Diversity Immigrant Visa Information System (DVIS)

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:** September 1, 2009

b. **Name of system:** Diversity Visa Information System

c. **System acronym:** DVIS

d. **IT Asset Baseline (ITAB) number:** 17

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

The Immigration and Nationality Act (INA) established a program in 1995 whereby an annual numerical limitation of 55,000 immigrant visas would be awarded each year to nationals of specific "low admission" countries through a process known as the Diversity Visa (DV) Lottery Program. The DVIS system is used by the Kentucky Consular Center (KCC) personnel to process more than 6 million applications received each year for the Diversity Lottery.

The DVIS system is used by the Kentucky Consular Center (KCC) personnel to process more than 6 million applications received each year for the Diversity Lottery. The DV program allows a pre-determined number of citizens of other countries to apply for immigrant visas to the United States. Entries in the Diversity Lottery are processed on a regional basis; the six world regions are Africa, Asia, Europe, North America, Oceania, and South America. Program applicants do not need to have a relative in the United States. The Diversity Lottery is completely separate from the immigrant visa process. Applications for the Diversity program are submitted from all over the world via the Internet using Electronic Diversity Visa (EDV) system, to KCC.

DVIS helps KCC personnel track the enormous number of entries submitted to the Diversity Lottery. Entries are tracked by rank numbers that are assigned based on the order of selection in the lottery.

When the entry period is over, an algorithm within DVIS is run to randomly select the winning entries. Each winning entry will go through the validation process. Once a case is determined to be complete, a selectee packet is sent to the selectee. The packet contains a letter saying that the user has been selected for further consideration in the Diversity Visa program, along with several forms that the selectee must complete to provide more information.

When the forms are sent back, they, along with any other documents that were sent, are assigned to a case file. A data entry user then enters any new information that the applicant provided. If the selectee provided all the necessary information (such as full name, education, occupation), the case is sent to another user for the second quality check to ensure all new information was entered correctly.

Once cases pass the second quality check, they are reported to the Visa Office (CA/VO). The Visa Office then determines cutoff numbers that are used when the visas are allocated. Any case with a lottery rank number below the cutoff numbers will be allocated visas slots for all eligible members. The cases are then scheduled for interviews at the posts based on the number of cases a post can handle per day.

Once a case has been scheduled for an interview, the appointment packet is sent to the applicant. The appointment packet contains a letter saying that the case has been sent to the relevant post for final processing and detailing the interview date and time that has been scheduled. All forms and case information are then sent to the post via electronic data transfer.

f. Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

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

☒ PIA Information Review

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

h. Date of previous PIA (if applicable): April 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 DVIS primarily collects and maintains information on foreign nationals as part of the U.S. diversity visa lottery and application process. As such, the information provided by the diversity visa entrant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). Because the visa applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the Privacy Act.

However, a DVIS record may include PII on persons associated with the diversity visa applicant, such as a legal representative, who are US citizens or legal permanent residents and who are covered by the Privacy Act.

If provided by the applicant, this PII data may include the following:

- Last Name
- First Name
- Middle Name
- Firm
- Street (of law office)
- City
- State
- Zip Code/+4
- Phone (Work)
- Phone (Home)
- Phone (Other)

Entrants are the primary source of the information when they apply online using the electronic Diversity Visa (e-DV) web application. The data is then transferred to DVIS.

b. How is the information collected?

The information is collected when the entrants enter online using the electronic Diversity Visa (e-DV) web entry. The data is then transferred to DVIS.

c. Why is the information collected and maintained?

The information is collected to determine the eligibility of applicants who have applied, or are applying, for an Immigrant Visa to the United States.

d. How will the information be checked for accuracy?

Accuracy of the information on an immigrant visa application is primarily the responsibility of the applicant. Contract staff or Department personnel also validate the accuracy of the information before submission and transfer into DVIS.

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

- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

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

The DVIS collects the minimum amount of personally identifiable information (PII) necessary as part of the U.S. diversity visa lottery and application process.

Due to the strict security controls that are required to be in place before operation of the system, no identified privacy risks are associated with this system. The 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 DVIS.

4. Uses of the Information

a. Describe all uses of the information.

The only use of PII data in DVIS is for the purpose of communication with the Visa Applicants.

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

PII data is not analyzed in DVIS; no new information is produced.

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

The DVIS does not use commercial information, publicly available information or information from other Federal agency databases.

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

The DVIS is a government owned system. Government personnel are primary users of DVIS. Contractors are involved with the design and development of the system. All users were 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.

