1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: October 9, 2009

(b) Name of system: Consular Affairs Domestic Support Suite 2.0

(c) System acronym: CADSS

(d) IT Asset Baseline (ITAB) number: 919

(e) System description:

The Consular Affairs Domestic Support Suite (CADSS) is an application suite used by various offices within CA to perform daily domestic operations. CADSS is comprised of 14 modules of which, one module called the Children's Issues Case Management System (CICMS), stores case information about U.S. Citizens under the age of 18 who reside domestically. The other modules in CADSS do not store or maintain PII.

CICMS tracks American Citizen Services cases involving children and young adults. It supports activities associated with providing and managing the delivery of information and support to the government's customers. This module no longer collect personally identifiable information (PII); however, for the purpose of the remaining data stored within CADSS, it will address the PII data that was stored within the CADSS 1.0 CICMS module (still present) in the legacy client-server aspect of the application.

(f) Reason for performing PIA:

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

(g) Explanation of modification (if applicable): See above description.

(h) Date of previous PIA (if applicable):

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?

CADSS, via CICMS, data entry is strictly limited to track cases opened prior to 2006. The Passport Lookout Tracking System (PLOTS) has replaced CICMS; however, until such time that PLOTS transfers records prior to 2006, CICMS will be used to monitor existing case records. No new information is created; CICMS is merely a tracking system.

Existing case records within CICMS contain the following information on U.S. citizens under the age of 18 who are the subject of an American Citizen Services case:

- Full name;
- Date of birth;
- Place of birth;
- Social security number (SSN); and
- Passport number.

b. How is the information collected?

The source of the information is the parent, legal guardian, or officer of the court for the U.S. citizens under the age of 18 who are the subjects in the Children's Issues Case Management System (CICMS).

c. Why is the information collected and maintained?

Information is collected and maintained in CICMS as a tracking system for American Citizen Services (ACS) cases involving U.S. citizens under the age of 18. The information in CICMS is maintained until the case information is imported into the Passport Lookout Tracking System (PLOTS) is formally acknowledged as a PLOTS record.

d. How will the information be checked for accuracy?

The accuracy of the information provided to American Citizen Services (ACS) is the responsibility of the parent, legal guardian, or officer of the court who is opening the case for the minor. The data is read only. The responsibility for checking accuracy of the information entered falls upon personnel in CA/OCS/CI.

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

- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

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

CADSS (via CICSM) collects the minimum amount of PII necessary to complete its functions. It currently serves as a tracking system for American Citizen Services (ACS) cases regarding minors before the information is transferred to PLOTS, via CICSM. As a way to streamline the process, CICSM will be retired and all ACS information regarding minors will be housed in PLOTS. This streamlining mitigates privacy risk and eliminates a PII-collection within the Bureau of Consular Affairs (CA).

Due to the strict security controls required to be in place before operation of the CADSS, there are no identified privacy risks. 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 CADSS.

4. Uses of the Information

a. Describe all uses of the information.

Data stored within CICMS is used to generate a printed “Intake Letter.” This letter is addressed to the parent, legal guardian or cfficer of the Court acknowledging the U.S. minor has been entered into the Children’s Passport Issuance Alert Program (CPIAP). The letter contains information on whether a passport application/issuance has been found in the system, who applied for the passport and any additional relevant comments. This letter contains only the child(ren)’s names and the CICMS Case Number.

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

The report above is used to analyze the data 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.

CADSS does not use commercial information, publicly available information or information from other Federal agency databases.

d. Is the system a contractor used and owned system?

CADSS is a government owned and operated system.

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.

CICMS performs basic internal analytical functions on the PII but does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy/integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating any privacy risk. There is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Consular Affairs Records.

Information is retained on individual(s) until the age of 18 years old or when the information is transferred into PLOTS, whichever comes first.

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

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

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?

The information is shared at the discretion of the CA/OCS/CI and Consular Affairs, but with no other bureaus within the Department for the purpose of tracking American citizen children.

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

All records are maintained within the CA/OCS/CI until the person turns 18 years of age and/or the information has been retired or destroyed. Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. An Interface Control Document (ICD) and Memorandum of Understanding (MOU) define and disclose transmission format via OpenNet. All physical records containing personal information are maintained in secured file cabinets or in restricted areas

with access limited to authorized personnel only. Access to electronic files is protected by passwords and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

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

Internal CA regulations stipulate that this data is treated like Sensitive but Unclassified (SBU) and follows State Department policies. Access to information is controlled by application access controls. Management control reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal Department regulations.

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?

Information within CADSS is not shared externally.

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

Information within CADSS is not shared externally.

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

Information within CADSS is not shared externally.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

Provide number and name of each applicable system of records.
(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

Passport Records, STATE-26

☐ does not constitute a system of records covered by the Privacy Act.

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

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notice (SORN) STATE-26, Passport Records.

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

The individual is informed of the Privacy Act statement; whereby, the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the System of Records Notice (SORN) STATE-26, Passport Records.

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. The utility of the information in the system about a particular individual will not extend over the allotted time in the appropriate Department of State's Disposition of Records Schedule. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

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.

The Notice offered is reasonable and adequate in relation to the system's purposes and uses.

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?

CADSS information is protected and accessible in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN (State-26) and in rules published at 22 CFR 171.31 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 171.32.

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

Since information in CADSS is Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's

stated purposes and uses and its applicable legal requirements. Therefore this category of privacy risk is appropriately mitigated in CADSS.

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 CADSS is limited to authorized Department of State users who have a justified need for the information in order to perform official duties. To access the system, authorized users must be an authorized user of the Department's unclassified network. Access to CADSS requires a unique user account assigned by a supervisor. 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). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. 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. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

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

All users must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain 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.

Access control lists defining who can access the system and at what privilege level are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.)

User access to information is restricted according to job responsibilities and requires managerial level approvals. 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. The CADSS system administrator uses the User

Administration window to establishing, activating, modifying, reviewing, disabling, and removing CADSS user accounts. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

11. Technologies

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

CADSS does not employ any technology known to involve privacy risk beyond technologies already employed by OpenNet.

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

Since CADSS does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum, satisfactory in this application.

12. Security

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

CADSS 2.0 system is currently going through a full Certification and Accreditation process, with an anticipated completion date of December 2009.