

2DB PIA

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:** Electronic Passport Application Form Internet Website

(b) **Bureau:** CA - Bureau of Consular Affairs

(c) **System acronym:** 2DB

(d) **iMatrix Asset ID Number:** #897

(e) **Reason for performing PIA:**

- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

(f) **Explanation of modification (if applicable):** N/A

3. General Information

(a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**

Yes X No

(b) **What is the security Assessment and Authorization (A&A) status of the system?**

The Department of State operates the Electronic Passport Application Form Internet Website (2DB) in accordance with information security requirements and procedures required by Federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security management Act (FISMA) of 2002, the triennial assessment and authorization of this system is underway and is expected to be completed by September 2015. This document was updated as part of the triennial reauthorization of the system.

(c) **Describe the purpose of the system:**

The Electronic Passport Application Form (2DB) is a web based passport application system that provides public users with U.S. passport application forms. 2DB allows users to complete a passport form and print it with a barcode. The system provides online versions of these forms:

- Form DS-11 Application for a U.S. Passport
- Form DS-64 Statement Regarding a Lost or Stolen U.S. Passport Book and/or Card
- Form DS-82 U.S. Passport Renewal Application for Eligible Individuals
- Form DS-4085 Application for Additional Visa Pages or Miscellaneous Passport Services

- Form DS-5504 Application for a U.S. Passport - Name Change, Data Correction and Limited Passport Book Replacement.

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

The applicant completes one of the above forms using the web based 2DB application. After the applicant completes a form, the system offers the option to download or print it. The applicant downloads or prints the completed form along with the barcode generated by the 2DB application. The applicant's data is printed clearly on the form and some of the data is encoded in the barcode to facilitate subsequent processing. As soon as the user downloads or prints the form and barcode, the data is permanently deleted from the 2DB web application. For some forms, the applicant mails the printed form to a State Department facility which scans it, uploads the data from the barcode, and processes the passport request. For the Form DS-11 Application for a U.S. Passport, the applicant hands the form over to an Acceptance Agent who forwards it to a Department of State facility or State Department employee.

The data elements may include some or all of the following:

Forms DS-11, DS-4085, and DS-5504 may include any of the following fields:

- Name
- Gender
- Date and place of birth
- Permanent mailing address
- Telephone number
- Social Security Number
- Passport and/ or Driver's license number (or other identifying document number)
- Photograph
- Height
- Eye color
- Employer's name
- Occupation
- Marital status
- Parents' names
- Parents' date and place of birth
- Whether parents are U.S. citizens
- Emergency contact name
- Emergency contact phone number
- Emergency contact relationship to applicant
- Dates and destinations of any planned travel

Form DS-64 Statement Regarding a Lost or Stolen U.S. Passport Book and/or Card is a standalone form, but may also be used in conjunction with a DS-11 Application for a U.S. Passport when a previous valid or potentially valid U.S. passport book/card cannot be presented. Form DS-64 requires the following fields:

- Name
- Gender
- Date and place of birth
- Telephone number
- Social Security Number
- Passport numbers of lost or stolen passport(s)

- Issue date(s) of lost or stolen passport(s)
- Details regarding the loss or theft (when, where, how)
- Details regarding any efforts to recover the lost or stolen passport(s)

Form DS-82 U.S. Passport Renewal Application for Eligible Individuals may be used by persons seeking to replace a U.S. passport by mail if these conditions apply: 1) their most recent U.S. passport was issued within the past 15 years, 2) the applicant was over the age of 16 when their most recent U.S. passport was issued, and 3) the applicant submits their most recent U.S. passport with their Form DS-82.

The DS-82 may include the following fields:

- Name
- Gender
- Permanent mailing address
- Telephone number
- Social Security Number
- Height
- Hair color
- Eye color
- Employer's name
- Occupation
- Emergency contact name
- Emergency contact phone number
- Emergency contact address
- Emergency contact relationship to applicant
- Dates and destinations of any planned travel

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

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 26 U.S.C. 6039E (Information Concerning Residence Status)
- 22 U.S.C Sec. 211a-218 (Passports)
- Executive Order 11295 , August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)

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

Yes ___ No X

If yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

If a SORN is not required, explain how the information is retrieved without a personal identifier.

The 2DB web application collects data for the purposes of printing the passport forms. It does not store the data in the web application and cannot be searched by any identifier. The data is

encoded in the barcode on the printed form and subsequently scanned/ uploaded into State Department databases at a later time. While the 2DB web application does not require a SORN, the data collected is covered by State-26, Passport Records.

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes ___ No X

If yes, please notify the Privacy Division at 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 X

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.) The 2DB system does not store the information, and as a result does not need a records schedule. The TDIS and CLASS systems which process the forms have an approved NARA schedule.

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)):
- Type of information retained in the system:
- Length of time the information is retained in the system:

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

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

Yes X No ___

- If yes, under what authorization?

