PRIVACY IMPACT ASSESSMENT

DIVERSITY VISA INFORMATION SYSTEM (DVIS)

1. Contact Information

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

2. System Information

(a) Name of system: Diversity Visa Information System (DVIS)
(b) Bureau: Consular Affairs (CA)
(c) System acronym: DVIS
(d) iMatrix Asset ID Number: 17
(e) Reason for performing PIA: Click here to enter text.

☐ 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?

DVIS is currently undergoing an Assessment and Authorization (A&A) with an expected Authorization to Operate (ATO) by Spring 2021.

(c) Describe the purpose of the system:

DVIS supports the State Department's administration of the Diversity Immigrant Visa (DV) program, which promotes immigration from countries with historically low rates of immigration to the United States. The program creates an internet-based "lottery," randomly selects individuals from a pool of eligible entrants, and qualifies them to apply for immigrant visas.

DVIS is used by Department of State personnel to track and validate the number of applications submitted to the DV lottery.

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

The following details what PII is collected on U.S. citizens/Legal Permanent Residents (LPRs) and what is collected on non-U.S. citizens/non-LPRs:

US Citizen PII:

- Name
- Birthdate
- Place of birth
- Gender
- Address
- Petitioner/Legal Representatives' name, organization, business address and phone number.) Petitioner/Legal Representatives can be U.S citizens or non U.S, citizens.

Non-US Citizen PII:

- Name
- Birthdate
- Place of birth
- Phone number
- Nationality
- Passport or other ID numbers
- Personal address
- Email address
- Photos (DVIS contains photos of applicants; however facial recognition does not take place in DVIS.)

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

- 8 U.S.C. §§ 1101-1363a (Titles I and II of the Immigration and Nationality Act of 1952, as amended);
- 8 U.S.C. § 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C. § 2651a (Organization of the Department of State);

- 22 C.F.R. Parts 40-42, and 46 (Visas)

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

☒Yes, provide:

- SORN Name and Number: Visa Records, STATE-39, June 15, 2018

☐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:

- Schedule number Department of State Records Disposition Schedule:

B-09-002-40a: Diversity Visa Applicant Control System
Description: This on-line tracking and case management system maintains a data base of immigrant visa applicants who have applied for entry into the United States under the Diversity Visa Program. Master on-line file.
Disposition: Destroy when active use ceases.
DispAuthNo: N1-084-97-04, item 1a

B-09-002-40b: Diversity Visa Applicant Control System
Description: This online tracking and case management system maintains a data base of immigrant visa applicants who have applied for entry into the United States under the Diversity Visa Program. Off-line paper printouts of Immigrant Visa Workload Monthly Report (OF-186).
Disposition: Destroy when 2 years old.
DispAuthNo: N1-084-97-04, item 1b

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

- If yes, under what authorization?

(c) How is the information collected?

Applications for the DV program are submitted via the internet through the Electronic Diversity Visa (eDV) Applicant Entry System (AES). The applicant or petitioner completes the diversity application (Department of State (DS) Electronic Diversity Visa Entry Form (DS-5501)) via the eDV-AES for the lottery selection pool. (Note: eDV is not within the boundary of DVIS). DVIS is not accessed directly by the public.

(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?

A consular representative reviews the information provided on the Electronic Diversity Visa Entry Form (DS-5501) against the documentation provided by the applicant, in addition to information contained in other CA systems to verify the accuracy of the information entered. These CA systems include: electronic Diversity Visa Application Entry System (eDV/AES); Consular Consolidated Database (CCD); Immigrant Visa Information System (IVIS); Immigrant Visa Allocation Management System (IVAMS); and Overseas Consular Support Applications (OCSA)-Immigrant Visa Overseas System (IVO).

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

The applicant is responsible for ensuring that the information on the DS-5501 application form is current at the time of submission via eDV-AES, which is transmitted to DVIS. Those data are current as of the date of the lottery entry.

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

No, DVIS does not use commercial or publicly-available information.

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

DVIS is not a public-facing system nor does it collect information directly from applicants. The information is collected by eDV-AES which transfers information to DVIS.

A confidentiality statement pursuant to Section 222(f) of the Immigration and Nationality Act, (INA) is on the eDV website where the lottery application (DS-5501) information is being collected. eDV is outside the boundary of DVIS.

(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?

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

DVIS is not accessed by applicants and the data contained are collected from other systems that would provide the notice and obtain consent at the collection point.

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

The DVIS PII elements listed in Question 3d are the minimum necessary to perform the actions required by this 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 system to perform the functions for which it is intended.

5. Use of information

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

The intended use of the PII data in DVIS is to support the State Department’s Diversity Visa Program, by tracking the processing of actions for the diversity IV applications submitted.

(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 system was designed to support the State Department’s Diversity Visa Program. The collection is related to diversity visa application submissions, processing, and approval/denial decisions.

(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? N/A

(2) Does the analysis result in new information? N/A

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

With that understanding, information in the DVIS system will be shared internally with the following CA systems: electronic Diversity Visa Application Entry System (eDV/AES); Consular Consolidated Database (CCD); Immigrant Visa Information System (IVIS); Immigrant Visa Allocation Management System (IVAMS); and Overseas Consular Support Applications (OCSA)-Immigrant Visa Overseas System (IVO). All of these are **i**nternal systems used by Department of State personnel working domestically and overseas in connection with processing diversity immigrant visa applications.

