PRIVACY IMPACT ASSESSMENT

IMMIGRANT VISA INFORMATION SYSTEM (IVIS)

2. System Information

(a) Date of completion of this PIA: January 2021

(b) Name of system: Immigrant Visa Information System (IVIS)

(c) System acronym: IVIS

(d) Bureau: Consular Affairs (CA)

(e) iMatrix Asset ID Number: 49

(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:

The Department of State is responsible for issuing Immigrant Visas (IVs) at embassies and consulates overseas. The purpose of IVIS is to assist the National Visa Center (NVC) in tracking and processing immigration visa petitions based on local necessities and requirements established by the State Department.

The Department of Homeland Security (DHS) United States Citizenship and Immigration Service (USCIS) reviews and adjudicates the petitions and forwards approved petitions to the NVC for processing. Using IVIS, NVC performs visa processing activities that track petitions from initial NVC receipt (from the USCIS) to notification to the petitioner of the case being forwarded to post.

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

IVIS collects the following information on U.S. citizens:

- Name(s)
- Personal address
- Email address(es)
- Business address
- Business number
- Home phone number
- Financial and income information (for Joint Sponsors)

IVIS collects the following information on Non-citizens/non-LPRs:

- Name(s)
- Personal address
- E-mail address(es)
- Phone number(s)
- Date and place of birth
- Gender
- Race
- Marital status
- Mother's maiden name
- Alien number
- Social Security Number (SSN)
- Nationality
- Occupation
- Education
- Passport or Other ID Numbers
- Tax Identification Number (TIN)
- Substantive medical information
- Substantive legal information
- Arrests and convictions
- Substantive family information
- Organization name/Business address/Information

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

- 8 U.S.C. §§ 1151-1363a (Title II of the Immigration and Nationality Act of 1952, as amended);
- 8 C.F.R. § 245.1(a) (Title 8, Aliens and Nationality), Sec 245.1(a) Eligibility

- 8 U.S.C. § 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C. § 2651a (Organization of the Department of State);
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 26 U.S.C. § 6039E (Information Concerning Resident Status)
- Immigration Act of 1990, PL 101-649, November 29, 1990 (an Act to amend the Immigration and Nationality Act of 1952)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996, PL 104-208, Div. C, September 30, 1996
- Omnibus Consolidated Appropriations Act, 1997, PL 104-208, 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
- Child Status Protection Act of 2002, PL 107–208, August 6, 2002 (an Act to amend the Immigration and Nationality Act of 1952)
- Anti-Drug Abuse Act of 1988, PL 100–690, November 18, 1988

(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

☐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-14-001-01 thru A-14-001-25, Visa Records and B-09-002-18a thru 18f, Visa Petitions
- Disposition Authority Number: NC1-059-7913 thru N1-059-97-10

- Length of time the information is retained in the system: Records in these systems are retained on an average of one to twenty years or when it is determined that they are longer needed.
- Type of information retained in the system:
  Visa Records may include information regarding the following individuals when required by a visa application: U.S. petitioners and U.S. persons (Legal Permanent Residents) applying for returning resident travel documentation.

  Visa records and visa petition records maintain visa applications and related forms; biometric information; photographs; birth, marriage, death and divorce certificates; documents of identity; interview worksheets; biographic information sheets; affidavits of relationship; medical examinations and immunization reports; police records; educational and employment records; petitions for immigrant status and nonimmigrant status; bank statements; communications between the Visa Office, the National Visa Center, the Kentucky Consular Center, U.S. embassies, U.S. consulates general and U.S. consulates, other U.S. government agencies, international organizations, members of Congress, legal and other representatives of visa petitioners, relatives of visa petitioners, and other interested parties where such communications are, or may be, relevant to visa adjudication; and internal Department of State correspondence and notes relating to visa adjudication and petitions. Visa Records may also contain information collected regarding petitioners' U.S. family members; U.S. employers; other U.S. persons referenced by the petitioner.

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?

26 USC§ 6039E – Information Concerning Resident Status
8 USC§§1101-1503 Title II of the Immigration and Nationality Act of 1952, as amended

(d) How is the PII collected?

The information is provided by petitioners who submit immigration petitions to USCIS via paper form. USCIS reviews and adjudicates the petition and forwards the approved petitions (in paper and electronic form) to the State Department National Visa Center (NVC) located in Portsmouth, NH for visa processing, which are scanned into IVIS.

Some of the petitioner's data are transferred electronically to IVIS via the DHS/USCIS DataShare application, which provides high performance secure connectivity between the State Department and Department of Homeland Security (DHS) to support the exchange of visa data. A third party source of additional information is the commercial bank under State Department contract. A text file from the commercial bank with case numbers is used to track the payments from the petitioners.

The following forms are used during the petitioner process: I-129 (Petition for a Nonimmigrant Worker); I-130 (Petition for Alien Relative); I-360 (Petition for American, Widow(er) or Special Immigrant); I-140 (Immigrant Petition for Alien Worker); I-526 (Petition for Alien Entrepreneur); I-600/I-600A (Petition to Classify Orphan as an Immediate Relative); I-730 (Refugee/Asylee Relative Petition); I-800/800A (Petition to Classify Convention Adoptee as an Immediate Relative); I-824 (Application for Action on an Approved Application or Petition); or I-929 (Petition for Qualifying Family Member of a U-1 Nonimmigrant); AR-11 (Alien's Change of Address Card, outside of the Department of State); DS-1884 (Petition to Classify Special Immigrant as an Employee or Former Employee of the U.S. Government Abroad); :DS-260 (Online Immigrant Visa and Alien Registration Application); and DS-261 (Online Choice of Address and Agent).

(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?

