

DVIS PIA

1. Contact Information

A/GIS/IPS Director
 Bureau of Administration
 Global Information Services
 Office of Information Programs and Services

2. System Information

- (a) **Name of System:** Diversity Visa Information System
- (b) **Bureau:** Consular Affairs (CA)
- (c) **System Acronym:** DVIS
- (d) **iMatrix Asset ID Number:** 17
- (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?**

In December 2014, DVIS received a 12-month Authorization-To-Operate (ATO) that is contingent upon certain conditions being met by June 2015. If the conditions are met, the ATO will be extended to 2017. The system is currently undergoing a Streamlined Target Assessment (STA) for the controls impacted by the NIST SP 800-53 Revision 4.

(c) **Describe the purpose of the system:**

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

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

- Names of individuals
- Birthdates of individuals
- Phone numbers of individuals
- Business addresses
- Personal addresses
- Email addresses
- Images or biometric IDs

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

- 8 U.S.C. 1153(c) Diversity Immigrants
- 8 U.S.C. 1151(e) Worldwide Level of Diversity Immigrants
- 8 U.S.C. 1255(a) Adjustment and Change of Status
- 8 CFR 245.1(a)
- 22 CFR 42.33

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

Yes, provide:

System of Records Notice (SORN) Name and Number:

Visa Records – STATE-39

SORN publication October 25, 2012

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 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.)

Visa applications are retained in compliance with the Visa Lookout Accountability provisions of the Illegal Immigration Reform and Immigration Responsibility Act of 1996 and the records

disposition schedule. The complete disposition schedule for visa records is specified in the U.S. Department of State Records Disposition Schedule, Chapter 09: Consular Records Visa Services and Chapter 14: Visa records, approved by the National Archives and Records Administration.

Consular Records Visa Services

Schedule number (B-09-002-40a)

Length of time the information is retained in the system:

Destroy when active use ceases

Type of information retained in the system:

This on-line tracking and case management system maintains a database of immigrant visa applicants who have applied for entry into the United States under the Diversity Visa Program.

a. Master On-Line File

Consular Records Visa Services

Schedule number (B-09-002-40b)

Length of time the information is retained in the system:

Destroy when two years old

Type of information retained in the system:

This on-line tracking and case management system maintains a database of immigrant visa applicants who have applied for entry into the United States under the Diversity Visa Program.

b. Off-Line paper printouts of Immigrant Visa Workload Monthly Report (OF-186).

Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Schedule number (A-14-001-02c(1)(a))

Length of time the information is retained in the system:

Retain until alien is 90 years of age or older, provided there has been no visa activity for the past 10 years, at which time destroy. (ref. NC1-59-86-2, item 3c1(a) and c1(c)).

Type of information retained in the system:

c. Case files on individual aliens refused a visa.

(1) Cases of living visa applicants.

(a) Cases of applicants refused or presumed ineligible on the basis of Sections 212(a) (1), (2), (3), (4), (5), (9), (10), (12), (13), (19), (22), (23), (27), (28), (29), (31), and (34) of the Immigration and Nationality Act.

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

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

- Yes
 No

N/A as the system does not collect social security numbers.

If yes, under what authorization?

(c) How is the information collected?

The original source of the information collected from the applicants for the Diversity Visa Information System (DVIS) is from the application that is entered into the Electronic Diversity Visa Application Entry System (eDV/AES).

All application data is transferred from eDV to the Consolidated Consular Database (CCD) for staging to facilitate the Integrated Biometric System (IBS) processes of enrolling and searching the data for Facial Recognition (FR). After the data is in CCD, Fraud Prevention Program (FPP) users logon to CCD Web Security (WS) for facial recognition and iCLASS for name matching. The Visa Office determines how many applications from each region are considered for a visa, and a lottery process is run to assign a random ranking to each application. The top ranked applications in each region are imported into DVIS where the Kentucky Consular Center (KCC) personnel review all the preselected applicants.

