PRIVACY IMPACT ASSESSMENT

Document Authentication Review Tracking System

1. Contact Information

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

2. System Information

(a) Name of system: Document Authentication Review Tracking System
(b) System acronym: CA-DARTS
(c) Bureau: Consular Affairs
(d) iMatrix Asset ID Number: 372
(e) Child systems and iMatrix Asset ID Number (if applicable): N/A
(f) Reason for performing PIA:

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

(g) Explanation of modification (if applicable):

3. Purpose

(a) Describe the purpose of the system.

The Department of State (Department) is responsible for authenticating federal documents and state-issued authentication certificates to be used abroad by U.S. persons, commercial organizations, other government agencies, and foreign nationals. The CA Document Authentication Review Tracking System (CA-DARTS) is a service similar to those used by U.S. state governmental agencies responsible for document authentication of state documents.

CA-DARTS supports the Department's mission to authenticate documents. The CA-DARTS output is an authenticating certificate that certifies the submitted document is a public document signed and/or sealed by a government official in their official capacity. 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. Examples of the documents tracked in CA-DARTS include:

• State authentication certificates for adoption records, marriage and death certificates and other vital records
• State authentication certificates of notaries

• FBI background checks
• Federal court documents authenticated by the Department of Justice
• Other federal agency documents

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

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

U.S. Persons and Non U.S. Persons:

• Name
• Personal Address
• Personal Email Address
• Personal Phone Number
• Personal Cell Number
• Name of Business/Organization
• Business Address
• Business Phone Number
• Country
• Representative (If someone were to retrieve/submit the request on behalf of someone else's) contact information): Name, Company, Phone number, Email Address

(c) How is the PII above collected?

Authentication Requesters mail in, email, walk in, or drop off and pick up documents requiring certification by CA-DARTS personnel. The document authentication 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 personnel and/or contract staff. The physical paper form DS-4194 is used as a cover sheet for the document(s) submitted by the requester to be authenticated. Only the record of the certification and the PII of the requester is maintained in 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.

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

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.

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

☒Yes ☐ No

If no, please explain:

4. Authorities and Records

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

22 CFR Part 131 Certificates of Authentication

(b) If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security numbers.

N/A

(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)? *Contact your office or Bureau's legal advisor to confirm the correct SORN. If uncertain about the appropriate legal adviser, please notify the Privacy Office at Privacy@state.gov.*

☒ Yes, please indicate relevant System of Records Notice (SORN) below

- SORN Name and Number:

  STATE-05 Overseas Citizens Services Records and Other Overseas Records 09/08/2016
  STATE-26 Passport Records 03/24/2015
  STATE-39 Visa Records 11/08/2021

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

(d) 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.

(e) List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system? .

DispAuthNo : N1059-03-10, item 23

DispAuthNo: N1-059-03-10, item 23b (1)

PRIVACY IMPACT ASSESSMENT

5. Data Sources, Quality, and Integrity

(a) What categories of individuals below originally provide the PII in the system? Please check all that apply.

☒ Members of the public (U.S. persons which includes U.S. citizens or LPRs)
☐ U.S. government employees/contractor employees
☒ Other (people who are not U.S. citizens or LPRs)

(b) Do the individuals listed in 5(a) provide PII on individuals other than themselves? Please check all that apply.

☐ Members of the public
☐ U.S. government employees/contractor employees
☐ Other
☒ N/A

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

Accuracy of the information provided to the Department to authenticate documents is the responsibility of the individual requesting the authentication service. The information provided by the requester is verified by contacting the requester to validate the information on the documents, and through the return of the documents.

(d) What steps or procedures are taken to ensure the PII remains current?

Information submitted on DS-4194 by the requester is validated by Department 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 CA-DARTS personnel.

Once the authentication transaction is complete and the document is returned, the status information regarding that transaction (i.e., that the document is validated, returned, etc.) is recorded in CA-DARTS. No other action is 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.

(e) Was the minimization of PII in the system considered?

☒ Yes ☐ No

If no, please explain.

(f) Does the system use information, including PII, from commercial sources?

☐ Yes ☒ No

If yes, please list the commercial sources.

(g) Is the information, including PII, collected from publicly available sources?

☐ Yes ☒ No

If yes, please list the publicly available sources.

(h) Does the system analyze the PII stored in it?

☐ Yes ☒ No

If yes:

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

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record?

(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?

(i) If the system will use test data, will it include real PII?

☐ Yes ☐ No ☒ N/A - this system does not use test data

If yes, please provide additional details.

6. Redress and Notification

(a) Explain whether a notice is provided to the record subject at the point of collection of their information.

A Privacy Act Statement is included on the Department of State DS-4194 form at the point of collection of PII for the document authentication request. This PAS provides the applicant with notice of what authorizes the Department to collect this information, why the information is being collected, with whom the information will be shared, and the impact of the delivery of requested services if failure to provide the information requested.

(b) Are opportunities available for record subjects to decline to provide the PII?

☒ Yes ☐ No

If no, please explain why not.

(c) Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?

☐ Yes ☒ No

If yes, please explain.

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

SORN STATE-26, and STATE-05 provide procedures on how to contact an office for assistance to gain access to their information. Also, CA-DARTS authentication service requesters who have a change to their contact information previously provided can email, mail, or walk in to provide their information.

(e) Are procedures in place to allow a record subject to correct or amend their information?

☒ Yes ☐ No

If yes, explain procedures and how record subjects are notified.

Procedures allowing record subjects are published in the System of Records Notices (SORNs) STATE-05 and STATE-26. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated on form DS-4194 utilized for data collection. Also, CA-DARTS authentication service requesters who have a change to their contact information previously provided can email, mail, or walk in to provide their information. CA-DARTS does not scan and retain the document the requester wants certified.

If no, explain why record subjects are not able to correct their information.

7. Sharing of PII

(a) To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(b) For each of the entities in 7(a), list the PII from 3(b) that will be transmitted.

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(c) For each of the entities in 7(a), what is the purpose for transmitting the information?

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(d) For each of the entities in 7(a), list the methods by which the information will be transmitted.

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(e) For each of the entities in 7(a), what safeguards are in place for each method of internal or external transmission?

Internal (within the Department)	External (outside of the Department)
N/A	N/A

8. Security Controls

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

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

The CA-DARTS is configured according to the Department ' s Security Configuration Guides to optimize security while still providing functionality. 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. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need to perform official duties.

(b) 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.

(c) Below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.

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

(d) After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.

Accounts are reviewed and validated every 90 days by the supervisor and local Information System Security Officer (ISSO) for compliance with account management control requirements.

For access to CA-DARTS, management approval is required; approval is based on position and need to know. Local ISSOs and system administrators are responsible for managing the local systems accounts as approved by the supervisor. This local responsibility includes establishing, activating, modifying, reviewing, disabling, and removing accounts.

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

☒ Yes ☐ No

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

☒ Yes ☐ No

(g) Privacy Related Training Certification

- Do all OpenNet users of this system take the course PA318 Protecting Personally Identifiable Information biennially?

  ☒ Yes ☐ No

- Do all OpenNet users of this system take the course PS800 Cybersecurity Awareness Training annually?

  ☒ Yes ☐ No

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

  ☒ Yes ☐ No

  If yes, please list the related trainings here:

  IA210 System Administrator Cybersecurity Foundations Course