

eDV PIA

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of System: Electronic Diversity Visa System

(b) Bureau: Consular Affairs

(c) System Acronym: eDV

(d) iMatrix Asset ID Number: 722

(e) Reason for Performing PIA:

- New System
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

- Yes
- No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security assessment and authorization (A&A) status of the system?

The triennial Assessment and Authorization process is underway and eDV is expected to receive an Authorization-To-Operate by June 1, 2016.

(c) Describe the purpose of the system:

The Diversity Immigrant Visa Program is administered on an annual basis by the Department of State in accordance with section 203(c) of the Immigration and Nationality Act (INA) of 1952, as amended. A computer-generated, random lottery drawing chooses selectees for Diversity Visas (DVs). The visas are distributed among six geographic regions, with greater numbers of visas going to regions with lower rates of immigration, and with no visas going to nationals of countries sending more than 50,000 immigrants to the United States over the period of the past five fiscal years. Within each region, no single country may receive more than seven percent of the available DVs in any one year.

Instructions on how to fill out the lottery entry form are given on the web site accessible through travel.state.gov. No user IDs or passwords are issued to public users because of the one-way flow of entry form information. Once a public user submits an entry form, he or she is issued a confirmation number, which he or she later uses to access a notification as to whether he or she was or was not selected in the lottery for further visa processing. Once a public user submits an application, the system does not allow the applicant to subsequently read, modify, or delete the submitted information. eDV gathers only the application information.

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

The eDV 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 entrants themselves are not U.S. citizens or legal permanent residents, they are not covered by the provisions of the Privacy Act.

The eDV entrant PII collected includes:

- Names of Individual
- Birthdates of Individual
- Phone number(s) of Individual
- Personal Address
- e-mail address(es) of individual
- Images or Biometric IDs
- Gender, city & country where born
- Education, marital status, number of children in family applying for the diversity visa

There also exists the possibility that an eDV record may include PII on persons associated with the Diversity Visa applicant, such as a derivative spouse or child of the entrant who are U.S. citizens or legal permanent residents who are covered by the Privacy Act. While entrants are not required to submit information about U.S. citizen spouses or children, some do so. The U.S. Citizen or LPR PII could consist of:

- Name, DOB, gender, city and country of birth, and an image of each family member (spouse and children).

The data is then transferred to the Consular Consolidated Database (CCD) for use in the lottery drawing.

(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 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)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

SORN Name and Number: State-39, Visa Records

SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): October 25, 2012

- No, explain how the information is retrieved without a personal identifier.**
- N/A

(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 Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

- Yes
- No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:**B-09-002-40a Diversity Visa Applicant Control System (DVACS)**

Description: This on-line tracking and case management system maintains a data base of immigrant visa applicants who have applied for entry into the United States under the Diversity Visa Program.

Master On-Line File.

Disposition: Destroy when active use ceases.

DispAuthNo: N1-084-97-4, item 1a

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

- Yes
- No
- N/A

If yes, under what authorization?

(c) How is the information collected?

The information is collected online by the entrants using the electronic Diversity Visa (eDV) web entry forms. Users enter their information into a secure web site operated by the Bureau of Consular Affairs (CA) to accomplish this task.

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

If you did not select “Department-owned equipment,” please specify.

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

There is no process used to determine if the information entered into the eDV lottery entry is accurate. Required fields must contain data to be accepted. The application fields within the web page handle the logical format field checks by limiting the type of information that can be entered, such as alpha or numeric, or by providing drop down pick lists of available choices. Accuracy of the information on each eDV entry is the responsibility of the entrant.

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

The entrants are never able to update the data submitted through the eDV lottery entry website. However, if they are selected, they are able to change the data through the DS-260 application form provided on the Department's website. In this case, the Kentucky Consular Center (KCC) notes the changed information in the Diversity Visa Information System (DVIS), which is forwarded to the Immigrant Visa Overseas (IVO) system for review at post during the interview. If the lottery entrant is not selected nothing further happens. No data is discarded. At the end of the program year, all data is stored in the CCD and is no longer processed.

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

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

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

The information provided by the DV entrant submitting information via the eDV web form is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). The eDV immigrant visa entry form provides a statement that the information collected is protected by INA 222(f). INA 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.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

Yes

No

If yes, how do individuals grant consent?

Information is given voluntarily by the applicant or, with their consent, by their legal representative. Individuals who voluntarily apply to enter the Diversity Visa program must supply all the requested information and may not decline to provide part or all the information required, if they wish to be considered for selection in the diversity visa lottery.

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

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

During the design of the eDV information system the capability for applicants to input U.S. Citizen or Legal Permanent Resident Data (LPR) was included although this information is not required. Because U.S. Citizen or Legal Permanent Resident Data (LPR) can be included as part of this process, a PIA was created to show how eDV PII is handled. All PII is protected equally within the eDV information system.

5. Use of information

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

The purpose of the eDV system is to support the replacement of paper applications for the DV Lottery Program with an electronic application capture process based on web technology and the Internet. eDV reduces costly data entry errors and provides a more reliable method for eliminating and/or preventing duplicate applications.

