Electronic Passport Application Form Internet Website

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) **Date of Completion:** March 2024
(b) **Name of system:** Electronic Passport Application Form Internet Website
(c) **System acronym:** 2DB
(d) **Bureau**: Consular Affairs
(e) **iMatrix Asset ID Number:** 897
(f) **Child systems and iMatrix Asset ID Number (if applicable):** N/A
(g) **Reason for performing PIA:** To update existing PIA for a triennial security reauthorization
(h) **Explanation of modification (if applicable):** N/A

3. Purpose

(a) **Describe the purpose of the system.**

The Electronic Passport Application Form Internet Website (2DB) supports the Bureau of Consular Affairs' (CA) mission by allowing U.S. citizens to apply for passports or to report a lost or stolen passport. 2DB is an public facing application that is accessed via a web browser and allows an applicant to complete forms relating to a passport book, passport card, and/or report a lost or stolen passport. Once the applicant completes the online form(s) the applicant reviews the completed form, prints the application, and mails the application to the passport office.

The following Department of State (Department) forms can be generated via 2DB:

- DS-11: Application for a U.S. Passport
- DS-82: Application for Passport by Mail Renewal
- DS-5504: Passport Re-application (Changes/Corrections to a Current Valid Passport)
- DS-64: Statement Regarding Lost or Stolen Passport

2DB also provides management information reports and generic graphical representation of data on the 2DB website usage.

(b) **List the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:**

2DB contains the following U.S. Citizen's PII:

- Name
- Date of Birth
- Place of Birth
- Gender
- Educational Information
- Social Security Number (SSN)
- Personal Phone Number
- Nationality
- Passport Information
- Photograph
- Occupation
- Height
- Hair and Eye Color
- Personal Address
- Personal Email Address
- Familial Information

(c) **How is the PII above collected?**

The information in 2DB is obtained directly from the passport applicant who completes the form online depending on their need, prints the form with the barcode, and mails it to a passport agency. The 2DB system deletes all data once the completed form is barcoded and printed by the applicant.

(d) **What is/are the intended use(s) for the PII?**

The collection of the PII in 2DB is used to allow U.S. citizens to apply for passports or to report a lost or stolen passport.

(e) **Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?**

Yes

4. Authorities and Records

(a) **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)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218 (Passport Application and Issuance)
- 22 U.S.C. 2651a (Organization of Department of State)
- 22 U.S.C. 2705 (Documentation of Citizenship)
- 22 U.S.C. 3927 (Chief of Mission)
- 22 U.S.C. 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 C.F.R. 301.6039E-1 (Information Reporting by Passport Applicants)
- Executive Order 11295, August 5, 1966; (Authority of the Secretary of State in granting and issuing U.S. passports)

(b) **If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security numbers.**

- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 U.S.C. 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) **In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)?**

No

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

The 2DB system does not retain information inserted by applicants, instead 2DB saves the data to a barcode which is printed, and the system erases the inputs. Data is not stored; therefore, a search by a personal identifier cannot be accomplished in this system.

(d) **Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?**

No

(e) **List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system?**

Disposition Authority Number: DAA-GRS-2017-0003-0002 5

5. Data Sources, Quality, and Integrity

(a) **What categories of individuals below originally provide the PII in the system? Please check all that apply.**

Members of the Public (U.S. persons which includes U.S. Citizens or LPRs)

(b) **Do the individuals listed in 5(a) provide PII on individuals other than themselves? Please check all that apply.**

Members of the Public

(c) **What process is used to determine if the PII is accurate?**

The passport applicant is required to certify that the information is complete and accurate. The agency verifies the information by checking other Department CA databases and systems e.g., the Travel Document Issuance System and the Consular Lookout Support System (CLASS) after the package is received for processing.

(d) **What steps or procedures are taken to ensure the PII remains current?**

The applicant is responsible for ensuring that the information is current when the application is complete. Once the applicant downloads or prints the application with barcode, 2DB erases all entries. Data is not stored in 2DB thus there is not a requirement for currency.

(e) **Was the minimization of PII in the system considered?**

Yes

(f) **Does the system use information, including PII, from commercial sources?**

No

(g) **Is the information, including PII, collected from publicly available sources?**

No

(h) **Does the system analyze the PII stored in it?**

No

(i) **If the system will use test data, will it include real PII?**

N/A - this system does not use test data

6. Redress and Notification

(a) **Explain whether a notice is provided to the record subject at the point of collection of their information.**

A Privacy Act Statement (PAS) is located on each individual form that the individual fills out to request a passport or report a stolen or lost passport. The PAS provides the individual with notice of what authorizes the Department to collect the information, why the information is being collected, with whom the information will be shared, and the impact of the delivery of requested services if failure to provide the information requested. There is also a link to the agency privacy policy on the webpage where information is collected.

(b) **Are opportunities available for record subjects to decline to provide the PII?**

Yes

(c) **Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?**

No

(d) **What procedures allow record subjects to gain access to their information?**

Since 2DB does not retain data, individuals are unable to access information from this system. Individuals desiring access to their passport records can follow instructions for gaining access as stated in the System of Records Notices (SORNs) State-26, Passport Records, and State-05, Overseas Citizens Services Records and Other Overseas Records. Applicants may also visit the Department of State Privacy Act/FOIA web site for the privacy policy which includes instructions on how to obtain access to information by contacting the listed offices by phone or by mail.

(e) **Are procedures in place to allow a record subject to correct or amend their information?**

No

If no, explain why record subjects are not able to correct their information.

Individuals are unable to correct their information in 2DB because the system does not retain data. However, in the event an individual would like to correct their passport records, they are notified of the procedures to correct records in these systems by a variety of methods:

1. During or after their interview; applicants can contact the representative who assisted them.

2. Published SORNs the PAS on the forms requesting and   Department of State Privacy

Act website

3. Letter or email that a correction is needed.

7. Sharing of PII

(a) **To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.**

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(b) **For each of the entities in 7(a), list the PII from 3(b) that will be transmitted.**

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(c) **For each of the entities in 7(a), what is the purpose for transmitting the information?**

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(d) **For each of the entities in 7(a), list the methods by which the information will be transmitted.**

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(e) **For each of the entities in 7(a), what safeguards are in place for each method of internal or external transmission?**

Internal (within the Department)	External (outside of the Department)
N/A	N/A

8. Security Controls

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

The 2DB is secured within the Department of State (Department) intranet where risk factors are mitigated through the use of in-depth, defense layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information to perform their official duties. Applications are configured according to the State Department Bureau of Diplomatic Security (DS) Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) 800-53 guidance and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program.

(b) **Where is the information housed?**

Department-owned equipment

(c) **In the table below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.**

Internal Department of State user access to 2DB is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. Department 2DB users, system administrators, web administrators, and database administrators have access to 2DB based on prescribed roles to conduct required business to support the CA passport processing of services.

(d) **After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.**

Accounts are reviewed at least annually by supervisors, in coordination with the local Information Systems Security Officer (ISSO) to review access privileges of users under their supervision to verify that access and/or privileges are still required and updated as required.

(e) **Have monitoring, recording, auditing safeguards, and other controls been put in place to prevent the misuse of the information?**

Yes

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

Yes

(g) **Privacy Related Training Certification**

- Do all OpenNet users of this system take the course PA318 Protecting Personally Identifiable Information biennially?

Yes

- Do all OpenNet users of this system take the course PS800 Cybersecurity Awareness Training annually?

  Yes

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

  No