Immigrant Visa Overseas (IVO)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: October 2021
(b) Name of System: Immigrant Visa Overseas (IVO)
(c) System acronym: IVO
(d) Bureau: Consular Affairs (CA/CST)
(e) iMatrix Asset ID Number: 817
(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 Immigrant Visa Overseas (IVO) system provides automated support to the adjudication of an immigrant or diversity immigrant visa application from individuals wishing to come to the United States with the intent to establish permanent residence. IVO provides for the administration of federal law and regulations that govern the

issuance or refusal of either visa type and is a case record and maintenance application used at overseas posts to review and complete the visa adjudication. IVO's main processes are: 1) immigrant visa (IV) case processing, name clearance (through interfaces with name check applications), fingerprint and facial recognition clearance (through interfaces with biometric applications), adjudication, visa issuance, and refusal recording and tracking; 2) visa allocation management for allocations assigned to post; 3) biometric data collection (such as fingerprints and images for facial recognition); 4) automated tracking, scheduling and reporting of applicant interviews and medical exams; 5) internal fraud control, workload statistic management for post and Fraud Prevention Program (FPP) managers; 6) waiver processing; and 7) processing of boarding foils in connection with US Citizenship and Immigration Services (USCIS) approved cases.

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

IVO collects the following information from Non-U.S. citizens:

- Name
- Date of Birth
- Address
- Phone
- Emails
- Images/biometric identifiers
- Gender
- Nationality
- Language used
- Education
- Relationships
- Occupation
- Employment/ Employer information
- Financial information
- Aliases
- Alien registration numbers
- Marital status
- Social media information
- Family information
- Criminal information
- Medical information
- Final United States Address
- Passport number and other passport issuance information
- National Identification

IVO may also contain some information on U.S. citizens if a petitioner or attorney assists with the application, or if the applicant enters information in the system. The following PII may apply:

- Name
- Address
- Phone number
- Email
- Relationship to applicant
- Occupation information

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

8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
8 U.S.C. 1151-1363 (Title II of the Immigration and Nationality Act of 1952, as amended)
8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
22 U.S.C. 2651a (Organization of Department of State)
22 U.S.C. § 3927 (Chief of Mission)
26 U.S.C. 6039E (Information Concerning Residence Status)
22 C.F.R. Parts 40-42, and 46 (Visas)
8 U.S.C. 1701 et seq., Enhanced Border Security and Visa Entry Reform Act
U.S.C. 1101-1504 (Immigration and Nationality Act of 1952, as amended, Titles I-III, General, Immigration, Nationality and Naturalization)
8 U.S.C. 1701 et seq., Enhanced Border Security and Visa Entry Reform Act

(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: 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: B-09-002-08a, Immigrant Visa Overseas (IVO) System Issuances
Disposition Authority Number: N1-084-09-02, item 8a
Length of time the information is retained in the system: TEMPORARY. Cutoff at end of calendar year when issued. Destroy 5 years after cutoff or when no longer needed, whichever is sooner.
Type of information retained in the system: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Schedule number: B-09-002-08b, Immigrant Visa Overseas (IVO)- Cat I refusals
Disposition Authority Number: N1-084-09-02, item 8b
Length of time the information is retained in the system: TEMPORARY. Cutoff at end of calendar year when refused. Destroy 100 years after cutoff or when no longer needed, whichever is sooner.
Type of information retained in the system: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Schedule number: B-09-002-8-08c, Immigrant Visa Overseas (IVO)- Cat II refusals

Disposition Authority Number: N1-084-09-02, item 8c
Length of time the information is retained in the system: TEMPORARY. Cutoff at end of calendar year when refused. Destroy 25 years after cutoff or when no longer needed, whichever is sooner.
Type of information retained in the system: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Schedule number: B-09-002-08d, Abandoned Cases
Disposition Authority Number: N1-084-09-02, item 8d
Length of time the information is retained in the system: TEMPORARY. Cutoff at end of calendar year when abandoned. Destroy 50 years after cutoff or when no longer needed, whichever is sooner.
Type of information retained in the system: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic 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?

Visa application case data is electronically transmitted to the IVO system from the Immigrant Visa Information System (IVIS) and the Diversity Visa Information System (DVIS). DVIS and IVIS transmit information to IVO from visa applications, in-person interviews and supporting documentation provided by the applicant during the visa application process. The Non-Immigrant Visa (NIV) System transmits information to IVO for processing/issuance of K1/K3 visas.

(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 in the IVO system is the responsibility of the applicant completing the application for submission or entering data into the source system containing the visa application. The information is verified for accuracy by staff at posts using corroborating documentation and during in-person interviews. In addition, quality checks are conducted against the submitted documentation at every stage, and administrative policies minimize instances of inaccurate data. Staff at posts review the initial documentation and identification forms in the hard file sent by the National Visa Center (NVC) against what is loaded into the IVO application from IVIS. Any new documentation or identification forms submitted by the applicant from that point onward are also reviewed and verified against data in IVO.