Based on limits set by the Visa Office, the top ranked cases that passed the review are "Selected" for further processing in the diversity visa process. Case numbers (the Lottery Rank Number, or LRN) for the Selected cases are provided to the Electronic Diversity Visa Entrant Status Check (eDV/ESC) system so that applicants can determine their status. Those that were selected enter additional information into the DS-260 found on the Consular Electronic Application Center (CEAC) website. KCC personnel review the DS-260 information and enter additional or changed information into DVIS.

(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 entry, a second individual reviews the record to verify accuracy of the information entered.

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

The data in DVIS is current as of the date the applicant submits his/her Form DS-260 application for the program.

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

DVIS does not use commercial information, publicly available information or information from other federal agency databases.

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

Yes. The applicant is notified of the following:

1. the purpose for which the information is required
2. the possible uses of the information
3. the possibility that the data may be shared with other organizations/ agencies
4. how the data is protected from unauthorized/ illicit disclosure
5. the potential consequences if the applicant declines to provide the data (i.e., that his/her visa application may be declined).

(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?

At the time applicants complete the visa application, they are notified of their option to decline to provide the required information, and they are advised that to do so may cause the visa request to be denied. Visa applicants are also notified of the relevant privacy implications, such as how the information may be used and shared with other agencies. Visa applicants are not given the option to selectively consent to or deny specific uses of the information. The visa applicant grants complete consent upon signing the application. The applicant's signature constitutes authorization for the U.S. government to use and share the information.

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

Not applicable.

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

The information collected is the minimum amount necessary for the processing of visa applications. The PII is handled in accordance with federal privacy regulations regarding the collection, access, disclosure, and storage of PII.

5. Use of information**(a) What is/are the intended use(s) for the information?**

Information collected and maintained in the DVIS system is used to prepare the case file for the applicant's interview by a consular officer at a U.S. embassy or consulate overseas.

(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 information relates to Diversity Immigrant Visa issues and is required for application processing.

(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?

During the quality check process, the authenticity and the completeness of the information are validated. DVIS does not conduct analysis of or alter the data provided by the applicant.

(2) Does the analysis result in new information?

No new information is produced.

(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.

DVIS interfaces with electronic Diversity Visa (eDV), the Consular Consolidated Database (CCD), and the Immigrant Visa Overseas (IVO) applications, and also shares information with the Immigrant Visa Allocation Management System (IVAMS). All of these are internal systems used by Department of State personnel working domestically and overseas, in connection with processing diversity immigrant visa applications. Certain Department of Homeland Security, U.S. Citizen and Immigration Service (DHS/USCIS) staff have access to DVIS via the CCD.

(b) What information will be shared?

Information to be shared includes personal/biographic information about Diversity Visa applicants, status of applications, and appointment letters for applicants who are selected for further processing.

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

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

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

The information is shared by direct connections with other consular systems (CCD, IVO, CEAC, IVAMS, eDV), and email. All of these activities and systems reside on the Department's secure OpenNet network.

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

Internal recipients, i.e., those 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 attend annual privacy and security awareness training to reinforce safe handling practices. Certain DHS/USCIS staffs also have access to DVIS information via the CCD. These users are subject to the same training and policy requirements for handling PII.

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

Privacy concerns regarding the sharing of information focus on two primary sources of risk: 1) accidental disclosure of information to non-authorized parties, or 2) deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other. 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.

The Department of State mitigates these risks by enforcing rules and requirements regarding:

- 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;
- Strict access control based on roles and responsibilities, authorization and need-to-know;
- Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

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

Applicants do not have access to review or amend their information directly on the system; however, procedures for notification and redress are published in the Privacy Act System of Records Notice (SORN): Visa Records, State-39, and in rules published at 22 CFR 171 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.

(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, applicants have opportunities to update or correct information through correspondence with the post and at the formal interview for the visa.

The applicant may initiate updates to their information when filling out the DS-260. In addition, it is published on travel.state.gov that 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 the Post.

If no, explain why not.

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

Processing Specialists at KCC will identify discrepancies and send out letters to applicants requesting updated or corrected information. Guidance regarding how an individual could initiate contact to make a change is documented in 7(b). Procedures to correct information are published in the Privacy Act System of Records Notice (SORN): Visa Records, State-39, and in rules published at 22 CFR 171 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.