- 26 U.S.C. 6039E (Information Concerning Residence Status)
- 22 U.S.C. 213 (Application for Passport; Verification by Oath of Initial Passport)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)

- (c) How is the information collected?

Information is obtained directly from the passport applicant using one or more of the above forms. The applicant completes the form online, prints the form with the barcode and mails it to a passport agency. The 2DB web application deletes all the data in the form immediately after the form is downloaded or printed. The passport agency processes the form by scanning the barcode and uploading the data into the Travel Document Issuance System (TDIS) or the Consular Lookout Support System (CLASS).

- (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.

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

The passport applicant is required to certify that the information is complete and accurate. The agency verifies the information by checking other State Department databases and systems during processing. The 2DB web application deletes all the data in the form immediately after the form is downloaded or printed.

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

The applicant is the primary person responsible for ensuring that the information is current. Department of State personnel also ensure to the extent possible that the information is current when the application is reviewed and approved, but the systems involved in this "verification" process are not part of the 2DB web application. Once a passport is issued or replaced, it is valid until its expiration date unless it is renewed or revoked. Passport applicants can request changes or corrections to a passport by completing Form DS-5504 Application for a U.S. Passport - Name Change, Data Correction and Limited Passport Book Replacement.

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

The system does not use any commercial information, publicly available information or information from other federal agency databases. All of the information in the system is derived from the passport applicant.

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

Yes. Individuals are made aware of the uses of the information on the passport application forms. The individual is advised of the Privacy Act statement prior to completion of the form.

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

- If yes, how do individuals grant consent?

Filling out and submitting application for passport services is a voluntary action and the applicant's acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information for the purposes of a passport application. Individuals do not have the option to limit the use of the information to specific purposes.

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

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

All of the PII collected is essential to the passport application process. The PII information is not stored in the 2DB application; accordingly there are no privacy issues related to 2DB. The information is uploaded to Travel Document Issuance System (TDIS) and Consular Lookout and

Support System (CLASS) which are subject to stringent access control and auditing due to security and privacy concerns. State Department personnel with privileged access to these systems are required to adhere to all Federal regulations regarding the protection and use of PII. Also, use of the information is restricted according to job responsibilities and access control lists.

5. Use of information

(a) The intended use(s) for the information is/are:

The Department of State utilizes the information to determine whether the applicant is entitled to a U.S. passport and to document lost and stolen passports.

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

All information collected by the system is essential for the adjudication of a U.S. passport application and /or to report the loss or theft of a U.S. passport.

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

If yes:

- **What types of methods are used to analyze the information?**
N/A
- **Does the analysis result in new information?**
N/A
- **Will the new information be placed in the individual's record?**
N/A
- **With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?**
N/A

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The 2DB web based application is publicly accessible to anyone who wishes to complete a passport form, but the application does not store any data and does not provide a "search query" function. Applicants cannot return to the website and access a record. The applicant can only complete the form and print it. The information cannot be shared, either internally or externally, from within the 2DB application.

Once printed or downloaded, the information is stored on a barcode which may be shared internally within the Department of State. A passport agency employee can scan the barcode from the form and upload the information into the Travel Document Issuance System (TDIS) or the Consular Lookout and Support System (CLASS). The data from Form DS-11 Application for U.S. Passport, Form DS-82 U.S. Passport Renewal Application for Eligible Individuals, Form DS-4085 Application for Additional Visa Pages or Miscellaneous Passport Services, and Form DS-5504 Application for a U.S. Passport - Name Change, Data Correction and Limited Passport Book Replacement is uploaded to TDIS. The data from Form DS-64 Statement Regarding a Lost or Stolen U.S. Passport Book and/or Card is uploaded to CLASS.

The information is accessible in TDIS and CLASS by authorized Department of State personnel who process the passport application and manage passport related issues such as revocation and law enforcement "holds."

(b) What information will be shared?

The information on the passport forms will be uploaded to TDIS and CLASS as outlined in section 6(a), above. The information can be accessed in TDIS and CLASS by authorized users internally within the Department of State. The information is not stored in the 2DB web application at any time. There is no direct connection between 2DB and TDIS, or between 2DB and CLASS.

(c) The purpose for sharing the information is:

Authorized State Department personnel access the information in TDIS or CLASS in order to process passport applications or record information about a lost or stolen passport.

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

The information is uploaded to TDIS and CLASS from a barcode scan as outlined in section 6(a), above. The passport related information stored in TDIS and CLASS is accessible only from the State Department's intranet. There are no external users. The information is not transmitted at any time.

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

The information is only shared internally. There are no external sharing arrangements. Internally, the information is accessible to authorized users of TDIS and CLASS. TDIS and CLASS are subject to stringent access policies, auditing and monitoring.

In accordance with U.S. government policies, any Federal government employee or contractor with access to Personally Identifiable Information (PII) must adhere to strict requirements for protection and storage of PII. Department of State personnel are required to comply with these requirements and to complete yearly training regarding cyber security and the protection of Personally Identifiable Information (PII).

