

# Diplomatic Clearance Application System (DCAS)

## Privacy Impact Assessment

### 1. Contact Information

**A/GIS/IPS Director**

Bureau of Administration

Global Information Services

Office of Information Programs and Services

### 2. System Information

- (a) Name of system: Diplomatic Clearance Application System
- (b) Bureau: PM/ISO
- (c) System acronym: DCAS
- (d) iMatrix Asset ID Number: 879
- (e) Reason for performing PIA: Click here to enter text.
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): Click here to enter text.

### 3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
  - Yes
  - No - Contact IRM/IA at [IASolutionCenter@state.gov](mailto:IASolutionCenter@state.gov) for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?  
Currently undergoing re-authorization
- (c) Describe the purpose of the system:

The DCAS supports Political–Military International Security Operations (PM/ISO), mission requirements for operational issues, military exercises, humanitarian operations, and administrative functions related to the joint efforts of the Department Of State and the Department Of Defense.

The U.S. Department of State (DOS), Bureau of Political Military Affairs, International Security Operations (PM/ISO), is responsible for issuing diplomatic overflight/landing

and vessel clearances. These clearances apply to all non-U.S. government and military flights over-flying or landing and ship visits in the United States or its territories, often carrying foreign dignitaries or other luminaries.

The purpose of DCAS is to provide a web-based application for foreign embassies to electronically submit applications for diplomatic over flight or maritime clearance. Foreign embassies will use the DCAS application to manage over flight/maritime requests specific to their country. Other U.S. Government agencies (e.g. FAA and U.S. Customs and Border Protection (CBP)) will have read-only access to the system to keep informed of foreign government flights coming in to and out of U.S. airspace and territorial waters. All information transmitted is SBU and secured over a TLS (version 1.2) connection.

- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The system collects minor PII such as names, addresses, telephone numbers, and email addresses of primarily non-US citizens. Occasional US citizen information may be entered from operators (i.e. pilots, ship captains, etc.); however, this information is limited. No social security, financial, or health data is included in DCAS.

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

National Strategy for Aviation Security

- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number: [Click here to enter text.](#)
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): [Click here to enter a date.](#)

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

Information is retrieved by application number.

- (g) 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 Division at [Privacy@state.gov](mailto:Privacy@state.gov).

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?  Yes  No

(If uncertain about this question, please contact the Department's Records Officer at [records@state.gov](mailto:records@state.gov).)

If yes provide:

- Schedule number): A-24-050-01b
- Length of time the information is retained in the system: When records have reached their retention period of three years, they are immediately retired to the

Records Service Center, then later transferred in accordance with the National Archive and Records Administration.

- Type of information retained in the system:  
Subject files/port visits

**4. Characterization of the Information**

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

- (b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes  No

- If yes, under what authorization?

[Click here to enter text.](#)

- (c) How is the information collected?

Users enter the information via online form on the DCAS website.

- (d) 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.

[Click here to enter text.](#)

- (e) What process is used to determine if the information is accurate?

Manual review by Federal staff

- (f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

All information and applicable records are short-term records that correlate to flights and marine transportation. Once the flight/voyage is over, the record is no longer current and is available solely for reference.

- (g) Does the system use information from commercial sources? Is the information publicly available?

There is no public or commercial information. All information is access controlled.

- (h) Is notice provided to the individual prior to the collection of his or her information?

Yes, on the DCAS login banner, replicated below:

*I understand that as a user of the Diplomatic Clearance Application System (DCAS), I have been granted privileges to access the DCAS and facilitate the request for diplomatic aircraft clearance. I understand that as a condition of my use I must adhere to the following restrictions:*

*·I am responsible for the safeguarding of the username and password assigned to me by the Department of State.*

*·Passwords will expire every 6 months. Passwords may be changed without notice if the application administrator determines that a potential compromise of login information has occurred.*

*·I will not let another user access the DCAS using my login credentials. Doing so would be considered a security violation.*

*·I will use the DCAS to conduct official U.S. government business only. Limited personal information of mine is collected and maintained on this website.*

*I have read and understand the above limitations on my use of the DCAS website and will comply with the restrictions. I understand that my use of the U.S. government provided DCAS account may be monitored and that violation of any of the aforementioned security may result in immediate lockout from the system.*

- (i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?  Yes  No

- If yes, how do individuals grant consent?

