PRIVACY IMPACT ASSESSMENT

Consular Affairs Document Authentication Retrieval and Tracking System (CA-DARTS)

1. Contact Information

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

2. System Information

(a) Name of system: Consular Affairs Document Authentication Retrieval and Tracking System (CA DARTS)

(b) Bureau: Consular Affairs

(c) System acronym: CA DARTS

(d) iMatrix Asset ID Number: 372

(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): Click here to enter text.

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?
CA DARTS is currently undergoing an Assessment and Authorization (A&A) to renew its Authorization to Operate (ATO) status. The estimated ATO date is November 30, 2019.

(c) Describe the purpose of the system:

The Department of State (DoS) is responsible for authenticating documents that will be used abroad by U.S. citizens, commercial organizations, other government agencies, and

foreign nationals. This authentication service is similar to that provided by a notary public in the United States.

The Document Authentication Review Tracking System (CA DARTS) supports the Department of State's mission to authenticate documents. The CA DARTS output is an authenticating certificate that certifies the submitted document adheres to international laws governing trade and other areas. Individuals mail in, email, walk in, or drop off and pick up documents requiring certification by CA DARTS personnel. The document is certified by Government personnel who input only required data in CA DARTS to track and complete the certification process. CA DARTS does not store images of the documents or certificates provided for authentication. CA DARTS authenticate the five (5) types of documents, as listed below:

- Adoption certificates
- Business certificates
- Educational certificates
- Legal certificates
- Marriage certificates

In addition to document authentication, CA-DARTS also supports retrieval, tracking, and return of submitted documents.

CA DARTS does not interface with any other systems internally within the Department of State (DoS) or externally with the public or other organizations.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
Name
Name of Company/Organization
Address
Country
Email Address
Work and Personal Phone Numbers

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
22 CFR Part 92 Notarial and Related Services
22 CFR Part 131 Certificates of Authentication

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
- STATE-26 Passport Records, March 24, 2015
- STATE-39 Visa Records, June 15, 2018
- STATE -05 Overseas Citizens Records and Other Overseas Records, September 8, 2016

☐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 .)

If yes provide:

A-13-004-1: Authentications Office (Authentication Document Authentication Retrieval and Tracking System (CA DARTS)
Description: The CA DARTS application software is used by the Authentications Office to facilitate the document authentication, retrieval, and tracking responsibilities of the office.
Disposition: Temporary: see items 01a(1) through 01d for specific dispositions.
DispAuthNo: N1059-03-10, item 23

A-13-004-01b(1): CA DARTS Master File
Description: Normal Certification. Contains information extracted from documents with authentication requests. Current and previous year data are maintained on-line.
Disposition: Temporary. Cutoff at end of fiscal year. Transfer to archive tape when two years old. Maintain off-line for 3 years or until no longer needed for current business operations, whichever is later. Delete tape upon notification by supervisor.
DispAuthNo: N1-059-03-10, item 23b(1)

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) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No N/A. SSNs are not collected or maintained in CA DARTS.

- If yes, under what authorization?
Click here to enter text.

(c) How is the information collected?
The requester completes the DS-4194, Request for Authentications Services form. The PII obtained from the DS-4194 is manually entered or scanned into CA DARTS by Department of State personnel and/or contract staff. Document authentication requesters do not have access to CA DARTS. The information is maintained in the CA DARTS production environment which resides on the State Department's intranet. The physical paper form DS-4194 is used as a cover sheet for the document(s) submitted by the requester to be authenticated.

(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.
Click here to enter text.

(e) What process is used to determine if the information is accurate?
Accuracy of the information provided to DoS to authenticate documents is the responsibility of the individual requesting the authentication service. The PII listed in paragraph 3(d) is required in order for the Document Examiner/Analyst to contact the requester regarding the documents requiring authentication services and the return of the documents.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Information submitted on DS-4194 by the requester is validated by Government personnel prior to the record being stored in CA DARTS. The document information contained on the DS-4194 is either manually entered or scanned into storage providing information on what documents are being authenticated by the DoS Document Examiner/Analyst personnel.

Once the Document Examiner/Analyst completes the authentication transaction and returns the document, the status information regarding that transaction (i.e., that the document is validated, returned, etc.) is recorded in CA DARTS. No other actions are needed to ensure information remains current. If additional documents need to be authenticated, the requester must submit those documents and a new completed DS-4194.

(g) Does the system use information from commercial sources? Is the information publicly available?
CA-DARTS does not use commercial information or publicly-available information.

(h) Is notice provided to the individual prior to the collection of his or her information?
A Privacy Act Statement is currently being approved by Department officials for form DS-4194. This notice will inform the requester of the routine uses of the information, the governing authorities for the collection of the data, and any disclosures associated with this particular form. Presently, the DS-4194 form does include guidance that informs the requester that the form is used by the U.S. Department of State for documents submitted by U.S. citizens and foreign nationals to authenticate. The DoS Authentications Office is responsible for signing and issuing certificates under the Seal of the U.S. Department of State for documents being sent to foreign countries.