8. Security Controls

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

The DVIS system is secured within the Department of State intranet where risk factors are mitigated through the use of multiple layers of security controls, including management security, auditing, firewalls, and physical security.

(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.

As a matter of policy, the Department of State Chief Information Officer and Information System Security Officer require certain fundamental procedures for all systems. Potential users are

screened and assigned privileges based on their roles, responsibilities and the need-to-know. Specific privileges for a given user are only granted after careful consideration of the user role. There are five types of DVIS user roles: Administrator, Alternate Administrator, Security, Power Users, and View Only. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

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

The security posture will be considered in terms of operations and administration, audits and monitoring, and operational assurance. All system modifications are evaluated to prevent them from detracting or circumventing any established security or assurance controls.

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

In accordance with Department of State computer security policies, DVIS users are required to complete the Cyber Security Awareness Training and the PII Training at least once a year. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users must protect PII through appropriate safeguards to ensure security, privacy and integrity. The following list details just a few of the numerous requirements covered under the "Rules of Behavior" related to PII.

Users are prohibited from the following activities:

- Browsing PII records without authorization or for purposes other than those directly connected with their official work-related responsibilities;
- Disclosing PII to others, including other authorized users, unless there is a need to do so in the performance of official duties;
- Removing PII from the workplace unless it is for an approved work-related purpose;
- Storing PII in shared electronic folders or shared network files;
- Storing PII on any computing device not owned by the government;
- Altering or deleting PII unless the action is part of their official duties and responsibilities.

Users are also required to take the following actions:

- Protect access to all media on which PII is processed;
- Store hard-copy PII in locked containers or rooms;
- Safeguard any PII (electronic or hard-copy) which is removed from the workplace in the performance of official duties;
- Protect against eavesdropping on telephone or other conversations in which PII is discussed.

(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.

DVIS uses data encryption.

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

The Department of State has long been concerned with the protection of individuals' personal information in accordance with U.S. government policies. Visa information and the PII contained therein, constitute the substantive portion of the information contained in DVIS.

9. Data Access**(a) Who has access to data in the system?**

Applicants do not have access to the system data. Only State Department personnel (i.e., System/Web Administrators, Application Administrators and Database Administrators) have access to the system and the data.

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

An individual's job functions/role determines what data he/she may access.

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

Yes

No

CA/CST adheres to a formal, documented audit and accountability policy that addresses purpose, scope, roles, and responsibilities. In addition, there are documented procedures to facilitate the implementation of the policy and the audit and accountability controls.

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

There are five types of DVIS user roles: Administrator, Alternate Administrator, Security, Power Users, and View Only. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. Users will have access based on their roles/job functions.

- **System/Web Administrator**

The System Administrator must first receive his/her Department of State badge and email account. Once received, the Project Manager completes the System Administrator Account Request Form. The Project Manager signs the form authorizing the account to be established /activated and a current System Administrator creates the account. System Administrator accounts are reviewed every 60 days; unneeded accounts are disabled and removed upon review.

- **Application Administrators**

The System Administrators and DVIS Application Administrative users are responsible for establishing, activating, modifying, reviewing, disabling, and removing Application Administrative accounts in the DVIS OpenNet database server. (OpenNet is the Department's unclassified computer network.)

- **Database Administrators (DBAs)**

DBA access is controlled by the Data Integrated Services (IS) team. DVIS DBAs are authenticated using Windows operating system authentication only. The IS Government Technical Monitor GTM is responsible for reviewing and approving accounts. The current DBA activates/establishes an account when he/she adds the new user to the Windows security group. Access is disabled when no longer required; accounts are reviewed every 60 days to determine when access should be disabled.

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

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Audit logs are reviewed at the Application, Database, and System level as follows:

- Application level: DVIS administrators review the application level audit logs as necessary and take the appropriate action if suspicious activity or suspected violations are identified.
- Database level: System Service Operations (SSO) reviews the Structured Query Language (SQL) logs for indications of inappropriate or unusual activity on the DVIS database, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
- System level: SSO reviews the Operating System (OS) logs for indications of inappropriate or unusual activity on the DVIS system, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.