There are two main accuracy checks for IVIS: (1) IVIS has built-in functionality to validate and check the data against information in the database that is being entered, and (2) Visa Processing Specialists review petitions to ensure all required data are provided and match data sent by USCIS; for example, the date of birth is compared with the birth certificate.

Information is also checked by the DoS Visa processing specialists against information in the other CA systems; Consular Electronic Application Center (CEAC), Consular

Consolidated Database (CCD), Pre-Immigrant Visa Overseas Technology (PIVOT) and Electronic Document Processing (eDP) to track and process visas.

A letter is sent to petitioners requesting any inaccurate or missing data to be provided during the review process.

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

Visa Processing Specialists can pull up petitioner and attorney/agent information on their screen to review and validate the data. They also compare the data on the actual paper form with the data received from DHS/USCIS electronically.

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

Petitioners' payment information is produced and provided by the U.S. Bank and provided in electronic form to IVIS. No information is publicly available.

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

The PII elements collected by IVIS 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 IVIS to perform the functions for which it is intended, which is to track the processing of immigration visa petitions.

5. Use of information

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

The intended use of the PII is to assist the NVC in validating information received from DHS/USCIS, to track cases throughout the NVC process, and to process the immigration visa petitions based on requirements established by the State Department.

(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. IVIS processes information for the State Department's Immigrant Visas to effectively track the status and processing of immigration visa petitions.

(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?

IVIS compare and contrast methods are used to analyze the information used to track petitions. The analysis results in numerous reports, case status updates (current, non-current, ready for next action), and initiates communications to case beneficiaries (welcome packets, letters requesting additional information, etc.).

(2) Does the analysis result in new information?

Yes. Case-related tables will be updated, case notes may be placed on a case if appropriate, and dates of actions taken will be recorded on the case history

(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 (CA) 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 the IVIS system will be shared internally with other CA systems CEAC, CCD, Pre-Immigrant Visa Overseas Technology (PIVOT) and Electronic Document Processing (eDP) to track and process visas. Information is shared between CEAC and IVIS to assist in tracking petitions. The DS-260, (Online Immigrant Visa and Alien Registration Application); DS-261, (Online Choice of Address and Agent) and DS-1884 (Petition to Classify Special Immigrant as an Employee or Former Employee of the U.S. Government Abroad) are completed and submitted via Consular Electronic Application Center (CEAC) system (which is not within the boundary of this system's PIA).

External: There is no external sharing of information.

(b) What information will be shared?

Information listed in paragraph 3(d) will be shared in all cases.

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

Information is shared among CA/CST systems to acquire the status of visas in process and to generate required reports for IVIS end users to perform their duties.

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

IVIS information shared among CA/CST systems is via database to database. IVIS information is shared by the CCD or via text files emailed to posts visa offices.

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

Safeguards in place for internal sharing arrangements include secure transmission methods (Data encryption using Secure Socket Layer/Transport Layer Security cryptographic keys, certificates, Hash Authentication, multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers, hand-shaking, header checks) permitted by internal State Department policy for the handling and transmission of sensitive but unclassified (SBU) information.

7. Redress and Notification

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

IVIS does not collect information directly from petitioners. IVIS obtains information from other internal CA systems and external sources addressed in paragraph 6(a) or by contact with NVC directly. The source systems and applicable forms provide appropriate notice to petitioners.

(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?

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

IVIS does not collect information directly from petitioners. IVIS obtains information from other internal CA systems and external sources addressed in paragraph 6(a) or by contact with NVC directly. The source systems and applicable forms provide appropriate notice to petitioners regarding consequences of not providing required PII. They also have the option of not completing information via the source systems and or processes above.

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

Petitioners cannot gain access to the information stored in IVIS, however they can review the PII text data associated with their visa applications via CEAC, which is external to IVIS. They can also follow instructions for access to their information as stated in SORN STATE-39, Visa Records.

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

☒Yes ☐No

If yes, explain the procedures.

Petitioners do not have access to IVIS. However, they can correct inaccurate or erroneous information regarding visa applications in general from the system that originally collected information. They may also contact the National Visa Center (NVC) to update or amend collected information.

If no, explain why not.

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

Petitioners are notified when services are being requested in person at the NVC and via the source systems in which they submit their application for visa services. Information is provided at that time on how to correct information in that specific system.

8. Security Controls

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

IVIS 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 IVIS is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily. Data shared with DHS/USCIS are carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency.

IVIS is configured according the State Department Bureau of Diplomatic Security Configuration Guides to optimize security while still providing functionality (complies 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 in place and are 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).

Access to IVIS is role-based and the user is granted only the role(s) required to perform officially assigned duties. There are three types of IVIS user roles: IVIS Department of State users (Department of State employees and contractors), System/Security Administrators, and Database Administrators.

(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.

Separation of duties and least privilege is employed and 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.

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

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

IVIS Users - IVIS users track and process immigrant visas. User access controls determine how, when, and where IVIS users will gain access to the system. The IVIS users perform visa-processing activities that track petitioners requesting immigration services from the initial NVC receipt from USCIS through final disposition to the Posts.

System/Security Administrator - System/Security Administrator are responsible for all of the daily maintenance, establish access control lists (ACLs). Since the duties of system administrators require that they be granted full access, the concept of separation of duties is specifically applied. System/Security administrators have logon identifications associated with their name that allows for user auditing.

Database Administrators - Database Administrators are responsible for updating reference tables within the IVIS application. Responsibilities include daily maintenance, upgrades, patches, backups and database configuration. The access of database administrators is limited to only those database application files necessary to perform daily activities. The limited access is controlled through the use of ACLs. Administrators have logon identifications associated with their name that allows for user auditing.

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

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also 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.

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

The IVIS System Security Plan includes information and procedures regarding access to data in IVIS.

(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, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially. The State Department’s standard “Rules of Behavior” regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.