Immigrant Visa Information System (IVIS)

Privacy Impact Assessment

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: May 28, 2010

(b) Name of system: Immigrant Visa Information System

(c) System acronym: IVIS

(d) IT Asset Baseline (ITAB) number: 49

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

IVIS is a computerized Management Information System (MIS). IVIS is used by the National Visa Center (NVC) to manage the processing of immigrant visa petitions received from the Department of Homeland Security (DHS) - United States Citizenship and Immigration Services (CIS) regional service centers and district offices. IVIS provides for the recording of petitioner and beneficiary data, the processing of cases based on priority and cut-off dates, the creation and recording of correspondence with the beneficiary, petitioner and/or agent and the transmittal of data to the Immigrant Visa Overseas (IVO) system at post for final processing.

The mission of IVIS is to assist the NVC in tracking and processing immigration visa petitions based on local necessities and requirements established by the Department of State. The immigrant visa issuance process begins with the submission of a petition for immigration to the CIS. CIS reviews and adjudicates the petition and forwards approved petitions to the Department of State for visa processing. Prior to late 1991, the approved petitions were forwarded directly to the overseas post where the visas were to be issued. However, many of the petitions were approved in categories that had numerical limitations (i.e., a quota for a given fiscal year) established by statute.

The NVC performs several visa-processing activities that track petitions requesting immigration services from initial NVC receipt from CIS through final disposition to the posts. NVC processing includes:

- Mail room receipt and tracking
- Case review and verification
- Data entry
- Preparation of case folders for posts
- Case problem resolution
- Preparation and distribution of informational materials for petitioners, agents and beneficiaries processing
- Verification of all stages of case processing with rigorous quality control

procedures
- Communication with the general public and federal organizations
- Domestic fee collection updates
- Document collection and review
- Scheduling of immigrant visa appointments
- Security Advisory Opinions

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): June 26, 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

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

The following PII regarding the petitioner are collected from the petitioner, either directly or through DHS USCIS, and maintained by IVIS:

- Full Name
- Address
- E-mail address
- Telephone Number
- Petitioner Date of Birth
- Gender
- Marital Status
- Alien Number
- Social Security Number (SSN)
- Tax ID
- Organization Name
- U.S. Status
- Nationality
- Petitioner Country of Birth
- City of Birth
- Income information for Joint Sponsors

The sources from which the information is collected are:

- Petitioner
- Beneficiary
- Third Party/Agent
- Attorney
- DHS USCIS
- The U.S. Bank (under Department of State contract)

b. How is the information collected?

The information is obtained from an individual petitioner who submits a petition for immigration to the USCIS. USCIS reviews and adjudicates the petition and forwards the approved petitions (paper form) to Department of State NVC located in Portsmouth, NH for visa processing.

Some of the petitioner's data is transferred electronically to IVIS via DataShare, which provides high performance secure connectivity between the Department of State and DHS to support the exchange of visa data.

A 3rd party source of information is the U.S. Bank under Department of State contract. A text file from the U.S. Bank with case numbers is used to track the payments from the petitioners.

Updates to PII information is submitted to the NVC via forms and documents mailed by the petitioner or legal representative to the NVC, as well as through telephone and email exchange of information.

c. Why is the information collected and maintained?

Each element of PII collected and maintained by IVIS is required by DHS USCIS to approve immigrant visa applications, and for the Department of State to adjudicate the issuance of visas to approved applicants.

d. How will the information be checked for accuracy?

There are two main accuracy checks: (1) IVIS has built-in functionality to validate and check on the data being entered, and (2) Visa Processing Specialists review petitions to ensure all required data is provided. A letter is sent to applicants requesting any inaccurate or missing data be updated or provided. Examples of the information being checked during the review process are:

- Date of Birth is compared with birth certificates provided by the applicant.
- Financial data on the I-864 form is compared with tax returns from the last three years provided by the applicant.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

IVIS was developed and modified to support U.S. immigration and nationality law as defined in the major legislation listed below:

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 22 U.S.C 2651(a) (Organization of Department of State)

- The Immigration and Nationality (INA) act, 8 U.S.C. 1202, Section 222 (f)
- Immigration Act of 1990
- Illegal Immigration Reform and Immigration Responsibility Act of 1996
- (IIRIRA96)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000)
- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)
- Child Status Protection Act (HR 1209) 2002

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

The collection of PII creates the vulnerability that DHS USCIS and Department of State - NVC employees may use the PII for purposes other than those required by the Department of State and thereby misuse the PII. The potential threats to privacy include:

- Inadequate security by the USCIS and NVC — USCIS and NVC employees may create a new repository of PII that is vulnerable to unauthorized access, use, disclosure and retention;
- Inadequate data integrity - USCIS and NVC data entry personnel may enter the data into IVIS wrong and may modify the data without authorization; and
- Inadequate openness and transparency— USCIS may not provide sufficient details to allow applicants to understand how their information will be used.

