PRIVACY IMPACT ASSESSMENT

Electronic Passport Application Form Internet Website (2DB)

1. Contact Information

PIA Completed By: Name: Joyce France Title: PIA SME/IAE Org: CA/CST/ST Phone: 703-639-0384 Email: FranceJM@state.gov	**System Owner:** Name: Gerald L. Pascua Title: CA/CST Deputy Director and System Owner Org: CA/CST Phone: 202-485-7721 Email: PascuaG@state.gov
Program Manager: Name: Sharon B. Westmark Title: Program Manager Org: CA/CST/PSDD Phone: (202) 485-7722 Email: WestmarkSB@state.gov	**IT Security Manager:** Name: Edward F. Bacon Title: IT Security Branch Chief/ISSO Org: CA/CST/ST/S Phone: (202) 485-7813 Email: BaconEF@State.gov
A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services	

2. System Information

(a) **Name of system:** Electronic Passport Application Form Internet Website

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

(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):

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 for assistance

(b) What is the security Assessment and Authorization (A&A) status of the system?
The system is currently undergoing its initial Assessment and Authorization (A&A) with a planned Authorization to Operate (ATO) date of Spring 2021.

(c) Describe the purpose of the system:

The Electronic Passport Application Form Internet Website (2DB) supports the Bureau of Consular Affairs mission requirements by allowing U.S. citizens or U.S. nationals to apply for passports or to report a lost or stolen passport. 2DB is an internet 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 forms can be generated via the 2DB online:

- 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.

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

2DB contains the following PII: name, date and place of birth, race, gender, education, Social Security Number, phone number, nationality, passport information or other ID Numbers, photo, occupation, height, hair and eye color, personal address, email address, education, occupation, family information.

(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)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 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)

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

☐ Yes, provide

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

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

The 2DB system does not retain information input by applicants – it saves the data to a barcode which is printed, and then the system erases the inputs. No data is stored; therefore, no search by a personal identifier can be accomplished in this system.

(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.

(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 .)

Department of State Records Disposition Schedule:
A-13-001a,b & d: Passport Records; Passport and citizenship Case Files
Description: Case files containing; passport applications, reports of birth of American Citizens Abroad; certificates of Witness to Marriage, Applications for Amendment or Extension of

Passport; certificates of loss of nationality; and other supporting forms, documents and correspondence pertaining to each case.
Disposition: A-13001a, transfer to the National Archives when 50 years old. Destroy when 100 years old. **A-13-001 b(1),(2),(3)** transfer and destroy in accordance with the respective disposition authority. **A13-001-01d**, Transfer to Washington National Records Center (WNRC) on an annual basis.
DispAuthNo: NC1-059-79-12, N1-059-04-02, N1-059-96-05 respectively.

A-13-002-03 Tracking/Issuance System
Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation.
Disposition: Permanent: Delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 3

A-13-002-06a Intermediary Records
Description: Hard copy and electronic input documents or forms designed and used solely to create, update or modify the records in an electronic medium and not required for audit or legal purposes (such as need for signatures) and not previously scheduled for permanent retention in NARA-approved agency records schedule. Also includes adhoc reports output for reference purposes or to meet day-to-day business needs.
Disposition: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
DispAuthNo: DAA-GRS-2017-0003-0002

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system?

☒ Members of the Public (<u>are</u> US citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☐ Other (are <u>not</u> U.S. Citizens or aliens lawfully admitted for permanent residence)

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

☒Yes ☐No

- If yes, under what authorization?
26 U.S.C. 6039E - Information Concerning Resident Status
26 C.F.R. 301.6039E-1 (Information Reporting by Passport Applicants)
22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) How is the information collected?

The information in 2DB is obtained directly from the passport applicant who completes the form online, prints the form with the barcode, and mails it to a passport agency. The application deletes all data in 2DB once the completed form is barcoded and printed by the applicant.. 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 and 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 after the package is received for processing.

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

The applicant is responsible for ensuring that the information is current when the application for service is complete. Once the applicant downloads or prints the application with barcode, 2DB erases all entries. The applicant mails the printed document/information. The package is checked upon receipt of the application package. Data is not stored in 2DB so there is no requirement to ensure it remains current.

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

No, 2DB does not use information from commercial sources or publicly available information.

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

Yes, a Privacy Act statement (PAS) is prominently displayed on the webpage that collects the PII and there is a link to the agency privacy policy.

(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?

2DB provides an Opt In checkbox where the applicant reads the Privacy Act Statement and must check the box agreeing to it before being allowed to continue.

- 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?

The PII listed in paragraph 3d is the minimum necessary to perform the actions required by the 2DB system to provide passport services. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered and addressed during the system design and security configuration. Impact is minimized as the PII information collected is limited to only what is required for the 2DB to perform the function for which it was intended and erased after it is printed.

5. Use of information

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

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

(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 PII is used according to the purpose –to allow applicants to apply for passports or to report a lost or stolen passport.

(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?

(2) Does the analysis result in new information?

☐Yes

☒No

(3) Will the new information be placed in the individual's record?

☐Yes

☒No

(4) With the new information, will the State 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.

