DEPARTMENT OF STATE
FY 2008
PRIVACY IMPACT ASSESSMENT
Consular Affairs Domestic Support Suite (CADSS)

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Programs and Services
Privacy E-mail: pia@state.gov

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

(1) Does this system collect, maintain or disseminate personally identifiable information (PII) about individual members of the public?**

YES _X_ **NO**___

> ** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".

If the above answer is YES, please complete the survey in its entirety. If NO, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.

1) Does a Privacy Act system of records already exist?

YES _X_ **NO**___

If yes, please provide the following:
System Name _CADSS_____ **Number** _Passport Records/State-26__

If no, a Privacy system of records description will need to be created for this data.

2) What is the purpose of the system/application?

The Consular Affairs Domestic Support Suite is an application suite used by various offices within the Bureau of Consular Affairs (CA) to perform daily domestic operations.

A client-server version CADSS Domestic Support Suite (v1.0) is currently in production throughout CA. The CADSS client-server suite is the end-result of integrating over 50 homegrown, internal CA office Access 97 database applications into a single environment to implement version control, user permissions and eliminate data redundancy between 2000 and 2003. Currently, the Suite contains 14 distinct modules. Each module contains its own back-end database and there are several shared databases used across the Suite. The Suite's collection of databases is centrally located in a single SQL Server 2000 repository. As of February 2007, the CADSS Software Development Team has upgraded all 14 front-end modules to Microsoft Access 2003.

3) What legal authority authorizes the purchase or development of this system/application?

8 U.S.C 1101-1503 (Immigration and Nationality Act of 1952, as amended)

B. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

CADSS is comprised of 14 modules of which, one module called the Children's Issues Case Management System (CICMS), stores information about U.S. Citizens under the age of 18 who reside domestically.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

Parent, legal guardian, or officer of the court

b. What type of information is collected from the source of the information?

Full Name, date of birth (DOB), place of birth, social security number and passport number

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

N/A

b. How will data be checked for completeness?

N/A

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

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.

C. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

Yes

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

No

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

No

4) Will the new data be placed in the individual's record?

N/A

5) How will the new data be verified for relevance and accuracy?

N/A

6) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved by using personal identifiers such as name, date of birth (DOB), or place of birth.

7) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The only form printed from CICMS is an Intake letter. This letter is addressed to the parent, legal guardian or officer 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 have been

found in the system, who applied for the passport, and additional relevant comments. This letter contains only the child(ren)'s names and the CICMS case number. No sensitive data exists on the Intake Letter.

D. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

CICMS is operated at CA/OCS/CI located at State Annex (SA-29); one site only.

2) What are the retention periods of data in this system?

CICMS tracks the case until the child turns 18 years of age. Once the child is 18, the case record is transferred from an open to archived status.

Passport Records:

A-13-000-01c(2)(a)	**Passport Case Files**
Description:	c. Passport Case Files, 1983-present. Consist of passport applications with photograph attached; applications for amendment or extension of passports; and related correspondence. (2) Microfilm. (a) Original Silver Halide (Archival).
Disposition:	Transfer to WNRC monthly. Destroy when 100 years old.
DispAuthNo:	NC1-59-79-12, item 1b(2)(a)

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Files of closed cases are retired or destroyed in accordance with published record schedules of the Department of State and as approved by the National Archives and Records Administration (NARA). See above

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

N/A, CADSS is not using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)

5) How does the use of this technology affect public/employee privacy and does it restrict access to the system?

N/A, see E4

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**
N/A, system does not provide monitoring.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**
N/A

8) **Are there forms associated with the system? YES ___ NO _X_**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

F. **ACCESS TO DATA:**

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**
Managers, contractors, users, system administrators and developers have access to data based on access controls and the permissions of the role in which the person is placed.

2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**

All users must first have an OpenNet account and be apart of the CA domain. Domain users are controlled through the use of the Active Directory (AD) Organizational Units (OU). A government manager must request that a user be added and level of access required.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**
Once a CADSS user is properly identified and authenticated on the CA domain, they are authorized to perform only the functions commensurate with their assigned role. CADSS employs logical access controls in accordance with the principle of least privilege and the concept of separation of duties.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**
The CADSS employs logical access controls in accordance with the principle of least privilege and the concept of separation of duties. This reduces the risk and prevents the misuse of data.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Yes. Contractors are the primary designers and developers of CADSS. All contractors have abided to regulatory guidelines and have signed and follow CA's Rules of Behavior.

All contracts include a privacy handling statement. All contract staff must attend annual security awareness / privacy awareness training.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
Currently, there are no interfaces to the CADSS application. The Passport Lookout Tracking System has replaced the CICMS module in CADSS and will eventually receive the records prior to 2006. For the data contained within CADSS and PLOTS, CA/CST is responsible for protecting the privacy rights of the public.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**
No.

8) **Who is responsible for assuring proper use of the SHARED data?**
CA/OCS/CI