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

Information is checked for currency at the point of collection of the source system where the applicant is requesting service. Information is also checked against supporting documentation provided. If a visa is reissued, the information is verified prior to reissuance.

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

IVO does not use commercial sources of information nor is the information publicly available.

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

The PII items listed in Question 3d are the minimum necessary to perform the actions required by the IVO system. Concerns about collecting and maintaining PII 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 IVO system to perform the intended function.

5. Use of information

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

The IVO PII collected is used to process visa cases for identity verification, facial recognition, and fingerprint matching and to automate tracking, scheduling, and reporting of applicant cases to assist in determining if the applicant is eligible for travel and immigration to the U.S.

(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 information collected is used to validate information provided against other CA systems and documentation to make determinations on the issuance of immigrant visas.

(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.

The IVO system shares information with the following CA systems: Consular Affairs Enterprise Service Bus (CAESB), Consular Shared Tables (CST), Consular Consolidated Database (CCD), Diversity Immigrant Visa Information System (DVIS), Immigrant Visa Information System (IVIS), Independent Namecheck (INK) system, Immigrant Visa Allocation Management System (IVAMS), Accountable items (AI) system, Consular Foreign & Domestic Post Infrastructure (CFDPI), and the Ten Print Live Scan System (TPLS).

External: None.

(b) What information will be shared?

Internal: Information addressed in paragraph 3d is shared internally within the Consular Affairs systems listed above, except for INK and TPLS. PII shared with INK consists of name, any aliases, phone number, address, birthdate, place of birth, photo, nationality, passport numbers, and national identification numbers. IVO PII shared with TPLS consist of biometric images and fingerprints.

External: N/A

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

Internal: The PII in Question 3d is shared with the CA systems in Question 6a to process visa requests by: (1) verifying applicant information through the use of biometrics, name checks, tracking of appointments; and (2) providing automated capabilities to manage visa case files to support the adjudication process of visa applicants wishing to come to the United States.

External: N/A

External: N/A

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

Internal: Information is shared database to database within CA by secured transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

External: N/A

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

Internal: IVO safeguards entail secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS)) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior outlined in the security controls for each major application, including IVO. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In addition, DoS employees must have a Personal Identity Verification/Personal Identification Number (PIV/PIN), as well as a separate unique user identification (ID) and password to access IVO data.

External: N/A

7. Redress and Notification

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

IVO does not collect information directly from applicants. Respective notices are provided via the source systems collecting the information from applicants requesting immigrant visas. Individuals are informed that failure to provide the information necessary to process the application may result in the application being rejected.

(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?

Individuals can decline to provide the information at the point of collection by the source system where the immigrant visa application is being submitted. However, the consular services requested for consideration of an immigrant visa may not be provided due to incomplete information provided.

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

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

System of Records Notice (SORN) STATE-39 Visa Records provides information and organization points of contact regarding questions and procedures to access information.

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

☒Yes ☐No

If yes, explain the procedures.

SORN STATE-39 Visa Records includes procedures on how to contact an office or individual for assistance to inquire about the existence of records pertaining to the individual.

Applicants can also follow procedures of the source system where the application was submitted for visa services and during the in-person interviews.

If no, explain why not.

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

SORN STATE-39 Visa Records provides information on procedures to access information and points of contact to inquire about information.

8. Security Controls

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

IVO is secured within the Department of State intranet which mitigates risk factors through 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 to perform official duties. Access to IVO information is further protected with additional access controls set at the database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer.

IVO is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable 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. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need to perform official duties.

(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).

Department of State IVO users, system administrators, database administrators and the security administrator have access to data in the system based on their prescribed roles and duties approved by the supervisor.

IVO users: Department of State IVO users consist of DoS post users and IVO headquarters management. These users facilitate, adjudicate, and process visa requests for immigrants applying for visas to come to the United States.

Security administrators: The Security Administrators are responsible for implementing management of security features of IVO, including proper activation, maintenance, and use of security features on the system.
System administrators: System Administrators are responsible for all daily maintenance.
Database administrators: Database Administrators (DBAs) are responsible for updating reference tables within the application. Responsibilities include daily maintenance, upgrades, patch/hotfix, and database configuration.

(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 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.

Least privileges are restrictive rights/privileges or access users need for the performance of specified tasks. The Department of State ensures through least privileges principles 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) 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 data of user roles listed in 8(b) is based on the position, role, and need to perform officially assigned duties as described. Supervisors and the local ISSO must approve access to IVO based on the specific role and level of security of information and personnel. Once personnel leave the project, their access to IVO is terminated.

(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 systems comply and remain compliant with Department of State and federal 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 applications for changes to the Department of State mandated security controls. Access control lists on OpenNet servers and devices along with Department of State Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures.

In accordance with Department of State 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 IVO System Security Plan (SSP) contains the procedures, controls, and responsibilities 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.

There is no specific role-based training. 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.