PRIVACY IMPACT ASSESSMENT

Electronic Diversity Visa (eDV)

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: March 2022
(b) Name of System: Electronic Diversity Visa
(c) System acronym: eDV
(d) Bureau: Consular Affairs (CA)
(e) iMatrix Asset ID Number: 722
(f) Child systems (if applicable) iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The eDV system supports the implementation of the Diversity Immigrant Visa Program, also known as the DV Program, which is administered on an annual basis by the Department of State (Department) in accordance with section 203(c) of the Immigration and Nationality Act (INA) of 1952, as amended. The eDV system is a public facing

website which public users access via https://dvprogram.state.gov, to enter data required to apply for the program, as well as to check the status of entries.

The eDV system supports the replacement of paper applications for the DV Program with an electronic application process based on web technology and the Internet. This is accomplished through the two components of the eDV system: the Applicant Entry System (AES) and the Entrant Status Check (ESC). Potential applicants from all over the world can apply for Diversity Visas (DVs) during the open registration dates specified on the site. A computer-generated, random drawing chooses selectees for DVs.

(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 Immigrant Visa Program 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 lawful permanent residents (LPR), they are not covered by the provisions of the Privacy Act.

The eDV entrant PII collected includes:

- Name of individual
- Date of birth
- Phone number
- Mailing Address
- e-mail address
- Pictures
- Images/Biometric IDs
- Gender
- Place of birth (City & country of birth)
- Education
- Nationality
- Employment
- Family Information
- Current Marital Status & Spouse information
- Number of Children (all: natural, adopted, stepchildren, etc.)

An eDV record may include PII of persons associated with the Diversity Visa applicant, such as a derivative spouse or child of the entrant, who are U.S. citizens or lawful permanent residents (LPRs) who are covered by the Privacy Act. While entrants are not required to submit information about U.S. citizen or LPR spouses or children, some do so. The U.S. citizen or LPR PII may consist of:

- Name, date of birth, city and country of birth, address, gender, pictures of U.S. citizen family members (e.g., spouse and children) and the

relationship to applicant.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
8 U.S.C. 1153(c) Allocation of Immigrant Visas – Diversity immigrants
22 U.S.C. 2651a (Organization of Department of State)
22 C.F.R. Parts 42.33

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

☒Yes, provide:
SORN Name and Number: Visa Records, STATE-39
SORN publication date: November 8, 2021

☐No, explain how the information is retrieved without a personal identifier.

(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 Office 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 (Consolidate as much as possible):

Schedule number: B-09-002-2b: Intermediary Records
Disposition Authority Number: DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)
Length of time the information is retained in the system: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
Type of information retained in the system: Immigrant Visa, Non-immigrant Visa, and Consular Consolidated Database hard copy and electronic input records, including applications, supplemental questionnaires, refusal worksheets and supporting or related documentation and correspondence, relating to persons who have been refused immigrant or nonimmigrant visas (including quasi-refusals), under the following section(s) of law: INA subsections 212(a)(1)(A)(i), (iii), and (iv); (2); (3); (6)(C), (E), and (F); (8); (9)(A) (if alien convicted of an aggravated felony), and (C); and 10(D) and (E); 222(g); Title IV of the Helms-Burton Act (22 USC 6021 et seq.); any cases requiring the Department's opinion code00 (Except quasi-refusal cases under (6)(C)(i)); INA subsection 212(a)(10)(C); Quasi-Refusals under 212(a)(6)(C)(i); 212(a)(9)(B); INA subsection

212(f); and Section 5(a)(1) of the Tom Lantos Block Burmese JADE (Junta's Anti-Democratic Efforts) Act of 2008.

Also includes output records such as ad hoc and other reports that contain summarized or aggregated information created by combining data elements or individual observations from a single master file or data base.

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) On what other entities above is PII maintained in the system?

☒ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☐ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

The information in paragraph 3(d) above is collected online from the entrants using the electronic Diversity Visa (eDV) web entry.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Accuracy of the information in the eDV system is the responsibility of the applicant applying for the diversity visa. After initial data are collected via the eDV system,

consular representatives review the record to verify the completeness of the information. 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 dropdown lists of available choices.

Information is also verified during the interview process if the applicant is selected for the DV program.

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

The data in the eDV system are current as of the date the applicant submits his/her application for the DV program. If the individual is selected for the program, the information is validated during the interview to ensure that it is current. If the entrant is not selected, the information is no longer processed and is disposed of in accordance with the record disposition schedules.

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

No, eDV does not use commercial sources of information nor is the information publicly available.

(i) How was the minimization of PII in the system considered?

The PII items listed in Question 3d are the minimum necessary to perform the actions required by the eDV system. Concerns about collecting and maintaining PII include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the eDV system to perform the intended function of supporting the diversity visas program.

5. Use of information

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

The PII in the eDV system is used 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.

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

Yes.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

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

(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

(d) If the system will use test data, will it include real PII? ☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal: The term "internal sharing" traditionally refers to the sharing of information within the Department of State, but external to the owning organization (referred to as "bureau" at the Department of State). However, since the various Bureau Consular Affairs offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau. The eDV system shares information with the CA Consular Consolidated Database (CCD).