The DVIS performs basic internal analytical functions on the PII but does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of “function creep,” wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

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 DVIS system administrator uses the User Administration window to establish, activate, modify, review, disable, and remove DVIS user accounts. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

5. Retention

a. How long is information retained?

Visa applications are retained in compliance with the Visa Lookout Accountability provisions of the Illegal Immigration Reform and Immigration Responsibility Act of 1996 and the records disposition schedule. The complete disposition schedule for visa records is specified in the U.S. Department of State Records Disposition Schedule, Chapter 14: Visa records, approved by the National Archives and Records Administration.

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

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 the National Archive and Records Administration (NARA) rules.

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?

The DVIS information is shared with Department of State consular officers that may be handling a legal, technical or procedural question resulting from an application for an immigrant visa. The DVIS also has interconnections with the following CA systems:

Interfacing System & Description	Connection Description	Data Flow	ATO Expiration
Consular Consolidated Database (CCD): **ITAB #: 9** The CCD system is an extremely large data warehouse resides at SA-26 and SA-1 that hold all current data, and all archived data from all of the Consular Affairs post databases around the world. It was created to provide Consular Affairs a near real-time aggregate of the consular transaction activity collected in post databases worldwide. The CCD supports query and reporting requirements, data entry requirements, as well as the full recovery of post databases.	DVIS connects to CCD for sole purpose of production data replication.	One-way: from DVIS to CCD	February 2010
Electronic Diversity Visa (EDV): **ITAB #: 722** The EDV system is a website application used by potential Diversity Visa applicants to enter information electronically for possible lottery selection for the Diversity Visa program. The EDV System eliminates the need for paper applications through the US Postal Service, with subsequent manual data entry and helps reduce costly data entry errors. DVIS provides enhanced editing, error handling capabilities, more sophisticated checks for duplicate applications and fraud detection using advance Facial Recognition technology. The information collected run through facial recognition software, packaged and sent to DVIS via files stored in directory made accessible to DVIS.	EDV user flags cleared applications/cases and converted the files into XML format. An automated process runs every night to collects all cleared applications/cases and put it into a zip file. DVIS system administrator logon to EDV Batch Transfer Service (BTS) to extract/download the zip file to the local directory and logon to EDV Application Review System (ARS) to import/upload the zip file into DVIS on a daily basis.	One-way: from EDV to DVIS	May 2010

Interfacing System & Description	Connection Description	Data Flow	ATO Expiration
Immigrant Visa Allocation and Management System (IVAMS): **ITAB #: 97** IVAMS is an inventory system for Immigrant Visa (IV) and Diversity Visa (DV). IVAMS receives immigrant visa authorization requests from all immigrant visa processing posts (including the NVC) and from the Immigration and Naturalization Service. It controls the allocation of immigrant visa numbers in accordance with the rules on foreign state chargeability, priority date, and preference category as specified in the Immigration and Nationality Act, and based on the posts' monthly reports of qualified applicants. IVAMS acts as a repository for worldwide visa statistics. IVAMS tracks the posts' demand requests for and allocations of immigration and diversity visas. This system automatically calculates visa quotas based on US Government policies and sends Qualifying Dates and Allocation Information to the IVIS system at NVC and IV posts abroad. IVAMS deals with numbers of visas as opposed to individual visas and the associated applicant names.	DVIS uses the statistical data and allocation information from IVAMS to process Diversity immigrant visas utilizing Report 20 (a fixed format text file) and transmitted via OpenNet as an email attachment.	One-way: from IVAMS to DVIS	August 2010
Immigrate Visa Information System (IVIS): **ITAB #: 49** IVIS is a computerized Management Information System (MIS). The mission of IVIS is to assist the National Visa Center (NVC) performs several visa-processing activities that track petitions requesting immigration services from initial NVC receipt from CIS through final disposition to the Posts.	Alien Numbers (A-Numbers) are assigned to each member of a case when sending case(s) to Post during Transfer Case to Post. The A-Numbers are generated and maintained by the IVIS system at the NVC. A-Numbers are requested from IVIS via OpenNet email. Upon request, the NVC will email a file of A-Numbers generated by IVIS to be imported into DVIS (in the form of a binary file) using the A-Numbers File Import option.	One-way: from NVC to DVIS	August 2010

