PRIVACY IMPACT ASSESSMENT

Enterprise Visa Application Forms (EVAF)

1. Contact Information

<table>
<thead>
<tr>
<th>A/GIS Deputy Assistant Secretary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bureau of Administration</td>
</tr>
<tr>
<td>Global Information Services</td>
</tr>
</tbody>
</table>

2. System Information

(a) Name of system: Enterprise Visa Application Forms
(b) Bureau: Consular Affairs (CA)
(c) System acronym: EVAF
(d) iMatrix Asset ID Number: 723
(e) Reason for performing PIA:
   ☒ New system (as a consolidated boundary)
   □ Significant modification to an existing system
   □ To update existing PIA for a triennial security reauthorization
(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
   ☒Yes
   □No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
   This system is undergoing a reauthorization in order to receive an Authorization to Operate (ATO) by May 2018.

(c) Describe the purpose of the system:

   EVAF was developed to provide the following service for foreign nationals and U.S. citizens:

   The ability to schedule both American Citizen Services (ACS) and Non-Immigrant Visa (NIV) appointments at posts which are not serviced by a Global Support Strategy (GSS) provider. EVAF is a public-facing application (with internal non-public administrative components). The EVAF public-facing application allows applicants to schedule appointments for NIV and ACS services, which are separate components outside the boundary of EVAF. After the appointment and applicant
information is entered, the applicant clicks a button in EVAF to submit the appointment request. 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 appointment record is valid and that it exists in CEAC. If the EVAF appointment record is valid, the applicant receives a computer generated appointment confirmation. If it is not valid, EVAF will display an error indicating the data entered for the appointment does not match the data entered in the CEAC record and prevents the applicant from successfully submitting the NIV or ACS requests.

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

The information provided by the visa 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 persons associated with the visa U.S. sponsor/petitioner.

Foreign Nationals: DS-160 barcode number, surname, given name, passport number, email address, and telephone number when scheduling an NIV appointment.

U.S. Citizens: The surname, given name, date of birth, telephone number, and email address from U.S. citizens when scheduling an ACS appointment. In addition, country of citizenship, country of birth, gender and passport number are also collected for ACS appointments related to notarial appointments.

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

- 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. 211a-218, 2705; Passports and Consular Reports of Birth Abroad of a U.S. Citizen
- 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)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
(f) **Is the information searchable by a personal identifier (e.g., name or Social Security number)?**

☒ Yes, provide:
- State-39, Visa Records; October 25, 2012
- State-26, Passport Records; March 24, 2015
- State-05, Overseas Citizens Service Records and Other Overseas Records, September 8, 2016

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

(g) **Do the existing SORNs need to be amended to reflect the inclusion of this new or significantly modified system?**

☐ Yes  ☒ No

If yes, please notify the Privacy Division 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:

- Schedule number (e.g., (XX-587-XX-XXX)):
  
  A-13-001-23 - Passport Records: Routine Passport Application Status Check and Expedite Fee Upgrades E-mail
  Description: Email messages regarding the status of passport applications and requests for expedited service.
  Disposition Temporary: Destroy/delete when 25 days old
  DispAuthNo: N1-059-98-03, item 1

  A-15-001-02 Overseas American Citizens Services Records
  Description: 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. ACS supports domestic consular operations and consular activities at overseas Posts.
  **Disposition:** Overseas American citizen service records are retained from 6 months up to 30 years, depending on the type of record.

  B-09-002-04a Non-Immigrant Visas – Issuances
Description: Information obtained from issued non-immigrant visa application forms (DS-156, 157, 158, 160 and related forms) and supporting documentation. Nonimmigrant visa case records potentially include the following types of case level data: unique identifier; applicant personal and biographic data; passport data; adjudication data; visa class information; foil history; case summary data; case status data; and notes.

Disposition: Temporary. Cutoff at end of calendar year when issued. Destroy 25 years after issuance.

- Length of time the information is retained in the system:
  Retention depends on the type of record in the above listed schedules. Specific information may be obtained from: http://infoaccess.state.gov/recordsmgmt/recdipsched.asp.

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 (are US citizens or aliens lawfully admitted for permanent residence)
☐ U.S. Government/Federal employees or Contractor employees
☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐ Yes
☒ No --- None of these systems collect SSNs

- If yes, under what authorization?

(c) How is the information collected?

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

(d) 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.
(e) **What process is used to determine if the information is accurate?**

Accuracy of the information entered on appointment requests is the responsibility of the applicant. The information is verified during the applicant’s appointment.

(f) **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 is entered into the public facing module of EVAF when scheduling an ACS or NIV appointment. If the applicant is scheduling an appointment for ACS services, he/she will enter his/her name, phone number, and email address. If the applicant is scheduling an appointment for ACS notarial services, he/she will also enter passport number, country of citizenship, country of birth, and gender. If the applicant is scheduling an appointment for a NIV interview he/she will also enter his/her DS-160 barcode number, in addition to name, passport number, phone number, and email address. During the interview, the data will be verified. (The ACS and NIV systems are outside of this boundary).

(g) **Does the system use information from commercial sources? Is the information publicly available?**

These systems do not use commercial information, publicly available information, or information from other Federal agency databases.

