

Electronic Diversity Visa (eDV)

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 10, 2009

(b) Name of system: Electronic Diversity Visa

(c) System acronym: eDV

(d) IT Asset Baseline (ITAB) number: 722

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

Electronic Diversity Visa (eDV) is a mission-supportive system that supports the Diversity Visa Lottery Program with an electronic application-capture process based on Web technology and the Internet. Applicants for immigrant visas can use eDV to apply for a visa online through a web application. eDV reduces costly data entry errors and provides a better method for preventing duplicate applications.

(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?

Electronic Diversity Visa (eDV)

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 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, an eDV record may include PII on persons associated with the diversity visa applicant, such as a legal representative, who is a U.S. citizens or legal permanent resident.

If provided by the applicant, eDV collects information about the applicant's legal representative, typically a U.S. person. This PII data may include the following:

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

Applicants are the primary source of information when they apply online using the electronic Diversity Visa (e-DV) web application.

b. How is the information collected?

The information is collected directly from the visa applicants when they apply online using the electronic Diversity Visa (e-DV) web application.

Potential applicants from all over the world can access the application during the 60 days of the Diversity Visa Lottery Application Window and will be granted anonymous web access via the Internet. Instructions on how to access the web site are given in the Federal Registry announcement. Instructions on how to fill out the application are given on the application web site. No user IDs or passwords are issued to public users because of the one-way flow of application information. Once a public user submits an application the system does not allow the public user to subsequently read, modify, or delete the submitted information. eDV only gathers the application information. The process involves the public user accessing the eDV system using a web browser. The applicants are made aware that personal information is being forwarded and are given a choice to send it encrypted through SSL or unencrypted.

Electronic Diversity Visa (eDV)

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 the responsibility of the applicant and the contract staff or Department personnel to validate the correctness of the information before submission into eDV and further processing.

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) and
- 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.

eDV collects the minimum amount of information necessary to perform its duties of providing a web application for visa applicants to enter their own personally identifiable information (PII). This reduces costly data entry errors and provides a better method for preventing duplicate applications, enhancing the integrity of the data and reducing privacy risk.

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 and formal certification and accreditation (C&A). 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 eDV.

4. Uses of the Information

a. Describe all uses of the information.

The only use of PII data by eDV is for the purpose of communicating with the visa applicants.

There are three distinct phases of EDV's operation. During Phase I the EDV system resides at an Internet Service Provider (ISP) in Ashburn. The ISP, through a Service

Electronic Diversity Visa (eDV)

Level Agreement (SLA), provides the facility, network environment support, and bandwidth capacity.

During Phase II the prepared data in Ashburn becomes available to the Kentucky Consular Center (KCC) users through a secure socket layer (SSL) connections. The KCC local area network (LAN) does connect to OpenNet.

During Phase III a copy of the EDV Database is transferred to KCC to support Visa Operations and the visa adjudication process.

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

The eDV does not analyze PII data and 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 eDV 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 eDV is a government owned system. Government personnel are primary users of eDV. 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.

Appropriate use of the information is regulated by automated controls in the eDV system. Instruction for use of the system is periodically refreshed and re-issued. The eDV system does not provide a flexibility of features that might initiate a functional vulnerability creep or threat.

5. Retention

a. How long is information retained?

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 (NARA).

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

Electronic Diversity Visa (eDV)

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 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 eDV information is shared with Department of State consular officers who may be handling a legal, technical or procedural question resulting from an application for an immigrant visa.

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. 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?

eDV does not share any information with external organizations.

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

NA

Electronic Diversity Visa (eDV)

c. No information is shared outside of the Department of State. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

eDV information is shared with U.S. government systems 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) immigrant visa application 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.

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

Information is given voluntarily by applicants and with their consent, by a 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.

Electronic Diversity Visa (eDV)

- 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?**

Applicants 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 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 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 eDV is considered a visa record subject to confidentiality requirements under INA 222(f).

Visa applicants may change their information at any time prior to submission of the application 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 9 FAM 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.

eDV 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 FOIA or the Privacy Act, as appropriate.

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

Electronic Diversity Visa (eDV)

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 eDV 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 eDV.

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 eDV 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 eDV 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.

Electronic Diversity Visa (eDV)

- 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?**

eDV 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 eDV 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 eDV 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, eDV was certified and accredited for 36 months to expire on May 31, 2011.