DEPARTMENT OF STATE

FISCAL YEAR 2007

PRIVACY IMPACT ASSESSMENT

FOR

Diplomatic Clearance Application System (DCAS)

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

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

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

YES _X_ **NO** ___

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

YES ___ **NO** _X_

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

The U.S. Department of State (DOS), Bureau of Political Military Affairs, International Security Operations (PM/ISO), is responsible for issuing diplomatic overflight clearances. These clearances apply to all **non-U.S.** government and military flights overflying or landing in the United States or its territories, often carrying foreign dignitaries and other persons of interest (VIP).

The purpose of the DCAS is to provide a web-based application for foreign embassies to electronically submit applications for diplomatic overflight clearance. This is a major application that has been designed to replace the current fax and phone technology, increasing the efficiency of handling the diplomatic overflight clearance application process.

Foreign embassies will use the DCAS to manage applications specific to their country. Other U.S. Government agencies (e.g. FAA and U.S. Customs) will have read-only access to the system to keep informed of foreign government flights coming in to and out of U.S. airspace. All information passed is SBU and secured over an SSL connection.

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

The Federal Aviation Act of 1958, as amended in (49 U.S.C. 40103 (d) Public Law 103-272 of July 5, 1994) states that the aircraft of the armed forces of any foreign nation shall not be navigated in the United States except in accordance with an authorization granted by the Secretary of State. Pursuant to 22 CFR 126.6 (b), the authority to grant such authorization has been delegated to the Office of International Security Operations pursuant to FAM 01-0414.2.

We interpret "foreign military aircraft" to include foreign military, state, or government owned aircraft and those aircraft chartered to transport a head

of state or government, cabinet minister, and/or other senior foreign government official, or other official delegation intending to land in, or fly over, the U.S. and its possessions. All aircraft of this type must obtain a diplomatic overflight or landing clearance to land on, or fly over, U.S. soil. Delegations or other foreign officials arriving on scheduled commercial airlines, foreign or U.S., do not require such clearances.

C. DATA IN THE SYSTEM:

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

Department of State employees; federal agency employees (e.g. FAA, TSA, Customs, etc.);
foreign embassy personnel; and contractors

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

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

Each foreign embassy representative requesting access to the system and submitting applications for a diplomatic clearance number will be the source of both personal contact information for each account as well as the flight information defined below in 2(b).

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

The following information is collected and reported from the Diplomatic Clearance Application System (DCAS) form.

Applicant Information	
Field	**Description**
Country	Country which is submitting the application
First Name	First Name of the person responsible for the application
Last Name	Last Name of the person responsible for the application
Organization	Organization responsible for the application
Title/Position	Title or position of the person responsible for the application
Address	Street address of applicant
City	City address of applicant
State	State address of applicant
Postal Code	Postal Code address of applicant
Telephone	Telephone number of applicant
Alternate Telephone	Alternate telephone of applicant

Fax	Fax number of applicant
Email	Primary email address of applicant
Alternate Email	Secondary email address of applicant
Flight Information	
Field	**Description**
Make/Model	Make and model of aircraft
Call Sign	Call sign of the aircraft
Tail Number	Tail number of the aircraft
ALAN	
NALAN	
AALAN	
Pilot's Name	Name of the pilots flying the aircraft
Number of Crew	Number of crew on the aircraft
Number of PAX	Number of passengers on the aircraft
VIP Names	Names of dignitaries onboard
Purpose of the flight	Reason for Diplomatic Clearance Application Request
Flight Comments	Additional comments regarding flight information
Flight Itinerary Information (Per Location)	
Field	**Description**
Country	Country
Airport	Airport
Arrival Date	Date of aircraft arrival
Arrival Time	Time of Arrival
Departure Date	Date of Departure
Departure Time	Time of Departure
Overnight?	Will the aircraft stay overnight?
Overfly?	Aircraft overflying?
Hazmat Information (If Applicable)	
Field	**Description**
Description	Description of Hazmat material
U.N. Classification	U.N. Classification of Hazmat Material
Measure/Weight	Measure of material
Weapons Information (If Applicable)	
Field	**Description**
Person	Name of person in possession of weapon

Weapon Type	Type of Weapon
Serial Number	Serial Number of Weapon
Ammo	Qty of Ammo
Department Information	
Field	**Description**
DCN	Diplomatic Clearance Number
Coordination	Description of necessary coordination activities.
Coordination Date	Date of coordination activities
Special Codes	Special 2 digit codes identifying characteristics of the flight.
Staff Notes	PM/ISO notes about this application.

3) Accuracy, Timeliness, and Reliability

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

Each application submitted through the DCAS web application is submitted by each individual. All information is required to be reviewed for accuracy and approved by a PM/ISO administrator before a diplomatic clearance number is issued.

b. How will data be checked for completeness?