As it relates to immigration visa processing, the impact of these threats on the applicants could include delays in responses, possible subsequent denial of immigration to the United States based on faulty data, or misuse of PII. As it relates to USCIS and NVC collection of PII, the impact of these threats on the applicant can include the loss of control over the use and disclosure of their PII. The opportunities for the misuse of PII, and the serious impact that USCIS and NVC misuse would have on covered petitioners and the integrity of the IVIS makes the misuse of PII by USCIS and NVC a high risk.

DHS and Department of State seek to address these risks by minimizing the collection and transmission of PII to the minimum required.

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports. In addition, these controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application. Only authorized users with a need to know are granted access to IVIS.

4. Uses of the Information

a. Describe all uses of the information.

The information collected by IVIS is used for processing, auditing and tracking of individual immigration visa applications as well as tracking the number of immigrant visas assigned that are subject to numerical limitations based upon the visa classification and country of chargeability.

Data can be retrieved using the following identifiers:

- Case number (most frequently used)
- Applicant, Petitioner, or Legal Representative name
- Social Security Number (SSN)
- Tax ID
- Date of Birth
- Place of birth
- CIS Receipt Number
- Organization Name
- Alien Number

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

Visa Processing Specialists can pull up petitioner, applicant 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.

In addition, reports can be produced for analysis such as, but not limited to:

Report	Use	Access
Current Detail Report	Obtain list of current cases	System Operator
Non-Current Detail Report	Obtain list of non-current cases	System Operator
Case Detail Reports	List of cases with Joint Agencies	System Operator / NVC User
Report 20	Visa Allocation	NVC User
Management Workload	Work performance information	Applicable Managers / NVC employees
Instruction Packet Reports	Obtain list of applicants receiving Instruction Packet Mail outs	NVC User

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Visa applicant data such as photo, fingerprint, proof of birth, birth place, other identifying documents, existing passports provided by visa applicant and/or foreign authorities is used to effectively identify the visa applicant.

d. Is the system a contractor used and owned system?

IVIS is a government owned system. Government personnel are the primary users of IVIS; however, contractors are involved with the design, development and maintenance of the system. Privacy Act information clauses have been inserted into all Statements of Work and become part of the signed contract. All users are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted.

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

It is mandatory for all Department of State employees and contractors to complete an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

Each domestic organization has at least one Security Officer who is responsible for managing the users within the organization. Security Officers are government employees who approve account requests and assign roles appropriate for each user's job requirement. Roles determine what a user can do within IVIS.

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. Contractors who support IVIS are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors involved in the development and/or maintenance of IVIS hardware and software must have a level "Secret" security clearance. Once the highest-level background investigation required has been completed, cleared technical personnel (government and contractors) will be allowed to access the server rooms housing the IVIS.

The CA post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that is SBU.

5. Retention

a. How long is information retained?

The retention time of the visa records varies depending upon the specific kind of record. Files of closed cases are retired or destroyed in accordance to the published record schedules of the Department of State and the National Archives and Records Administration, specifically GRS 20 items 2b and 2c. Some records, such as refused records, are retained until the subject is 100 years old and 10 years have passed since the last visa activity. Procedures are documented at the Office of Freedom of Information, Privacy, and Classification Review, Room 1239, Department of State, 2201 C Street NW, Washington, DC 20520-1239.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of IVIS throughout the lifetime of the data. Accuracy of the data is dependent on the individuals providing self-identifying information. The information is only retained for the amount of time that is required to perform the System's purpose.

Department of State OpenNet security protocols are used to ensure that the data is stored and backed up in a secure environment.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with published Department of State record schedules as approved by the National Archives and Records Administration.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

- **DataShare/Interagency Data Exchange Application (IDEA)** - provides application case data from the petition. This data will automatically appear in IVIS when creating a case.
- **Conversant Interactive Voice Response (IVR**) - an interactive voice response telephone application at NVC provides Case Number, Receipt Number, Letter destination information, Post Code, Visa Class, and FSC – fields that are downloaded from IVIS to Conversant IVR.
- **Consular Consolidated Database (CCD)** – connects to IVIS for the purpose of production data reproduction.
- **Telecommunications Manager (TCM) Parser -** allows name (including aliases) and geographic data sent from IVIS to be processed by TCM Parser which performs name checks on applicants in IVIS.
- **Immigrant Visa Allocation Management System (IVAMS)** - Case Number, FSC, Post Code, and Visa Class are loaded into IVAMS for the purpose of immigrant visa tracking and reporting.
- **Diversity Visa Information System (DVIS)** – Alien Numbers generated in IVIS are transferred to DVIS and the DV post systems.
- **Immigrant Visa Overseas (IVO)** – data on immigrant visas, petitions, and allocations is sent to post location and loaded into their IVO systems.
- **SharePoint** - data and images on immigrant visas, petitions, and appointment information is shared with post through a secure site.
- **Worldwide Refugee Admission Program System (WRAPS)** – data on immigrant visa petitions is sent to the Refugee Processing Center's WRAPS system.

