Electronic Diversity Visa System (eDV)

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: February 16, 2011

b. Name of system: Electronic Diversity Visa System

c. System acronym: eDV

d. IT Asset Baseline (ITAB) number: 722

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 natives of specific "low admission" countries through a process known as the Diversity Visa (DV) Lottery Program.

The congressionally mandated Diversity Immigrant Visa Program is administered on an annual basis by the Department of State and conducted under the terms of Section 203(c) of the Immigration and Nationality Act (INA). Section 131 of the Immigration Act of 1990 (Pub L. 101-649) provides for a class of immigrants known as diversity immigrants. Section 203(c) of the INA provides a maximum of 55,000 Diversity Visas (DVs) each fiscal year to be made available to persons from countries with low rates of immigration to the United States. The annual DV program makes visas available to persons meeting simple, but strict, eligibility requirements. A computer-generated, random lottery drawing chooses selectees for DVs. The visas are distributed among six geographic regions, with a greater number 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 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 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 gathers only 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.

f. Reason for performing PIA:

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

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

h. Date of previous PIA (if applicable): September 10, 2009

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 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 are U.S. 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:

- Names of individuals
- Birthdates of individuals
- Financial account numbers of individuals
- SSN or similar foreign personal identifying numbers (e.g., national IDs, country specific IDs)
- Address / phone or similar information
- Email address of individuals
- Images or biometric IDs

Information on the applicant may also include information of U.S. citizens when using the online electronic Diversity Visa (e-DV) web application. The data is then transferred to eDV for use in the lottery.

b. How is the information collected?

The information is collected online by the applicants using the electronic Diversity Visa (e-DV) web entry forms. Users can enter their information into a secure web site operated by CA staff.

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 through the diversity visa program. Each element of PII is necessary to establish the identity of the applicant, determine whether eligibility requirements are met, to send communications to the applicant and/or his or her legal representative, and to detect and prevent fraudulent applications from being approved.

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).

d. How will the information be checked for accuracy?

Required fields must contain an entry format 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 an immigrant visa application is the responsibility of the applicant.

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 eDV system collects the minimum amount of personally identifiable information necessary as part of the U.S. diversity visa lottery and application process.

The primary risk is misuse by Department employees and contractors. Misuse of PII could result in a delay in processing diversity visa applications, approving applicants who are not eligible and denying applicants who are eligible. Misuse could also result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress for individuals whose PII is compromised, in addition to administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State. The opportunities for the misuse of PII and

the serious impact that it would have on applicants and the integrity of eDV makes the misuse of PII a high risk.

The Department of State seeks to address these risks by minimizing the collection and transmission of PII to the minimum required to perform the business functions required of eDV. 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.

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 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 reliable method for preventing duplicate applications.

The only use of PII data in eDV is to establish the identity of the applicant, determine whether eligibility requirements are met, to send communications to the applicant and/or his or her legal representative, and to detect and prevent fraudulent applications from being approved. Immigrant visa lottery applicant records are routinely retrieved using name, date of birth, place of birth, case numbers or applicant IDs automatically generated by Oracle, to retrieve applicant data.

Controls prohibit use of eDV PII through: (i) placement on portable computers or portable storage devices; (ii) remote access to files or databases containing eDV PII, including telecommuting arrangements and extension of online access to other government agencies; and (iii) the creation of computer-readable extract of PII from databases intended to be accessed remotely or to be physically transported outside the Department’s secured physical perimeter on removable media or on portable/mobile devices.

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

PII data is not analyzed in eDV; no new information is produced. eDV primarily collects and maintains information on foreign nationals as part of the U.S. diversity visa lottery and application process. The PII collected and maintained by eDV is not an ingredient in any data mining activity as defined by federal law. Finally, the PII validation process does not occur within eDV; however, validation does occur in the Diversity Visa Information System (DVIS) which has been assessed under its own PIA.

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

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

d. Are contractors involved in the uses of the PII?

eDV is a government-owned system. Government personnel are the primary internal users of eDV. 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 have become part of the signed contract. Each contractor employee is required to attend mandatory briefings that cover the handling of classified and other such information prior to working on the task.

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 eDV performs basic internal analytical functions on the application 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.

All internal users, including contractors, are screened prior to their employment with the Department of State or with their respective agency. The Bureau of Diplomatic Security (DS) 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.

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.

The internal 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.

In addition, technical system security controls are in place as described in Section 3(f) above.

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 with the published record schedules of the Department of State and the National Archives and Records Administration (NARA), specifically General Records Schedule (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 eDV 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.

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?

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. The eDV also has interconnections with the following Bureau of Consular Affairs (CA) systems:

Interfacing System and Description	Type of Connection	Type of Data And How It Is Shared
Consular Consolidated Database (CCD): The CCD system is an extremely large data warehouse residing at SA-26 and SA-1 that holds 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.	One-way: from eDV to CCD	eDV connects to CCD for sole purpose of production data replication.
Diversity Visa Information System (DVIS): 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 U.S. 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 runs through facial recognition software, packaged and sent to DVIS via files stored in directory made accessible to DVIS.	One-way: from eDV to DVIS	An eDV user flags cleared applications/cases and converts the files into XML format. An automated process runs every night to collect all cleared applications/cases and put it into a zip file. DVIS system administrators log in 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.

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. Users of DVIS log in to Batch Transfer Services (BTS) (mentioned in the chart above) to extract or download relevant information from eDV to DVIS. 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.

The risks associated with sharing privacy information internally 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. To combat the misuse of information by personnel, numerous management, operational and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure, including, but not limited to, annual security training, separation of duties, least privilege, personnel screening, and auditing.

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 Department of State regulations.

eDV 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 and 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?

eDV information is not shared with any external agencies.

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

eDV information is not shared with any external agencies.

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

eDV information is not shared with any systems external to the Department of State. Even so, any potential 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.

- 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 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 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 (SORN) titled Visa Records, State-39.

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

Information is given voluntarily by the applicant or 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 to obtain 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?

Information is given voluntarily by the applicant or by 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.

Notice is given to individuals as described in Section 8(a) above. eDV 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 explains how the information may be used by the Department and how it is protected.

Access to eDV records is restricted to cleared, authorized Department of State direct hires and contractor personnel. eDV 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 eDV is considered a visa record subject to confidentiality requirements under INA 222(f). eDV 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.

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:

- Correspondence previously sent to or given to the applicant by the post;
- Civil documents presented by the applicant; and
- 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.

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 eDV may be covered by 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 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?

Internet-based end-user (applicant) access is only restricted by the end-user's ability to access the Internet and have the appropriate version of an Internet browser that can support 128-bit encryption. Internet-based end-users (applicants) all have the same level of privilege by design, which is strictly data entry.

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. 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 user's supervisor is the administrator for creating and modifying eDV accounts and grants 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 refresher 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 cybersecurity and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Internal 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.

No such residual risk is anticipated. Moreover, several steps are taken to reduce residual risk related to system and information 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 involve privacy risk?

eDV does not employ any technology known to elevate privacy risk. All known vulnerabilities identified by the industry related to eDV technologies have been mitigated. All new vulnerabilities identified in the future will be patch and fix during the regular monitor process.

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, the current eDV safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

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

The 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. The Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk and has 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, eDV was certified and accredited for 36 months in April 2008. Its Authority to Operate (ATO) will expire on May 31, 2011. The eDV full C&A process is underway as of this writing.