External: The eDV system does not share information externally. However, PII in the eDV database may be shared externally in connection with fraud investigations, law enforcement requests, or counterterrorism and border security efforts via other methods outside of eDV. Requests for eDV information must go through the Consular Affairs Visa Office and in turn the eDV information may be shared with the Department of Justice (DoJ), Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), or Federal Agencies in the Intelligence Community for use by personnel with an official need to know.

(b) What information will be shared?

Internal: Information addressed in paragraph 3d is shared internally with the CA CCD system.

External: Potentially all of the information contained in the eDV database may be shared with the Department of Justice (DoJ), Department of Homeland Security (DHS),

the Federal Bureau of Investigation (FBI), or Federal Agencies in the Intelligence Community for use by personnel with an official need to know.

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

Internal: The eDV PII in paragraph 3d is shared with the CA CCD system to process diversity visa requests by verifying applicant information, conducting the visa program drawing, and to adjudicate diversity visa applications.

External: PII in the eDV system may be shared externally in connection with fraud investigations, law enforcement requests, or counterterrorism and border security efforts via other methods outside of eDV.

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

Internal: All eDV information is shared internally database to database and is encrypted using SecureSocket Layer (SSL) and transport layer security (TLS).

External: The eDV system does not transmit data externally with external agencies. Any eDV information shared with external agencies is downloaded from the AES by a Consular Systems and Technology (CST) team. The eDV information is provided to the external agencies via encrypted email or downloaded to a DVD or other appropriate medium, encrypted, and then securely provided to an authorized representative of the external agency.

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

Internal: The eDV system safeguards entail secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS)) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior outlined in the security controls for each major application, including eDV. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In addition, Department employees must have a Personal Identity Verification/Personal Identification Number (PIV/PIN), as well as a separate password to access eDV data.

External: eDV PII data moved from the AES to the CCD are shared with external agencies via the CCD where safeguards for external sharing are handled in CCD. Data shared with other government agencies are carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency. Manual reports are emailed using digital signature and encryption.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, the eDV contains the following confidentiality statement: The information requested is pursuant to Section 222 of the Immigration and Nationality Act. 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.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?
If no, why are record subjects not allowed to provide consent?

Information is given voluntarily by consenting applicants. Individuals who voluntarily apply to enter the Diversity Visa program are notified on the application that failure to provide requested information may result in their application being rejected for consideration in the diversity visa program.

(c) What procedures allow record subjects to gain access to their information?

The eDV site provides a link to travel.state.gov, which includes information and procedures regarding access to information. Applicants can contact the U.S. Embassy, Consulate or the Kentucky Consular Center (KCC) for assistance to access their information. Applicants are not able to access the data via the eDV program entry website once submitted.

Additionally, System of Records Notice (SORN) STATE-39 Visa Records provides information and organization points of contact regarding questions and procedures to access information for U.S. persons.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Applicants can contact the U.S. Embassy, Consulate or the Kentucky Consular Center (KCC) for assistance to update their information. The entrants are not able to update the data submitted through eDV. However, if they are selected for the DV Program, they can change data by using the Department of State Form DS-260. The KCC notes

the changed information in DVIS, which is forwarded to Pre-Immigrant Visa Overseas (IVO) for review at Post during the interview. Applicants can also update information during the interview process.

SORN STATE-39, "Visa Records", also includes procedures for U.S. persons on how to contact an office for assistance about the existence of records pertaining to the individual.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

The eDV site provides a link to travel.state.gov, which includes information and procedures regarding contacting the U.S. Embassy, Consulate, or the Kentucky Consular Center (KCC) for assistance to correct information.

8. Security Controls

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

The eDV system is secured within the Department of State intranet which mitigates risk factors through defense-in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring.

The eDV system is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable NIST 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need to perform official duties.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Access to the eDV system is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. Department of State eDV users, system administrators, database administrators and public users have access to eDV based on prescribed roles to conduct required business and assigned roles to support the management and execution of the diversity visa program.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Separation of duties and least privilege access are employed; users have access to only the data that the supervisor and local Information System Security Officers (ISSOs) approve to perform official duties. Access is role-based, and the user is granted only the role(s) required to perform officially assigned duties.

Least privileges are restrictive rights/privileges or access users need for the performance of specified tasks. The Department of State ensures through least privileges principles that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) necessary to perform their job duties. Users are uniquely identified and authenticated before accessing PII.

(d) How is access to data in the system determined for each role identified above?

Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information to perform official duties. Access to eDV system information is further protected with additional access controls set at the database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer.

Access to data of user roles listed in 8(b) is based on the position, role, and need to perform officially assigned duties as described. Supervisors and the local ISSO must approve access to the eDV system based on the specific role and level of security of information and personnel. Once personnel leave the project, their access to the eDV system is terminated.

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

The eDV system CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides, conduct annual control assessments (ACA) to ensure systems comply and remain compliant with Department of State and federal policies.

Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's applications for changes to the Department of State mandated security controls. Access control lists on OpenNet servers and devices along with Department of State Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures.

In accordance with Department of State Configuration Guides, auditing is enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;

- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

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

☒Yes ☐No

The eDV System Security Plan (SSP) contains the procedures, controls, and responsibilities regarding access to data in the system.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially.

The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.