

# Holocaust Deportation Claims Tracking System

## 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: Holocaust Deportation Claims Tracking System

(b) Bureau: L/CID

(c) System acronym: HDCTS

(d) iMatrix Asset ID Number: [Click here to enter text.](#)

(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?

This system is an Access database, and as a Microsoft Office application, an A&A is not required.

(c) Describe the purpose of the system:

The purpose of the system is to track the progression of claims being processed under the claims program established by the U.S.-France Agreement for Deportation Claims.

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

The following would be collected in the database:

1. Name, address, phone number and email of applicant
2. Name of deportee
3. Nationality of the deportee
4. Name, address, phone number and email of an applicant's legal representative
5. Marital status of the deportee
6. Place of deportation and destination
7. Date of death

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

The State Department Basic Authorities Act, 22 U.S.C. §§2651 (a), 2656, and 2668(a), and the Agreement Between The Government of the United States of American and the French Republic on Compensation for Certain Victims of Holocaust-Related Deportation from France Who Are not Covered by French Programs.

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

Yes, provide:

- SORN Name and Number: Records of the Office of the Assistant Legal Adviser for International Claims and Investment Disputes, State-54
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 20, 2008

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

[Click here to enter text.](#)

- (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) .)

We are currently working on setting a retention schedule for the system of records.

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): [Click here to enter text.](#)
- Length of time the information is retained in the system: [Click here to enter text.](#)
- Type of information retained in the system:  
[Click here to enter text.](#)

#### 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?

The information would be collected from the claims form (DS-7713) which would be submitted by the claimant through mail, email, or fax.

- (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?

The data collected will mostly depend on the information provided by the claimant. Information regarding deportation may be verified by consulting the following public website: <http://www.memorialdelashoah.fr/index.php/en/>.

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

Most of the information collected would be historical data. However, contact information for claimants would be current. The data would be manually updated when the office receives notice of a change of address, phone number, or the like.

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

Yes. Information about the date and place of deportation is publicly available at <http://www.memorialdelashoah.fr/index.php/en/>.

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

Yes. The notice is provided in the Privacy Act Statement contained on DS 7713 Claim Form.

- (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?

The Privacy Act statement on the DS 7713 states that “providing this information is voluntary,” but notes that failure to provide the requested information could result in denial of the claim.

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

[Click here to enter text.](#)

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

We only collected the minimum amount of information necessary to process claims and contact claimants. We did not collect any additional PII. .

## 5. Use of information

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

The information would allow staff to track the status of claims and would assist in the determination of eligibility to receive compensation under the U.S.-France Agreement.

- (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. The information will allow staff to determine eligibility for compensation.

- (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?

There are three categories of eligible claims. The system would analyze the amount of compensation paid under each claim category.

- (2) Does the analysis result in new information?

No.

- (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 would be shared with the State Department employees responsible for processing Deportation Claims. Some PII might be shared with the Departments of Justice and Treasury in order to process claims. No PII will be shared with other countries.

(b) What information will be shared?

All information listed in Item 3(d) would be shared.

(c) What is the purpose for sharing the information?

Sharing of this information would prevent duplication of efforts among staff, would provide continuity of claim review, and prevent duplicative payments.

(d) The information to be shared is transmitted or disclosed by what methods?

The information would be shared in an Access Database that only the Deportation Claims processing staff would have access to.

(e) What safeguards are in place for each internal or external sharing arrangement?

Access to the database will be limited to only those individuals responsible for processing claims.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Only individuals involved in the processing of claims have access to the database, in order to minimize the risk of exposure of information.

## 7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The system contains Privacy Act-covered records. Therefore, notification and redress are the right of record subjects. Procedures for notification and redress are published in the System of Records Notice (SORN) Records of the Office of the Assistant Legal Adviser for International Claims and Investment Disputes (STATE-54), and, and in rules published within 22 CFR 171 Subpart D, Privacy Act Provisions.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes  No

If yes, explain the procedures.

Claimants may supplement their claims with additional information at any time prior to payment of the claim. The database would be updated when staffs receive notification of a change to information that is being stored.

If no, explain why not.

[Click here to enter text.](#)

- (c) By what means are individuals notified of the procedures to correct their information?

Claimants will be given the contact information of a staff member to assist them in filing a claim, or correcting information relating to a previously filed claim.

## 8. Security Controls

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

The information in the system would be secured via an Access Control List (ACL), i.e., only those individuals who are in the ACL on the server would be able to access the database.

- (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.

Any end user who has a need to access the system must be approved by the L/CID Office Director or the Deputy Office Director.

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

The end users of the system are aware of the negative consequences of misuse of the information. Only the persons processing claims will possess adequate permissions to access the system and the information within it. The system will track which user made the last edit to each entry. An auditing module will be built into the system once it is created.

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

In accordance with Department of State computer security policies, HDCTS users are required to complete the Department’s Cyber Security Awareness Training and the Department’s PII Training at least once a year. These Department of State training programs reinforce the obligation of users of any Department of State computer system and those who have access to the data it contains to protect PII through appropriate safeguards to ensure security, privacy and integrity.

- (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.

The database would only be accessible to end users who are in the ACL.

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

N/A – these security measures are used to secure any data or information on a Windows based file server.

## 9. Data Access

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

Persons responsible for processing deportation claims would have access to the data in the system. Managers and system administrators will also have access.

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

Only staff assigned to review claims would have access to the database.

(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.

Access to the system would be restricted to persons indicated in Item 6 (a). All authorized users have access to all information. This is necessary to persons processing claims can cross-reference other claims to make sure they are not duplicates.

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

Staff members are instructed that information is only to be used for the processing of Holocaust Deportation Claims. The system also will display the name of the last staff member who edits a particular entry field.