(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?

The DS-4194 informs the requester that their case may be rejected if the information is not provided. The requester can provide the information and sign the form as consent, or decline to fill in the information, in which case the request for certification of document(s) will be rejected.

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

Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The Department of State understands the need for personally identifiable information (PII) to be protected. Accordingly, the PII in CA DARTS is handled in accordance with federal privacy laws regarding the collection, access, disclosure, and storage of PII. CA DARTS only collects the information necessary to authenticate documents and to return them to the requester.

5. Use of information

(a) What is/are the intended use(s) for the information?
PII in CA DARTS is used to carry out authentication services requested by the public. PII is used to track documents submitted for authentication, to communicate with the requester and to return documents to the requester of services.

(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 PII is used according to the purpose of the system's design. Information is required to authenticate, communicate and return documents to the requester of services.

(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.
CA DARTS PII is not shared with any internal or external organizations.

(b) What information will be shared?
CA DARTS PII is not shared with any internal or external organizations.

(c) What is the purpose for sharing the information?
CA DARTS PII is not shared with any internal or external organizations.

(d) The information to be shared is transmitted or disclosed by what methods?
CA DARTS PII is not shared with any internal or external organizations.

(e) What safeguards are in place for each internal or external sharing arrangement?
CA DARTS PII is not shared with any internal or external organizations.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
CA DARTS PII is not shared with any internal or external organizations.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
The privacy policy on the Department of State public web site includes instructions on how to obtain access to records by contacting the listed offices by phone or by mail.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
Individuals who have a change to the contact information previously provided can email, mail, or walk in their information. CA-DARTS doesn't scan and retain the document the requester wants certified. Only the record of the certification and the PII of the requester depicted in paragraph 3(d) is maintained in the CA-DARTS. If there is a change in a document previously certified, the document must be re-certified by submitting the updated document with a new form DS-4194.
If no, explain why not.
Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?
Walk-in requesters will receive notification from the representative who assists them in the authentication process. Requesters who e-mail or mail documents for authentication will receive instructions in the response sent to them by e-mail or mail.

8. Security Controls

(a) How is the information in the system secured?
The CA-DARTS 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 CA DARTS 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 Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

(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.

Access to the DARTS system is role based, and restricted according to approved job responsibilities and managerial concurrence. To activate, the government manager initiates a request to the Service Desk via an automated access request form. 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?

Various technical controls for the CA DARTS are in place to deter, detect, and defend against the misuse of personally identifiable information. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State network and respective applications. From that point on any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Bureau of Diplomatic Security Configuration Guides, auditing is also enabled to track the following events on the CA DARTS 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. If an issue were to arise, administrators of the system would review (audit) the logs collected from the time a user logged on until the time he/she signed off. This multilayered approach to security controls greatly reduces the risk that PII will be misused.

(d) Explain the privacy training provided to 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 sign that they agree to the rules and must 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.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and

reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. IIB's goal is to ensure that information processed and stored is safe from unauthorized access, disclosure, disruption, or denial of service.

All CA systems must comply with all guidelines published by Systems Integrity Division, in addition to all Security Configuration Guides published by Diplomatic Security. Adherence to these guides is verified during the system's Assessment and Authorization process.

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

The information collected in CA-DARTS contains PII of U.S. citizens, companies, Legal Permanent Residents (LPR), and foreign nationals requesting document authentication services. Due to the sensitivity of information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing.

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. Security measures are in place to minimize these risks, 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 in paragraph 8(e) are 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?
DoS Document Examiners/Analysts, System Administrators and Database Administrators.

(b) How is access to data in the system determined?
An individual's job function determines what data can be accessed as approved by the supervisor and 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

Consular Affairs/Consular Systems and Technology (CA/CST) adheres to a formal, documented audit and accountability policy that addresses purpose, scope, roles, and responsibilities. Procedures and controls are documented in the System Security Plan. The Plan includes information and procedures regarding access to data in CA DARTS.

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

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

There are three types of user roles: DoS Document Examiners/Analysts, System Administrators and Database Administrators.

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

DoS Document Examiners/Analysts -include DoS personnel who are responsible for examining and analyzing documents, generating certificates, and entering processing fee information.

System Administrators – CA DARTS System Administrators are responsible for all daily maintenance, establishing access control lists (ACLs), maintaining user accounts, and backups.

The Database Administrators – The CA DARTS Database Administrators (DBA) fix applications, backups, and configurations to the database. DBA access is controlled through the use of Access Control Lists (ACLs) as authorized by the manager and established by the system administrators. CA DARTS DBAs are authenticated using Windows operating system authentication. The CA ISSO is responsible for reviewing and approving DBA accounts.

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

CA-DARTS information is protected by multiple layers of security controls including network security, Department site physical security and management security including:

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

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

- CA DARTS Database Administrators and internal users have access 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.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Audit logs are reviewed daily for suspicious activity.