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

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Access to electronic files is protected by passwords, and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

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

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. IVIS mitigates these vulnerabilities by working closely with the sharing organizations to develop secure standard operating procedures for using this data. These procedures are documented in sharing agreements.

Access to information is controlled by application access controls. User training at the application level is delivered annually in accordance with internal Department of State regulations.

IVIS has formal, documented procedures to facilitate the implementation of its audit and accountability processes. The application produces audit records that contain sufficient information to establish what events occurred, the sources of the events identified by type, location, or subject. System administrators regularly review and analyze the application audit records for indications of suspicious activity or suspected violations of security protocols.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

IVIS allows USCIS to share information collected on immigrant petitions and applicants. The Department of State shares data with USCIS using import and export features from DataShare.

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

OpenNet allows the NVC to utilize DataShare to move the data from the Consular Consolidated Database (CCD). In addition, DataShare allows text files to be converted into IDEA format and transferred to USCIS.

In all cases of sharing with DHS, all components are required to comply with the Department's security policies and procedures, particularly the *DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1).* This handbook establishes a comprehensive program for DHS to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules, which are applied to component systems, communications between component systems, and at all interfaces between component systems and external systems.

Each data sharing arrangement with federal agency partners is covered by a written agreement in the form of a Memorandum of Understanding or exchange of letters as well as technical documentation including an interface control document and interagency security agreement. Data is sent through encrypted lines.

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

Any data sharing, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. IVIS mitigates these vulnerabilities by working closely with the sharing organizations to establish formal agreements and develop secure standard operating procedures for sharing the data. The security program involves the establishment of strict rules of behavior for each major application, including IVIS. It includes a periodic assessment of physical, technical, and

administrative controls designed to enhance accountability and data integrity. It also requires that all users be adequately trained regarding the security of IVIS, that system users must participate in a security training program, and that contractors and consultants must also sign a non-disclosure agreement. External connections must be documented and approved with both parties' signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

- Visa Records, State-39

☐ does NOT contain information covered by the Privacy Act.

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

Yes, the following forms provide notice explaining the reason for collecting PII, how it will be used, and the effect of not providing the PII. Refer to the USCIS website, http://www.uscis.gov/portal/site/uscis, for more details on the USCIS forms. The DS-230 and DS-3032 are the Department of State forms:

- I-864
- DS-230
- DS-3032
- I-130
- I-140
- I-129F
- I-360
- I-526
- I-730
- I-600
- I-600A
- I-824
- I-797
- V37, V38, V39
- I-171H
- I-800

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

Yes, the petitioners have the right to decline to provide PII for use in processing their immigration visa application. However, failure to provide the information necessary to process the application may result in the application being rejected.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Information is given voluntarily by the applicants or his/her representative. No other special uses of the information are permitted. Individuals are advised on the use of the information being collected at the time of collection.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

IVIS relies on State-39 and on the notice given to the petitioners who fill out the form to mitigate the privacy risks posed by collection and use of PII.

The mechanisms for notice offered to individuals are reasonable and adequate in relation to the system's purpose and uses. The information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). The information provided on the forms and in the SORN regarding visa records fully explain how the information may be used by the Department and how it is protected.

Access to IVIS is restricted to cleared, authorized Department of State direct hires and contractor personnel. IVIS enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Information in IVIS is considered a visa record subject to confidentiality requirements under INA 222(f). IVIS information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a). In addition, covered petitioners may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Processing Specialists at NVC will identify discrepancies and send out letters to applicants requesting updated or corrected information.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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

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

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to IVIS 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. To access the system, users must be granted the status of an authorized user of the Department of State's unclassified network. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. The Operations Unit at NVC serves as the administrator for creating and modifying IVIS accounts, granting the appropriate level of system access based on the determination of the unit manager. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

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

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Internal based users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

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

11. Technologies

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

IVIS does not employ any technology known to elevate privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

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

12. Security

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

The Department of State operates IVIS, in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. The Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system,

IVIS has completed the C&A process, and IVIS was granted an Authority to Operate (ATO) in August 31, 2007. This ATO will expire in August 2010. Any significant change to IVIS will be reviewed. In addition, an Annual Control Assessment is used to monitor and reexamine the security safeguards put in place.