No information is shared externally.

(b) What information will be shared?

All information listed in paragraph 3(d) above is shared.

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

The purpose for sharing the information is to manage and track the Diversity Immigrant Visa applications.

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

The information is shared by secured internal connections (database to database) with other consular systems (CCD, IVO, IVIS, IVAMS, eDV/AES), and email. All of these activities and systems reside on the Department's secure intranet network, OpenNet. All physical records containing PII are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only and are not used for transmission.

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

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 biennial privacy and 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.

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

Privacy concerns regarding the sharing of information in these systems 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 risks of accidental disclosure of information.

2) Deliberate disclosure/theft or information to non-authorized parties regardless whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification. All users must also sign a user agreement.

2) Strict role -based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level

3) System authorization and accreditation process along with continuous monitoring via a 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.

4) All communications shared with external agencies are encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

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

Applicants do not have access to their information in DVIS because applications are submitted via the CA eDV system. Procedures for access and redress are provided by the eDV source system in which the the information is entered. The System of Records Notice (SORN) Visa Records, State-39 and rules published at 22 CFR 171 also provide information on how individuals can inquire about the existence of records, how to request access to the records, and how to amend records.

In addition, procedures are published on the Department of State public web site Travel.State.Gov which provides contact information for the Kentucky Consular Center (KCC) which assists diversity entrants with questions.

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

☒Yes ☐No

If yes, explain the procedures.

After the case records are sent to overseas posts for further processing of candidates selected for the program, applicants have opportunities to update or correct information through correspondence with post and at the formal interview for the visa. In addition, as published on travel.state.gov, KCC processes the cases and applicants are able to contact KCC directly. If KCC notices discrepancies in the data, KCC contacts the applicants. The applicants are notified by email to check Electronic Diversity Visa/Entrant Status Check (eDV/ESC). eDV/ESC displays their appointment letter which indicates their post assignment, the post address, and interview day/time. After that time, they are able to contact post.

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 these systems by a variety of methods:

1. During their visa interview
2. Published SORN State-39, Visa Records
3. Instructions on forms and web pages (or links to Agency Privacy Policy)
4. Being notified by letter that a correction is needed

Each method contains information on how to amend records and contact information.

8. Security Controls

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

The system is secured within the Department of State intranet 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.

Access to DVIS is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user’s supervisor and the local Information System Security Officer. The audit vault is used to monitor all privileged access to the system and any violations are reported to senior management. All physical records containing PII are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only.

DVIS is configured according the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes 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 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 DVIS, 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 and the local Information System Security Officer. Each authorized DVIS 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 DVIS is role-based, and restricted according to approved job responsibilities and requires managerial concurrence. 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.

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

Various controls are in place to deter, detect, and defend against the misuse of personally identifiable information. The CA System Manager and CA ISSO, in conjunction with the CA Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides. They also 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 Department of State-mandated security controls.

Access control lists on all Department of State servers and devices along with State Department 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.

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.

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

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 the systems. Additionally, Department of State civilian employees are required to take the course Privacy Act (PA459, Protecting Personally Identifiable Information) biennially. The Department’s standard “Rules of Behavior” regarding the use of any computer system and the data it contains require that users sign that they agree to the rules 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 Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit are 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 or data manipulation. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

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

Consequences of breached or exposed PII may include inconvenience, distress, damage to standing or reputation, financial loss to the Department or individuals, harm to Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation. The security measures listed above in paragraphs 8a-e are implemented to secure the data in DVIS in accordance with federal laws and policies, including Department policies.

9. Data Access

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

State Department personnel (i.e., System Administrators, Database Administrators and DVIS Users) have access to the system and the data.

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

Access is determined based on requests which are submitted and approved by the supervisor and the local ISSO. Access is role-based and the user is granted only the role(s) required to perform officially-assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Procedures and controls are documented in the DVIS System Security Plan.

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

Separation of duties and least privilege are employed and users have access to only the data that the supervisor and the local ISSO approves to perform official duties.

System Administrators
System administrators are authorized to access DVIS for the purpose of performing maintenance, troubleshooting technical issues, installing software and patches, and other actions needed to keep DVIS operational. System Adminisrators have access to all data. They have logon identifications associated with their name for the purpose of auditing.

Database Administrators
The access of database administrators is limited to only those Oracle application files necessary to perform daily activities. Database Administrators can see all of the information in DVIS, but they are limited to specific roles. This limit of access and roles is controlled through the use of access control lists (ACLs) as established by the system administrators.

DVIS Users
User access controls determine how, when, and where DVIS users will gain access to the system. DVIS users are assigned to various roles that allow them to perform duties commensurate with the employee's job function. Following are examples of the DV user group roles within DVIS: data entry, case view, problem resolution, pre-entry duplicate user, operations personnel, and security manager. All DVIS users can see the information in DVIS. However, DVIS users are assigned only specific functions that they can perform based on their position and job.

Once a user is properly identified and authenticated by the system, the user is authorized to perform all functions commensurate with the user's job requirements. In an effort to restrict users to only these required functions, DVIS employs logical access controls in accordance with the concept of separation of 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.

-Least Privileges is implemented, which restricts rights/privileges or accesses needed by 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.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN). Activities while logged in can be traced to the person who performed the activity. Users are aware of this by reading and clicking ‘I agree’ to the logon banner.