PRIVACY IMPACT ASSESSMENT

Electronic Diversity Visa (eDV) System

1. Contact Information

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

2. System Information

(a) Name of System: Electronic Diversity Visa (eDV) System

(b) Bureau: Consular Affairs (CA)

(c) System Acronym: eDV

(d) iMatrix Asset 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 Fall 2018.

(c) Describe the purpose of the system:

The eDV system supports the implementation of the Diversity Immigrant Visa Program, also known as the DV Lottery Program or "lottery", which 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. The eDV system is a public facing website which public users access via https://dvlottery.state.gov to enter data required to apply for the lottery program, as well as to check the status of their entry.

The eDV system supports the replacement of paper applications for the DV Lottery 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 lottery drawing chooses selectees for DVs.

Instructions on how to fill out the lottery entry form are given on a separate website, travel.state.gov. No user IDs or passwords are issued to public users. Once a public user submits an entry form, they are issued a confirmation number; this number is used when the entrant accesses the Entrant Status Check on the eDV site to allow them to see their lottery selection notification disposition. The system does not allow the applicant to subsequently read, modify, or delete the submitted 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 (LPR), they are not covered by the provisions of the Privacy Act.

The eDV entrant PII collected includes:

- Name of Individual
- Birthdate of Individual
- Phone number(s) of Individual
- Mailing Address
- e-mail address of individual
- Images or Biometric IDs
- Gender
- City & country of birth
- Education
- Nationality
- Employment
- Current Marital Status & Spouse information
- Number of Children (all: natural, adopted, stepchildren, etc.)

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 (LPRs) 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, date, city and country of birth, gender, 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. 1104 (Powers and Duties of the Secretary of State);
- 8 U.S.C. 1101-1363a (Titles I and II of the Immigration and Nationality Act of 1952, as amended);
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 22 U.S.C. 2651a (Organization of the Department of State);
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports)

(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): June 15, 2018

☐ 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-09-002-2b: Intermediary Records

Description:
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.

Disposition:

Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

DispAuthNo: DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)

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 (are US citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

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

☐ Yes

☐ No

☒ N/A – SSNs are not collected

- If yes, under what authorization?

(c) How is the information collected?

The information in paragraph 3(d) above is collected online from the entrants using the electronic Diversity Visa (eDV) web entry. For those entrants who are selected, further information is collected via a secure website operated by the Bureau of Consular Affairs (CA), the Consular Electronic Application Center (CEAC) using the online Department of State Form 260, Application for Immigrant Visa and Alien Registration. (Note CEAC is not within the boundary of eDV). Data is also transferred (database to database) from the Diversity Visa Information System (DVIS) to ESC for the purpose of uploading cleared potential lottery winners and notifying selectees of their interview appointment information.

(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?

After initial data is collected via the eDV, a consular representative reviews 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 during the lottery process.

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

The data in eDV is current as of the date the applicant submits his/her application for the lottery program. If the individual is selected for the lottery, the information is validated during the interview to ensure that it is current. If the lottery entrant is not selected, nothing further happens and the information is no longer processed and is disposed of in accordance with the record disposition schedules.

(g) Does the system use information from commercial sources? Is the information publicly available? No, the system does not use information from commercial sources nor is it publicly available.

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

Yes, the eDV contains a 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. 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 his/her consent, by his/her legal representative. 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 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?

The personally identifiable information (PII) collected for the eDV lottery is the minimum necessary to perform the functions of the Diversity Visa Lottery. During the design of the eDV information system, the capability for applicants to input U.S. citizen or Legal Permanent Resident (LPR) data was included, although this information is not required. Because U.S. citizen or Legal Permanent Resident (LPR) data can be included as part of this process, a PIA has been created to show how the eDV PII is handled.

All PII is protected equally within the eDV information system. Concerns 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 systems to perform the functions for which they are intended

5. Use of information

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

The PII in eDV 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. Immigrant visa lottery entrant records are routinely retrieved using the name, date of birth, and confirmation numbers that are automatically generated by the 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?

Yes. The use of the PII data within the eDV information system is utilized for the purposes for which the system was designed: to support the implementation of the Diversity Immigrant Visa Lottery Program.

(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.

Internal: eDV shares information with the Diversity Visa Information System (DVIS), and the Consular Consolidated Database (CCD). These are **internal** systems used by Department of State personnel working domestically and overseas in connection with processing diversity lottery immigrant visa applications.

DVIS: Data is transferred (database to database) from AES for the purpose of creating case records of potential selectees in DVIS. Data is also transferred (database to database) from DVIS to ESC for the purpose of uploading cleared potential lottery winners and notifying selectees of their interview appointment information.

CCD: CCD connects (database to database) to eDV for production data transfer of the application information from AES into the CCD. CCD replicates data allowing posts to view information in support of Consular Affairs operations.

External users:

The information in the eDV database may occasionally be shared externally in connection

with fraud investigations or law enforcement requests. Requests for eDV information must go through the Consular Affairs Visa Office and in turn may be shared with the Department of Homeland Security (DHS) or the Federal Bureau of Investigation (FBI) personnel with an official need to know.

(b) What information will be shared?

