



Privacy Impact Assessment (PIA)

**For Document Authentication Review Tracking
System (CA-DARTS)**

Version 05.06.00

Last Updated: September 12, 2014

1. Contact Information

Department of State Privacy Coordinator

Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** September 12, 2014
- b. **Name of system:** Consular Affairs Document Authentication Review Tracking System version 05.06.00
- c. **System acronym:** CA-DARTS
- d. **IT Asset Baseline (ITAB) number:** # 372
- e. **System description (Briefly describe scope, purpose, and major functions):**

CA-DARTS supports the Department of State's mission to provide authentication services on documents that will be submitted abroad by U.S. citizens, commercial organizations, other government agencies and foreign nationals as authenticated documentation. In addition to document authentication, CA-DARTS also supports the office responsible for tracking submitted documents and fees paid for the document authentication service.

CA-DARTS product is an authenticating certificate for the submitted document that adheres to international laws, governing trade, and other areas. CA-DARTS supports the authentication of Adoption Certificates, Business Certificates, Educational Certificates, Legal Certificates, and Marriage Certificates.

Requestors may submit a document for authentication either in person or by US mail. No web based interface is provided.

- 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):** N/A
- h. **Date of previous PIA (if applicable):** N/A

3. Characterization of the Information

The system:

- Does NOT contain PII. If this is the case, you must only complete Section 13.
- Does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

CA-DARTS output is an authenticating certificate for the submitted document that adheres to international laws, governing trade, and other areas. CA-DARTS supports the authentication of the five types of documents listed in Section 2e, and collects the types of PII as listed below:

- Name
- Address
- Phone Number
- E-mail

The sources of information are the applicant, the DS-4194 Request for Authentications Service and the document(s) to be authenticated.

b. How is the information collected?

The requestor completes form DS-4194. Information obtained from form DS-4194 is manually entered or scanned into CA-DARTS by Department of State and/or contract staff. Applicants do not have access to CA-DARTS. The information is collected in the CA-DARTS production environment, which resides on the State Department intranet. Requestors submit PII to CA-DARTS as part of the process of requesting document authentication services. The physical paper form DS-4194 is used as a cover sheet for the document(s) to be authenticated. Once the document has been authenticated and returned the DS-4194 is then retained on file for a 2 year period.

c. Why is the information collected and maintained?

The information is collected to support determinations of the authenticity of documents submitted to the Department of State prior to issuing a certificate of authenticity for use abroad.

PII is retained temporarily in order to be able to contact the requestor as needed until processing fees have been paid and the request is completed. When the request is completed, the PII is deleted from CA-DARTS.

d. How will the information be checked for accuracy?

Accuracy of the information provided to CA-DARTS is the responsibility of the individual requesting the authentication service.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 22 CFR Part 92 (Authority of Department of State notarizing officers)

- 22 U.S.C. 4221 (Depositions and Notarial Acts)
- Section 127(b) of the Foreign Relations Authorization Act, Fiscal Years 1994–1995 (Pub. L. 103–236)
- 22 U.S.C 2651(a) (Organization of Department of State)
- 22 U.S.C. 2671 (Delegation of authority pertaining to certification of expenditures)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)
- Federal Claims Collection Act of 1966, 31 U.S.C. 3701 - 3720E, as amended through the Debt Collection Improvement Act of 1996 (P. L. 104-134); Office of Management and Budget (OMB) Circular A-129; 22 CFR 34 (Debt Collection)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The CA-DARTS system collects the minimum amount of personally identifiable information necessary to support the Department of State's mission to authenticate documents that will be used abroad and ensure that the fees that are due are collected.

The primary risk is misuse by Department employees and contractors. Misuse of PII could result in delayed processing of documents to be authenticated or failure to collect all fees that are due. Misuse could also result in administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports.

Due to the strict security controls that are required to be in place before operation of the system, no identified privacy risks are associated with this system. The controls are subject to rigorous testing, and formal certification and accreditation (C&A). Authority to operate is authorized by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually, and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application. Only authorized users with a need to know are granted access to CA-DARTS data.

4. Uses of the Information

a. Describe all uses of the information.

The only uses of PII data in CA-DARTS are to track documents submitted for authentication, communicate with the requestor, and track the collection of fees.

Controls prohibit use of CA-DARTS PII through: (i) placement on portable computers or portable storage devices; and (ii) the creation of computer-readable extract of PII from databases intended to be accessed remotely or to be physically transported outside the Department's secured physical perimeter on removable media or on portable/mobile devices.

b. What types of methods are used to analyze the data? What new information may be produced?

CA-DARTS does not produce new data. PII data is not analyzed in CA-DARTS and no new information is produced.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

CA-DARTS does not use commercial information, publicly available information or information from other Federal agency databases.

d. Are contractors involved in the uses of the PII?