(h) **Is notice provided to the individual prior to the collection of his or her information?**

EVAF 4.1A release has been implemented to incorporate a Privacy Act Statement on both the ACS and NIV components of the public facing module of the EVAF system. The release includes a change to incorporate a Confidentiality Statement on the NIV component of the public facing module of the EVAF system. 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.

(i) **Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?** Yes ☒ No ☐

- If yes, how do individuals grant consent? (Security Control: IP-1)

   Applicants grant consent by clicking on the complete appointment box and submission of the information scheduling the desired NIV or ACS appointment.
EVAF

-If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII items listed in Question 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 stages. 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.

5. Use of information

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

This information is used to enable applicants to schedule ACS and NIV appointments.

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

Yes. The PII information is used according to the EVAF system’s purpose in order to schedule NIV and ACS appointments.

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

The EVAF system does not analyze information.

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

(2) Does the analysis result in new information? ☐Yes ☒No

(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

6. Sharing of Information

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

EVAF interfaces with Consular Electronic Application Center (CEAC) to check and verify the DS-160 Barcode. EVAF also interfaces with the Consular Consolidated Database (CCD) EVAF Schema. EVAF does not share externally.

(b) What information will be shared?
Applicant’s name, birthdate, phone and email address are shared. If the applicant is scheduling an EVAF ACS appointment for a notarial service: applicant’s passport number, gender, country of birth and country of citizenship is also collected and stored/shared internally.

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

The information is shared for data storage purposes as well as DS-160 Barcode Verification to assist in scheduling both American Citizen Services (ACS) and Non-Immigrant Visa (NIV) appointments at posts which are not serviced by a Global Support Strategy (GSS) provider. The barcode created on the end-user’s application form contains biographical and limited visa information to validate the identity of the applicant. The user has a printable PDF version of the form with their data and barcode information displayed on it. Once printed out they can present it at the Visa unit where the bar code is scanned to acquire services or use the barcode information to log into EVAF to change appointments. The validation of the barcode prevents users from making appointments and selling it to the valid applicant who needs appointment.

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

Information is transmitted using Department of State approved Information System Connection Ports, Protocols, and Services.

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

Internal sharing requires a connection agreement and OpenNet users with privileged role based access to manage the connection. Communications is secured using transport level security.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to non-authorized parties
b. Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other.

Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, “Sensitive but Unclassified”, and all higher levels of classification, and signing a user agreement.
- Strict access control based on roles and responsibilities, authorization and need-to-know.

- System authorization and accreditation process along with continuous monitoring. Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared internally are encrypted as per the Department of State’s Security Configuration Guides’ security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The applicant may contact his/her Department of State representative with whom he/she had an interview/appointment as well as follow the instructions in the Agency Privacy Policy posted on the Department of State Website, or follow the directions in the published SORN.

(b) Are procedures in place to allow an individual 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 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.

(c) By what means are individuals 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. Published SORNs.
3. Department of State Privacy Act Website (or link to it on application page).
4. Instructions on application forms and web pages (or link to instructions).
5. Being notified by letter that a correction is needed.

Each method contains information on how to amend records and who/what office to communicate with as well as contact information.

8. Security Controls

(a) How is the information in the system secured?
The system is secured within the Department of State intranet where risk factors are mitigated 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.

Access to applications is controlled at the application level; there are additional access controls at the database level. All accounts for the system must be approved by the user’s supervisor and the Information System Security Officer. The audit vault system is used to monitor all privileged access to the system and violations are reported to senior management daily, if applicable.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards & Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

To access the system, persons must be authorized users of the Department of State’s unclassified network, which requires a background investigation and an application approved by the supervisor and Information System Security Officer (ISSO). Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and (Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based and restricted according to approved job responsibilities and requires managerial concurrence. 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.

(c) What monitoring, recording, and auditing safeguards 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 and conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and Federal security policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA’s major and minor applications for changes to the Department of State mandated security controls.
The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities. 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.

Operating System (OS)-Level auditing is set in accordance with the Department of State Security Configuration Guide. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory annual security/privacy training is required for all authorized users including security training and regular refresher training. Each user must annually complete the Cyber Security Awareness Training and pass the PA-459 course, entitled Protecting Personally Identifiable Information. The Department’s standard “Rules of Behavior” regarding the use of any computer system and the data it contains require that users sign their agreement to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.
(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems requires dual factor authentication utilizing the personal identity verification/common access card (PIV/CAC) and personal identification number (PIN).

(f) How were the security measures above influenced by the type of information collected?

The security measures listed above were implemented to avoid the potentially adverse consequences to organizations or individuals whose PII has been breached or exposed to unauthorized users, which may include 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, and/or civil or criminal violations.

9. Data Access

(a) Who has access to data in the system?

Database Administrators, System Administrators, and EVAF users have access to the data in the system.

(b) How is access to data in the system determined?

Access is determined based on requests which are approved by the supervisor. Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Information is documented in the System Security Plan. The Plan includes information regarding system access to data.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Users other than administrators will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.
(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

- Access control policies and access enforcement mechanisms control access to PII.

- Separation of duties is implemented.

- 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 (CAC/PIV and PIN).