.C. 1101 et seq., Immigration and Nationality Act of 1952, as amended, including 8 U.S.C. 1104 Powers and duties of Secretary of State and 8 U.S.C. 1185, Travel Documentation of Aliens and Citizens
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 2651a (Organization of the Department of State)
- 22 U.S.C. 3904 (Functions of Service)
- Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 22 C.F.R. Parts 50-51 (Nationality Procedures and Passports)
- Omnibus Consolidated Appropriations Act, 1997, PL 104-208, September 30, 1996
- Illegal Immigration Reform and Immigration Responsibility Act, PL 104-208, Div. C, September 30, 1996
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107–56, October 26, 2001
- Enhanced Border Security and Visa Entry Reform Act of 2002 , PL 107-174, May 14, 2002

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

☒Yes, provide:

- **SORN Name and Number**: Visa Records; STATE-39
  SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018

- **SORN Name and Number**: Passport Records; STATE-26
  SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): March 24, 2015

- **SORN Name and Number**: Overseas Citizens Records and other Overseas Records; STATE-05
  SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): September 8, 2016

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

Schedule number: **A-13-001-23**
Title: Passport Records
Disposition Authority Number: N1-059-98-03, item 1
Length of time the information is retained in the system: Destroy/delete when 25 days old.
Type of information retained in the system: Email messages regarding the status of passport applications and requests for expedited service.

Schedule number: **A-15-001-02**
Title: Overseas American Citizens Services Records
Disposition Authority Number: N1-059-09-40, item 1
Length of time the information is retained in the system: Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is

later. NOTE: ACS case records are replicated to the Consular Consolidated Database each day for long-term recordkeeping.
Type of information retained in the system: The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. Record level data includes: biographic information, case information, and case activity log.

Schedule number: **B-09-002-09a**
Title: Non-Immigrant Visas- Issuance
Disposition Authority Number: N1-084-09-02, item 9a
Length of time the information is retained in the system: TEMPORARY. Cutoff at end of calendar year when issued. Destroy 25 years after cutoff or when no longer needed, whichever is sooner.
Type of information retained in the system: The NIV system is an electronic case management application designed to track and manage the actions taken during the non-immigrant visa application and adjudication process at overseas posts. NIV maintains non-immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic non-immigrant visa case records are maintained in the Consular Consolidated Database.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☐ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

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

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

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

- If yes, under what authorization?

(d) How is the PII collected?

The information is collected from applicants using the public facing EVAF webpage to make appointments for ACS services or NIV interview appointments by clicking on the links for the desired appointment.

After the appointment and applicant information is entered, the applicant clicks a button in EVAF to submit the appointment request. For U.S. citizens, once the appointment information is provided, they receive a confirmation page from the appointment and scheduling service and an appointment password in case they require modification or cancellation. For non-U.S. citizens, when the applicant clicks the button in EVAF to submit the request, EVAF calls a function in the Consular Electronic Application Center (CEAC) system to verify that the NIV appointment record is valid and that it exists in CEAC. If the EVAF appointment record is valid, the NIV applicant receives a computer generated appointment confirmation. If it is not valid, EVAF will display an error indicating the data entered for the appointment do not match the data entered in the CEAC record and prevents the applicant from successfully submitting the NIV request.

(e) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.

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

Accuracy of the information provided on the forms is the responsibility of the applicant. Applicant information provided for the appointment is checked against information in the CEAC records for NIV applicant information accuracy and is also vetted during the applicant's appointment. If it is not valid, EVAF will display an error indicating the data entered for the appointment do not match the data entered in the CEAC record and prevents the applicant from successfully submitting the NIV. NIV and ACS information can also be verified for accuracy during the interview process for the services requested.

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

The applicant is responsible for ensuring current data are entered into the public facing component of EVAF when scheduling appointments. ACS applicants can also update information by using the original appointment confirmation password provided to modify or update information in EVAF. NIV applicants can update information any time by accessing EVAF and providing their appointment information and the confirmation ID generated when the appointment was first made. In addition NIV and ACS applicant information is verified for currency during the interview process.

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

publicly available?

EVAF does not use commercial information or publicly available information.

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

The PII listed in 3d are the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended-to schedule NIV and ACS appointment requests.

5. Use of information

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

The intended use for the information in 3d is for contacting applicants to schedule appointments for the requested services and for validating the applicant's information. In addition, NIV appointment information is used to verify that the NIV appointment record is valid per the CEAC system.

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

Yes, the PII is used for scheduling and verifying appointment and applicant information.

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

If yes:

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

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(d) If the system will use test data, will it include real PII? ☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

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

With that understanding, information in EVAF will be shared internally with other CA systems: Consular Electronic Application Center (CEAC), Consular Consolidated Database (CCD), and the Non-Immigrant Visa (NIV) system and American Citizen Services (ACS) system which are both part of the Overseas Consular Support Systems (OCSA) Logical Business Group.

External: EVAF does not share information externally.

(b) What information will be shared?

Internal: Information in 3d will be shared.