The only uses of PII in eDV is to establish the identity of the entrant, determine whether eligibility requirements are met, send communications to the entrant, and to detect and prevent fraudulent or duplicate entries from being selected or approved for visas. Immigrant visa lottery entrant records are routinely retrieved using name, date of birth, and confirmation numbers automatically generated by the Oracle database.

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

The use of the information within the information system is utilized for the purpose for which the system was designed.

(c) Does the system analyze the information stored in it?

- Yes
 No

If yes:

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

(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

6. Sharing of Information

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

The eDV information is shared internally with Department of State employees who have access to CCD. Recipients of the information with a need to know are the Database Engineering Data Management (DEDM), Kentucky Consular Center (KCC), Consular Systems and Technology (CST), and Visa Office Personnel.

The eDV information in the eDV database may occasionally be shared internally or externally in connection with fraud investigations or law enforcement requests. Requests for eDV information must go through the Visa Office and in turn could be shared with DHS or FBI personnel with a need to know.

(b) What information will be shared?

The shared information may include the following to either internal and or external groups or agencies:

- Names of Individuals
- Birthdates of Individuals
- Phone number(s) of Individuals
- Personal Address
- e-mail address(es) of individuals
- Images or Biometric IDs
- Gender, city & country where born
- Education, marital status, number of children in family applying for the diversity visa

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

The purpose for sharing the information is to allow the Department of State to remove duplicates, perform facial recognition tasks, process the lottery drawing, and to adjudicate diversity visa applications.

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

Information is shared by secure transmission (https / ssl) methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. External information shared with DHS and FBI is completed by request by the CCD reporting team which accesses a copy of the eDV data that resides within the CCD. Only the requested data will be output to a spreadsheet and provided via email. eDV is not involved in transmission or data sharing. In addition, data is downloaded to a DVD and encrypted and then provided to an off-site contractor that audits the stored data using a special algorithm.

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

Any eDV data that is shared is done through queries by the CCD Reporting team using the replicated data that resides on the CCD. Safeguards in place for access to eDV data which resides in CCD include: electronic files that are password protected and under the supervision of system managers, audit trails that track and monitor usage and access, and regularly administered security/privacy training that informs authorized users of proper handling procedures.

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

Because eDV collects a variety of PII for the diversity visa lottery program, privacy concerns include intentional and/or unintentional disclosure of personal information by

personnel. This can result from social engineering, phishing, abuse of elevated privileges, or general lack of training.

To eliminate the possibility of disclosure, no one has access to the PII which resides within the eDV databases.

To further address privacy concerns of sharing data, there is no sharing of data from the public-facing DMZ. The only sharing of data happens through the CCD.

7. Redress and Notification

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

There are no procedures documented that state how an individual would gain access to their submitted information because there is no means that allow applicants to gain access to the eDV lottery entry form once it's submitted.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes

No

If yes, explain the procedures.

The entrants are never able to update the data submitted through eDV. However, if they are selected, they are able to change data through the DS-260. In this case, the KCC notes the changed information in DVIS, which is forwarded to IVO for review at Post during the interview. If an entrant is not selected, their data is not processed and will never be updated.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals do not receive formal notification regarding correcting their information. However, if they are selected, they are able to change data through the DS-260, which is the form required to apply for their visa application.

8. Security Controls

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

Currently, the eDV entry data is stored permanently in the CCD. All data is secured by implementing the Diplomatic Security Oracle Database Security Configuration Standard for Server and Client.

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

Internal access to eDV 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.

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 user’s supervisor specifies the appropriate level of system access based on the determination of the unit manager.

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

The database administrators and ISSOs use Oracle tools such as Oracle Enterprise Manager Audit Vault, Database Vault, and Database Audit Tables and Views to monitor, record, and audit database transactions.

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

All users must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the information system. In order to retain the access, users must complete annual refresher training. Additionally, all employees at the Department of State, and Locally Employed Staff that work with PII must take PA-459, a course entitled Protecting Personally Identifiable Information or a comparable course.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?

Yes

No

If yes, please explain.

Numerous levels of access control and identification and authentication are in place to reduce the chance an intruder could enter the eDV information system boundary. In addition, the auditing of system and information integrity controls occurs to monitor and record possible attempts at entering the eDV information system boundary.

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

Due to the sensitivity of the information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing of user activity. The information collected contains PII of foreigners and possibly U.S. Citizen / LPR. Although recourse for each group is different the PII is protected within the information system in the same manner. The measures implemented are the result and consideration of the amount and type of PII that eDV collects.

9. Data Access

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

Department of State employees and contractors who hold the title or job responsibility of internal users, system administrators, and database administrators for eDV have access to data within eDV.

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

An individual's job functions/role determines what data he/she may access. Access control lists and accounts are reviewed routinely to determine if people still need access.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

- Yes
 No

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

All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. Users will have access based on their roles/job functions.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

The risks associated with sharing privacy information internally and or externally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of personal information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. For this reason annual security awareness training is required prior to accessing the eDV information system. In addition, numerous levels of access controls, auditing, identification and authentication, media protection, and system and information integrity are implemented to reduce the risk and misuse of privacy information by personnel.