Each application submitted through the DCAS web application is required to be reviewed for completeness and approved by a PM/ISO administrator before a diplomatic clearance number is issued. The minimal required information needed to apply is controlled by required fields (on the form) within the application.

c. Is the data current?

Submitters are required to amend any application as necessary throughout the course of flight should information regarding the flight change. PM/ISO administrators are responsible for maintaining the currency of the open applications in the system as well as archiving closed applications once they have expired.

D. 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?**
No.

5) **How will the new data be verified for relevance and accuracy?**
Each application submitted through the DCAS web application is required to be reviewed for accuracy and approved by a PM/ISO administrator before a diplomatic clearance number is issued.

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.**
The DCAS is a web based application. Access and data manipulation occurs by accessing the DCAS forms through a web browser. Information on an individual will rarely if ever be retrieved, except to update contact information for applications. Applications will most likely be retrieved by the assigned Diplomatic Clearance Number.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
Currently, the reporting features of the DCAS are limited. The only report that can be printed regarding an individual is their contact information (see applicant information under 2b), which is available to users with administrator and submitter roles. (**Note:** Submitters may only print their own information.) The only other report that can be printed is a flight violation report containing how many violations a country had per given year, which has no personal information attached to it. The violation report is used to reassert FAA regulations to those countries not abiding by the overflight procedures.

E. 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?**
DCAS is operated in only one location.

2) **What are the retention periods of data in this system?**
At this point, the DCAS retains all information indefinitely. Future releases may enable archiving of expired records.

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?**
N/A

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
No. DCAS uses programmatic access.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**
The DCAS has very little impact on public and employee privacy. Besides name, contact information, and travel itinerary, no other personal information is stored about individuals or groups. Access is restricted to users with a valid DCAS account. An established procedure is set up to manually verify the identity of an individual before authorizing a login for that person. Currently, all applications are sent over an unsecured fax and telephone. DCAS will improve communication security of the information by establishing a secure socket layer (SSL) between the web server and client.

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?**
The DCAS has very basic capabilities to log and monitor users accessing the system. Each of these capabilities is local to the DCAS servers and is secured by access privileges built into the operating system and each service.

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

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?**
DCAS administrators (PM/ISO – DOS employees);
DCAS submitters (foreign embassy personnel);
DCAS Readers (other federal government agencies: FAA, Customs, etc.);
Contractors (for backup and maintenance);
System Administrators (VC/VO personnel); and
Developers (for database and Web Code).

2) **What are the criteria for gaining access to the system?**
The System Security Plan documents the access control mechanism for the system. In short, physical access is granted to those individuals who are responsible for the backup and maintenance of the DCAS application. Access and control to the hardware is maintained by VC/CO and DS. User Accounts and privileges within the DCAS application are granted by the PM/ISO system manager. Accounts are established for those individuals who require the ability to submit applications or read applications that have been submitted. All access is determined with the "need-to-know" requirement.

3) **Will users have access to all data on the system or will the user's access be restricted?**
DCAS users are provided a level of access to the DCAS system when their user account is created. One of three access levels can be granted: (1) reader; (2) submitter, or (3) administrator. Access control is handled programmatically within the website and provides the following functionality at each level of access:

(1) Reader: Readers are permitted to log into the DCAS. They are able to change their own personal contact information and login information. They have access to external resources, such as links to help pages and other web sites. They have READ ONLY access to diplomatic clearance application for which an administrator has issued them access. This is initiated when administrators accept an application and add the reader to the notifications list. When a reader has been given access to an application, they may only read and print its contents. Readers can be given access to applications from different countries. They have no ability to alter or delete information pertaining to applications.

(2) Submitter: Submitters are permitted to log into the DCAS. Submitters are able to change their own personal contact information and login information. They have access to external resources, such as links to help pages and other web sites. Submitters have Read and Write access to diplomatic clearances that have been entered into the system for their home country. Submitters do not have the capability to see applications from other countries, but do have access to all applications for their country whether the application was initiated with their login or the login of someone.

(3) Administrator: Administrators are permitted to log into the DCAS. Administrators have full read/write access to all information and settings within the DCAS.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access?**
The DCAS programmatically implements three separate levels of access to data. This architecture helps to alleviate potential misuse, but in no way extinguishes it. Standard operating procedures and security requirements are

established and included in training session to notify each user of their responsibilities while logged into the DCAS. Misuse will result in loss of privileges.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**?
PM/ISO contracts out the development and maintenance of the DCAS application. Under the established purchase order, Privacy Act contract clauses were NOT inserted in their contracts and other regulatory measures were NOT addressed, nor have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended.

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?**
At this time, no other systems share data with the DCAS application.

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?**
Other federal agencies will have established reader accounts allowing them to view applications for which they have been granted access. The FAA, TSA and Customs agencies for example will have read only access to the DCAS system.

8) **Who is responsible for assuring proper use of the SHARED data?**
The responsibility for assuring proper use of the DCAS system lies with the PM/ISO System Manager.