External: N/A

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

Internal: The information is shared for verification against other CA databases, for data storage purposes, and to assist in scheduling both American Citizen Services (ACS) and Non-Immigrant Visa (NIV) appointments at posts.

EVAF shares NIV applicant information with CEAC to schedule and verify appointment information. Information is shared with ACS to schedule appointments to provide U.S. citizens required services. EVAF data are shared and replicated in CCD. EVAF also uses the CCD system to authenticate the unique Department of State (DoS) user ID and password with associated roles. CEAC, NIV, ACS and CCD systems are not a part of the EVAF boundary.

External: N/A

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

Internal: The connection between OpenNet and the EVAF servers is currently deployed and protected using Transport Layer Security (TLS) 1.2 for encrypting data between the client servers. EVAF also uses the secure protocol connections (Hypertext Transfer Protocol (HTTP)) which provides secure encryption interface with the CCD,

CEAC, ACS and NIV systems. The information is shared using Department of State approved information system connection ports, protocols and services.

External: N/A

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

Internal: EVAF uses the secure protocol connections (HTTP) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior required by security controls for each major application, including EVAF. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In addition, DoS employees must have a Verification/Personal Identification Number (PIV/PIN), as well as a separate unique user ID and password to access EVAF data. Data are transmitted within DoS database to database.

External: N/A

7. Redress and Notification

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

EVAF provides a Privacy Act statement on the public facing module of the EVAF system. A confidentiality statement is also included on the NIV component of the public facing module of the EVAF system. The EVAF system requires users to select a box confirming that he/she has read the Privacy Act statement in order to proceed with scheduling an appointment through the EVAF system.

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

☒Yes ☐No

If yes, how do record subjects grant consent?

The system requires users to select a box confirming that he/she has read the Privacy Act statement in order to proceed with scheduling an appointment for ACS or NIV. Individuals may decline to enter the information; however, if the mandatory fields are not filled in, the individual may not receive the requested appointment.

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

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

The applicant can access their information by using the confirmation password (U.S. citizens) or ID (non-citizens) provided at the time the appointment was made to access

their information. Applicants can contact his/her Department of State representative with whom he/she had an interview/appointment as well as follow the instructions in the published SORNs STATE-39, STATE-26, and STATE-05. The applicant can also contact the overseas consulate where the applicant plans to have an appointment regarding their information.

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

☒Yes ☐No

If yes, explain the procedures.

1. Once an applicant completes the appointment online, they are assigned a password or ID where they can go into the system and cancel an appointment and resubmit it with corrected information.
2. The data provided by the applicant can also be corrected during the interview process.

If no, explain why not.

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

Individuals are notified of the procedures to correct records in these systems by a variety of methods:

1. During their interview.
2. Instructions on application forms and web pages (or link to instructions).
3. Being notified by letter that a correction is needed.

Each method contains information on how to amend records and contact information.

8. Security Controls

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

EVAF is secured through the use of defense in depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

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

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).
General public users, DoS EVAF users, system administrators, and database administrators have access to data in the system based on their prescribed roles and duties.

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

General Public Users: Applicants requesting appointments have public access via EVAF to sign up for NIV and ACS appointments. Applicants can only see their information in EVAF while scheduling appointments.

For DoS EVAF, System, and Database Administrator users: Separation of duties and least privilege access are employed; users have access to only the data that the supervisor and local Information System Security Officers (ISSOs) approve to perform official duties. Access is role-based and the user is granted only the role(s) required to perform officially assigned duties to schedule NIV and ACS appointments via EVAF.

Least Privileges are restrictive rights/privileges or accesses users need for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties. Users are uniquely identified and authenticated before accessing PII.

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

Access to information is role based. The following applies:

- **General Public Users:** Users access EVAF for ACS and NIV appointments via the internet public facing pages on the Travel.State.Gov site. The general public users only have access to their information during completion of the application.

<u>DoS Internal EVAF users:</u>

- **DoS EVAF User:** Department of State personnel accessing EVAF consist of DoS post users and local hires. These users can view data, but there are restrictions as to what data each user can access. Post users are mostly limited to viewing the data for their own post.
- **System Administrators:** Include both government and contract personnel. System administrators are responsible for the daily maintenance, establishing access control lists (ACLs) and backups. The local information system security officer (ISSO) based on supervisor approval authorizes the establishment, activation, modification and disabling of EVAF system administrator accounts. System administrators have access to all data.

- **Database Administrators:** Database Administrators (DBA) are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configuration to the database. DBAs have access to application files necessary to perform daily activities to manage the databases. They can see all of the information in EVAF, but are limited to the specific roles listed above, as granted. The local ISSO is responsible for reviewing and approving DBA accounts.

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

The CA system manager and CA ISSO, in conjunction with CA security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Access control lists on OpenNet servers and devices along with Department of State Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures.

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

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

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

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

☒Yes ☐No

The EVAF System Security Plan (SSP) provides procedures and controls regarding access to data in the system.

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

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component.

PA318 Protecting Personally Identifiable Information is a mandatory biennial course required for all DoS personnel and contractors accessing DoS computers.