[Click here to enter text.](#)

- If no, why are individuals not allowed to provide consent?

All DCAS information is required to fulfill the mission requirements. No unnecessary information is collected.

- (j) How did privacy concerns influence the determination of what information would be collected by the system?

Personal information is required for PM/ISO to complete its mission. PM/ISO is responsible for issuing diplomatic overflight/landing and vessel clearances and uses the information contained with DCAS to do so. The least amount of personal information is collected in order to accomplish the PM/ISO mission.

## **5. Use of information**

- (a) What is/are the intended use(s) for the information?

The information is collected to provide data and metrics for review by appropriate USG agencies in order to clear foreign officials attempting to enter the U.S. This information is used strictly within DCAS and is not released to any other system or party.

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes.

- (c) Does the system analyze the information stored in it?  Yes  No

If yes:

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

[Click here to enter text.](#)

- (2) Does the analysis result in new information?  
[Click here to enter text.](#)
- (3) Will the new information be placed in the individual's record? Yes No
- (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?  
Yes No

**6. Sharing of Information**

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.  
The information is shared with the Federal Aviation Administration (FAA) and Customs and Border Protection (CBP).
- (b) What information will be shared?  
All pertinent information for individual flight or marine travel is shared.
- (c) What is the purpose for sharing the information?  
The purpose is to provide necessary information and tools to the correct parties at the correct time for individual flight or marine travel for specific foreign nationals who are entering the United States.
- (d) The information to be shared is transmitted or disclosed by what methods?  
All CBP and FAA users are standard DCAS users (i.e. it is accessed by the web portal). There is no interconnection.
- (e) What safeguards are in place for each internal or external sharing arrangement?  
Bureau policy and technical access controls.
- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?  
None. All information is required for the fulfillment of the PM/ISO mission.

**7. Redress and Notification**

- (a) What procedures allow individuals to gain access to their information?  
Standard web application log in. Individuals submit their information via the portal, so they can log in to access or correct their information.
- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?  
Yes No  
  
If yes, explain the procedures.  
All users can update their specific information in the DCAS account web page.  
If no, explain why not.  
[Click here to enter text.](#)
- (c) By what means are individuals notified of the procedures to correct their information?

DCAS users can change their personal information at any time via the account page; there is no notification per se.

## **8. Security Controls**

- (a) How is the information in the system secured?

The information is secured using industry standard technologies, such as TLS encryption for data-in-transit and TDE encryption for the database. Access to information is restricted to approved users who have authorization to use DCAS.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

All information is segregated by user account – the application and database structure does not allow unauthorized access to other individuals’ information. Ensuring only those with a need-to-know see the information when individuals at external agencies access DCAS is the responsibility of those agencies.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Multiple safeguards include firewall, operating system, and application audit logs. In particular the Web Application Firewall (WAF) inspects all encrypted traffic that the perimeter firewall cannot “see”.

- (d) Explain the privacy training provided to authorized users of the system.

All DoS users receive DoS privacy training via PS-800 (Cybersecurity Awareness) and PA-459 (Protecting Personally Identifiable Information). Foreign/outside users do not receive training.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?  Yes  No

If yes, please explain.

DCAS is available only via encrypted website (HTTPS) and transmits data by way of TLS 1.2 with AES-256 encryption. Additionally, it transmits keys via Ephemeral Diffie-Hellman (ECDH) which is more modern than RSA.

- (f) How were the security measures above influenced by the type of information collected?

All security controls were put in place in accordance to NIST 800-53 guidance and no “special” controls were used, other than the addition of a Web Application Firewall.

## **9. Data Access**

- (a) Who has access to data in the system?

Authorized users, administrators, and the system owner only.

- (b) How is access to data in the system determined?

Access to the data is dependent upon a person's role and the permissions PM/ISO grants.

- Submitters only access their individual’s country information.

- Readers only access what PM/ISO authorizes them to see and can only add info applicable to their office.
- Super Readers can only view all information without the ability to manipulate anything.
- Administrators have full access to all DCAS data.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?  Yes  No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

User access is restricted by user so that they can access their specific information only. Some users, such as the system owner and his delegates, are “super users” who can access all data, as required.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

For regular users, technical controls are in place to prevent unauthorized browsing. For super users, policy and need-to-know are in place to prevent unauthorized browsing.