The shared information may be any of the data types listed in paragraph 3(d) above to either internal and external agencies or law enforcement entities.

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

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

The eDV information occasionally shared externally is in connection with fraud investigations or law enforcement requests.

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

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

eDV is not involved in external transmission or data sharing by automated means. 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. The approved requested data is provided via encrypted email or 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?

Internal sharing: Internal recipients within the Department of State are required to comply with U.S. government requirements for the protection and use of PII. These safeguarding requirements include, but are not limited to, security training and following internal Department policy for the handling and transmission of "Sensitive but Unclassified" information. In addition, all Department users are required to complete the annual security awareness training to reinforce safe handling practices. Defense in depth is deployed as well as role based access based on least privilege. Audit trails track and monitor usage and access.

External sharing: Any eDV data that is shared externally is done through queries by the CCD Reporting team using the replicated data that resides on the CCD. Since eDV data

is shared via CCD, safeguards for external sharing are handled in CCD. Data shared with other government agencies is 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.

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

Privacy concerns regarding the sharing of information focuses on two primary sources of risk:

(1) Accidental disclosure of information to non-authorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

(2) Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other.

Both of these risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know and clearance level.

- System authorization and accreditation process along with continuous monitoring Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All CCD communications shared with external agencies are encrypted as per the Department of State's Security Configuration Guides' security policies and procedures.

7. Redress and Notification.

(a) What procedures allow individuals 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 lottery entry website once submitted.

For any information on U.S. citizens, the Privacy Act System of Records Notice (SORN), Visa Records, State-39, and rules published at 22 FR 171 provide information to individuals on how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record.

(b) Are procedures in place to allow an individual 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, they are able to change data by using the form DS-260. In this case, 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 their information during the interview process.

If no, explain why not.

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

Individuals are notified of the procedures to correct records in the eDV system by a variety of methods:

1. During their Diversity Visa interview
2. Instructions on forms and web pages (or links to Agency Privacy Policy)
3. Being notified by letter that a correction is needed
4. Published SORNs provide procedures for U.S. citizens.

Each method contains information on how to amend records and with whom/what office to communicate as well as contact information.

8. Security Controls

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

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

Internal access 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. All administrative accounts for the system must be approved by the both the Government Task Manager (GTM) and the Consular Affairs Information Systems Security Officer (CA ISSO).

CA Systems are configured according to State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (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. Vulnerabilities noted during testing are reported appropriately and are tracked until compliant or acceptably mitigated.

(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.

To access the system, persons must be authorized users of the Department of State's unclassified network, which requires a background investigation and an application approved by the supervisor. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/ Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based and restricted according to approved job responsibilities requiring managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Information System 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.

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

misuse of the information?

The 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 and conduct annual control assessments (ACA) to ensure that all systems/applications 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 major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with Department of State Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

Operating System (OS)-Level auditing for eDV is set in accordance with the Department of State Security Configuration Guides. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. The system log records events logged by the OS interface system components. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

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

In accordance with Department of State computer security policies, mandatory security (PS800 Cyber Security Awareness) and privacy (PA459 Protecting Personally Identifiable Information) training is required for all authorized users. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users electronically acknowledge and agree to the rules and to protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems requires dual factor authentication utilizing PIV/CAC and PIN.

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

The eDV information collected contains PII of foreigners and possibly U.S. citizens / LPRs. Although recourse for each group is different, the PII is protected within the information system in the same manner.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. The security measures are in place to minimize that risk, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above were implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

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/CCD have access to the data.

Internal users: Department of State personnel working domestically and overseas in connection with processing diversity lottery immigrant visa applications. Applications are submitted to the Kentucky Consular Center (KCC) via the eDV internet website. The Diversity Visa Information System (DVIS) is used by Visa KCC personnel to further process applications that pass validations in eDV and the Consular Consolidated Database (CCD).

System & Database Administrators: Consular Affairs/Consular Systems & Technology (CA/CST) system and database administrators connect to the CA Secure and Web enclaves for systems management. System & Database Administrators are responsible for the maintenance, upgrades, patches/hotfixes, software and database configuration. The access of administrators is limited to only those system and database application files necessary to perform daily activities.

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

Access is role based and user is granted only the role(s) required to perform officially assigned duties, which are approved by the supervisor and the ISSO.

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

☒Yes

☐No

Information is documented in the System Security Plan. The Plan includes information regarding system access to data.

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

eDV access is granted in accordance with assigned roles and responsibilities. Access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties based on their roles/job functions. Separation of duties and least privilege is employed and users have access to only the data the supervisor approves to perform official duties.

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

- Access control policies and access enforcement mechanisms control access to PII.

- Separation of duties is implemented; access is role based as required by policy.

- eDV System Administrators and internal users have access to eDV via OpenNet from the Department of State configured workstations. Users must dual factor authenticate utilizing PIV/CAC and PIN to access data. Users are uniquely identified and authenticated before accessing PII and while logged in can be traced to the person who performed the activity.

- Least Privileges are restrictive rights/privileges or accesses of users for the performance of specified tasks. The Department of State ensures 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) that are necessary to perform their job duties.

- System and information integrity auditing are implemented to monitor and record unauthorized access/use of information.