Interfacing System & Description	Connection Description	Data Flow	ATO Expiration
Immigrant Visa Overseas (IVO): **ITAB #: 817** IVO provides automated support to the issuance of an immigrant or a diversity visa to individuals wishing to come to the United States with the eventual goal of becoming a U.S. citizen. The system also provides for the administration of federal regulations that govern the issuance of either type of visa. IVO is a consolidation of the IV/DV systems. The IVO primary system functions include Petition Case Management, Case Applicant Management, and Visa Allocation Management. This system handles the final processing of Immigrant Visas and Diversity Immigrant Visas. IVO supports the maintenance of application records, performs CLASS name checks, processes clearances electronically or via clearance letters, handles quota control functions, permits queries by individual record, prepares correspondence, schedules appointments, generates statistic and management reports, record officer's decision, and print and account for visas and foils. Updates visa refusal and information to CLASS, distributes issuance and refusal information to a domestic repository, scans application forms and supporting documents, and allows for the handling and tracking of visa inquiries received form government agencies and Congress. Information is shared from this system with many agencies and organizations, usually through CCD.	DVIS transfers immigration cases to IVO for final processing.	One-way: from DVIS to IVO	August 2010

Interfacing System & Description	Connection Description	Data Flow	ATO Expiration
Telecommunications Manager (TCM): **ITAB #: 564** TCM is a software application that facilitates client systems to query and/or add refusal information to appropriate name check system databases. TCM is predominantly deployed at overseas sites and servers as a connection point (middle-tier) between the name check systems - Consular Lookout and Support System (CLASS) and the client modernized systems - Immigrant Visa Overseas (IVO), Non-Immigrant Visa (NIV), Diversity Visa (DV) systems, and American Citizen Services (ACS). TCM maintains historical information utilized by the Consular Affairs Management System (CAMS). In order to keep the transaction flow between all of these systems, TCM serves as a translator and maintains the data flow between the modernized client applications (posts) and CLASS in Washington DC, and serves as a network monitor and data re-director.	DVIS connects to TCM for name check, Security Advisory Opinions (SAO) request, and responses.	Two-ways: from DVIS to TCM and back	May 2011

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. An Interface Control Document (ICD) and Memorandum of Understanding (MOU) define and disclose transmission format via OpenNet. 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.

Access to information is controlled by application access controls. Management Control Reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal DoS regulations.

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?

The DVIS information is shared with the National Crime Information Center (NCIC) to gather beneficiaries (16 years old and up) who have been allocated visas with NCIC. The beneficiaries' information is stored in DVIS for informational purposes.

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

NCIC and DVIS are not interconnected. DVIS extracts a list of beneficiaries utilizing the Report 20 and deliver via email over the Department secure communication line, OpenNet.

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.

DVIS information is shared with NCIC with a statutory requirement and in accordance with confidentiality requirements under INA section 222(f). Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure any risk is addressed through the user-authorization process.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems)

- 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?

The information provided by the immigrant visa Applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

The Electronic Diversity Visa (EDV) system is a website application used by potential Diversity Visa applicants to enter information electronically for possible lottery selection for the Diversity Visa program. The EDV immigrant visa entry form provides a statement that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

Also, notice is provided in the System of Records Notice Visa Records, State-39, Visa Records.

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

Information is given voluntarily by the Entrant and with their consent, by Legal Representative.

Individuals who voluntarily apply for a U.S. immigration visa must supply all the requested information, and may not decline to provide part or all the information required, if they wish immigration visa services.

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?

Entrants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system’s disclosed purposes and uses).

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.

The notice offered is reasonable and adequate in relation to the system’s purposes and uses.

The information provided by the entrant 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 form and in the SORN regarding visa records fully explain how the information may be used by the Department and how it is protected.

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?

The information in DVIS is considered a visa record subject to confidentiality requirements under INA 222(f).

Visa entrants may change their information at any time prior to submission of the DV entry online.

Once a visa application is filed, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request and this guidance is available to the public in Volume 9 of the Foreign Affairs Manual (FAM) Section 40.4:

1) Correspondence previously sent to or given to the applicant by the post;
2) Civil documents presented by the applicant; and
3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted; i.e., with any remarks or notations by U.S. Government employees deleted.

DVIS information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to the Freedom of Information Act (FOIA) or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN (STATE-39, Visa Records), 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 DVIS may be Privacy Act-covered, 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 DVIS.

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 DVIS is limited to authorized Department of State users that have a justified need for the information in order to perform official duties. To access the system, authorized users must be an authorized user of the Department of State’ unclassified network. Access to DVIS requires a unique user account assigned by a supervisor. 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. 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?

All users must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain 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 available 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?

DVIS 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 DVIS 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

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

Department of State operates DVIS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. 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, DVIS was certified and accredited for 36 months to expire on November 30, 2011.