CA-DARTS is a government-owned system. Government personnel are the primary internal users of CA-DARTS. Contractors are involved with the design, development, and maintenance of the system. Privacy Act information clauses have been inserted into all statements of work and have become part of the signed contract. Each contractor employee is required to attend mandatory briefings that cover the handling of PII information prior to working on the task.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

CA-DARTS does not create new information about the record subject, or draw inferences based on the information provided. PII is used for purposes which do not create additional information about the record subject.

All internal users, including contractors, are screened prior to their employment with the Department of State or with their respective agency. The Bureau of Diplomatic Security (DS) is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit, and fingerprint records, and may include a personal interview if warranted.

It is mandatory for all Department of State employees and contractors to complete an annual computer security briefing and Privacy Act briefing from the Department of State. Contractors must also complete the briefings provided by the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

The internal users, system administrators, and database administrators are required to take annual security awareness training to safeguard PII from unauthorized users.

In addition, technical system security controls are in place as described in Section 3(f) above.

5. Retention

a. How long is information retained?

PII is retained in the CA-DARTS system for a very limited period in order to be able to contact the requestor as needed until processing fees have been paid and the request is completed. When the request is completed, the PII is deleted from the CA-DARTS system because the transaction is closed. The physical paper DS-4194 is used as a cover sheet for the document(s) to be authenticated. Once the document has been authenticated and returned the DS-4194 is then retained on file for a 2 year period per Department of State Consular Affairs office policy.

This reference [DispAuthNo: N1-059-03-10, item 23b(1)] is cited in the Records Retention Schedules:

A-06-021-33b(1) DARTS Master File

Description: Normal Certification.

Contains information extracted from documents associated 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.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

PII is retained for a very limited period to allow the Department to contact the requestor as needed until processing fees have been paid and the request is completed. This short retention period coupled with the very limited PII that is collected presents a minimal privacy risk. Any risks that are associated with the retention of PII are mitigated through controls that prohibit the use of CA-DARTS PII through: (i) placement on portable computers or portable storage devices; and (ii) the creation of computer-readable extract of PII from databases intended to be accessed remotely or to be physically transported outside the Department's secured physical perimeter on removable media or on portable/mobile devices.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

CA-DARTS PII information is not shared with any internal organizations.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

CA-DARTS PII information is not shared with any internal organizations.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

CA-DARTS PII information is not shared with any internal organizations.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

CA-DARTS information in the database is not shared with any external agencies.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

CA-DARTS information is not shared with any systems external to the Department of State.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

CA-DARTS information is not shared with any systems external to the Department of State.

8. Notice

The system:

contains information covered by the Privacy Act

System of Records Notice (SORN)

- State-73 Global Financial Management System
- State-39 Visa Records.
- State-26 Passport Records

does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Information is voluntarily provided by the individual when the document certification request is submitted. CA-DARTS relies on State 73 and State-39 and on the notice given to the requestors who fill out the form to mitigate the privacy risks posed by collection and use of PII.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes, all information collected by CA-DARTS is voluntarily provided by the applicant.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No, individuals do not have the right to consent to limited, special, and/or specific uses of the information. However, all information is given voluntarily by the applicant for the limited purpose of receiving authentication services. No other special uses of the information are permitted. Individuals are advised on the use of the information being collected at the time of collection.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is given to individuals as described in Section 8(a) above. CA-DARTS relies on State-39, State-73 and on the notice given to the requestors who fill out the form to mitigate the privacy risks posed by collection and use of PII.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

There are no procedures for an individual to gain access and amend information in CA-DARTS. Individuals are responsible for submitting accurate information with their request. CA-DARTS does not permanently retain the information so there is no need for the individual to gain access and amend their information.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Individuals are responsible for submitting accurate information with their request. CA-DARTS does not permanently retain the information. There is no need for the notification or redress regarding the individual's data so there is no privacy risk associated with those procedures.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to CA-DARTS 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. To access the system, users must be granted the status of an authorized user of the Department of State's unclassified network. Each authorized user must sign a user access agreement before being given a user account. The authorized

user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified.

b. What privacy orientation or training for the system is provided authorized users?

Users must attend a security briefing and pass the computer cyber security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outlines the expected use of these systems and how they are subject to monitoring prior to being granted access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.) As a result of these actions, the residual risk is low.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

CA-DARTS does not employ any technology known to elevate privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since CA-DARTS does not use any technology known to elevate privacy risk, the current safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

a. What is the security certification and accreditation (A&A) status of the system?

The Department of State will operate CA-DARTS in accordance with information security requirements and procedures required by federal law and policy to ensure that

information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security management Act (FISMA) of 2002, the system is undergoing its initial assessment and authorization to operate process. CA-DARTS received its authorization to operate in June 2014. This document was drafted as part of the initial authorization of the system.