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

The system collects the minimum amount of information required to adjudicate a U.S. passport application and/or report a U.S. passport as lost or stolen. There is a risk that some employees with access to the PII may use it for purposes other than those authorized by Federal law and regulations and guidance issued by the Department of State. The Department mitigates these risks by minimizing the collection of PII and limiting its access to authorized users.

7. Redress and Notification

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

Passport applicants are the original sources of the information at the time the application is completed. Applicants cannot access their records after the barcode has been generated in the online form.

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

Yes X No _____

If yes, explain the procedures.

Any errors that appear on the final passport can be corrected by completing Form DS-5504 Application for Name Change, Data Correction and Limited Passport Book Replacement.

If no, explain why not.

- (c) **By what means are individuals notified of the procedures to correct their information?**
Procedures for notification and redress are published on the Department of State's Freedom of Information Act (FOIA) website which posts the Passport Records System of Records Notice (SORN) STATE-26. Individuals are notified of STATE-26 via the Privacy Act Statement included on the forms.

8. Security Controls

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

2DB makes it possible for public users to complete and print an online form with a barcode to request passport services. The website requires an internet browser that supports 128-bit encryption. As soon as the form is printed, the information is deleted from the web application.

- (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.**

The 2DB web application does not permit access or retrieval of information because the applicant's data is deleted when the form is downloaded or printed. The information is accessible in TDIS and CLASS after the form has been processed and uploaded. Access to TDIS and CLASS is strictly controlled, audited and users are required to complete yearly cyber security and privacy awareness training. Access to the TDIS and CLASS systems is based on job functions and need-to-know requirements. System/Web Administrator privileges are also based on job functions and managers must approve their access.

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

The system automatically generates audit trails which are analyzed and reviewed regularly. Non-production uses (e.g. testing, training) of production data are restricted by administrative controls.

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

All State Department employees and contractors must complete yearly cyber security and privacy awareness training in order to maintain their access to the system. Privacy awareness training reiterates the requirements that PII must not be stored on non-secure storage media, and users must secure supervisory permission to transfer any PII to removable media.

- (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

Please explain.

At the passport applicant's point-of-access, the website requires an internet browser that supports 128-bit encryption. Once the application is received at a State Department facility, it is scanned and the data from the barcode is uploaded. At this point the passport request is processed. State Department personnel and contractors (authorized users) can only access the information from a secure internal Department network.

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

The PII collected as part of the passport application process is extremely sensitive and private information. The Department of State is cognizant of the sensitive nature of the information and

takes all appropriate measures including access control, mandatory security clearances, enhanced cyber security, mandatory privacy awareness training, and PII encryption to ensure secure collection, storage, and transmission of PII.

The Department of State mitigates the risks by minimizing the PII collected. It is limited to that PII which is necessary to adjudicate a U.S. passport application and/or report a U.S. passport as lost or stolen. The Department also enforces strict compliance with all Federal regulations regarding collection, access, storage and transmission of PII. Numerous management, technical, and operational security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST).

9. Data Access

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

As soon as the passport applicant downloads or prints the form, the data is deleted from the web application. Accordingly, there is no information retained in the 2DB system which can be "accessed" or "searched." When the applicant's printed form with the barcode is processed by Department personnel and contractors, the data is uploaded into other databases (TDIS and CLASS) which can report, view, manage and approve the passport related records.

(b) Access to data in the system is determined by:

The 2DB web application can be accessed by any public user with an internet browser that supports 128-bit encryption. The 2DB application permits public users to print completed passport application forms. Once the forms are printed, the data is deleted from the web application and the applicant cannot return to the site and search or print anything.

The 2DB System Administrator privileges are based on job functions and roles. Senior managers must approve all access requests but the access and privileges only permit the System Administrators to manage the application. There is no data stored in the 2DB application to retrieve or search. Furthermore, all State Department personnel must complete mandatory cyber security and privacy awareness training for the protection of PII.

The passport record information which is uploaded from the form into TDIS and CLASS is restricted to authorized users of those systems. Access and privileges is strictly controlled by access lists, permissions and privileges settings, auditing, and reporting.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

Yes X No

2DB System Administrators have established procedures and controls governing access to the system. However, there is no data to access in the 2DB application. There are no procedures or controls necessary for 2DB application users because the application is available to the public.

For TDIS and CLASS, the two database systems which actually store passport information, the procedures, controls, and responsibilities regarding the access and activities of State Department users are documented in system accounts by managers who approve access and privileges. Access and activities of those TDIS and CLASS users are closely monitored and audited.

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

There is no data to access in the 2DB application.

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

System audit trails are automatically generated and regularly analyzed to deter and detect unauthorized uses. Non-production uses, for example, testing, training with production data are restricted by administrative controls. However, there is no data to access in the 2DB application.