Internal Information Sharing:

The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau. With that understanding, information in the 2DB system will be shared internally with the CA systems Travel Document Issuance System (TDIS) and the Consular Lookout and Support System (CLASS) to process passport applications.

2DB printed barcode with passport application information is scanned to upload into TDIS, and CLASS. The information can be accessed in TDIS and CLASS by authorized users internally within the Department of State Bureau of Consular Affairs. The 2DB Reporting Tool provides management with information reports and generic graphical representation of data on the 2DB website usage. The applicant's information is not stored in the 2DB web application at any time.

External Information Sharing:

2DB does not share information externally.

(b) What information will be shared?

The PII listed in paragraph 3(d) above will be shared.

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

To provide passport receipt, renewal and loss services to U.S. citizens.

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

Data in 2DB is not transmitted electronically. The application is printed with a barcode containing all the data. TDIS and CLASS scan the 2DB barcode to upload the data. The 2DB barcode is generated from the application, printed on the downloaded .pdf form, and is read from a TDIS scanner and uploaded into TDIS.

The DS-64 online form (Statement Regarding a Lost or Stolen Passport), is completed via 2DB. The web application tool processes the form and sends information to CLASS (database to database) to invalidate the passport. The DS-64 paper forms submission are mailed and information is manually entered into 2DB and processed to invalidate the passport. All 2DB data is removed once information is downloaded and barcoded.

(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 in CA and is 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 PII.

All paper mailed application records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

Details of the Secure Transmission Methods

The use of Transmission Control Protocol/Internet Protocols (TCP/IP) are used for 2DB data transport across the network. The TCP/IP protocol suite consists of multiple layers of protocols that help insure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary. Additionally, the transmissions are secured using digital certificates (including web-based Secure Socket Layer (SSL) certificates), and encrypted communications. The connection between all the sites that the 2DB servers reside on is protected using SSL with 128-bit data encryption.

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

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

b. Accidental disclosure of information to non-authorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies.

b. Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal or other.

These risk areas are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, sensitive but unclassified, and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know.

- System authorization and accreditation process along with continuous monitoring (Risk Management Framework). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications are encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

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

Since 2DB does not retain data, invididuals 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, March 24, 2015; and State-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016. 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.

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

☐Yes ☒No Individuals are unable to correct their information in 2DB because the system does not retain data.

If yes, explain the procedures.

(c) By what means are individuals notified of the procedures 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 their interview; or after the interview, applicants can contact the representative who assisted them
2. Published SORNs
3. Department of State Privacy Act Website
4. Being notified by letter or email that a correction is needed

If no, explain why not.

8. Security Controls

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

The 2DB is secured within the Department of State intranet where risk factors are mitigated through the use of defense in-depth 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 in order to perform their official duties.
All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer (ISSO).

Applications are configured according 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) **Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.**

To access the 2DB system, persons must be authorized users of the Department of State's unclassified network, OpenNet, which requires a background investigation and an application approved by the supervisor and local ISSO. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) (and) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports to be restricted. Local Information System Security officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

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

The CA System Manager, in conjunction with the CA ISSO and Security team, periodically scan and monitor information systems for compliance with DS Security Configuration Guides and conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host 2DB's application for changes to the Department of State mandated security controls.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.
Operating System (OS)-level auditing is set in accordance with the DS Security Configuration Guide. The OS interface allows the system administrator or local ISSO to review audit trail information through the security log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

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

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, Department of State direct hired civilian employees are required to take the one-time course (PA459 Protecting Personally Identifiable Information). The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must 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.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access while the data is being entered and/or scanned. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) **How were the security measures above influenced by the type of information collected?**
If data becomes exposed to unauthorized users while it's being entered or scanned, it may result in inconvenience, distress, or damage to standing or a reputation, financial loss, harm to State Department programs or public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation. The security measures listed above were implemented to secure the data in the system in accordance with federal laws and policies, including Department policies.

9. Data Access

(a) **Who has access to data in the system?**
2DB Public users, DoS OpenNet-based Users, Web Administrators, Database Administrators

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

The 2DB accounts are as follows:

2DB Public Users

2DB Internet users are U.S. citizens who are applying for a U.S. passport or need to report a lost or stolen U.S. passport. The Internet-based users do not require individual user accounts, as the 2DB application is configured for anonymous access. The application form is not saved anywhere within the 2DB. Instead, a barcode is generated once the applicant types in all information. The user then mails or in person presents the form (with the bar code) for processing.

2DB OpenNet Users

OpenNet users are cleared Department of State direct hire employees and contractors, who have a need to access the 2DB system per their position and/or role, which are primarily at the management level.

Web Administrator Web Administrators are responsible for all daily maintenance, establishing access control lists (ACLs), maintaining user accounts and backups. Since the duties of web administrators require that they be granted full access, the concept of separation of duties is specifically applied. The application of this concept segregates administrators into functional groups such that no single administrator is responsible for the same function (e.g. one administrator will be responsible for system backups while another administrator will handle user account management).

Database Administrator

Database Administrators are responsible for the daily maintenance, upgrades, patch/hotfix, and database configuration. The access of database administrators is limited to only those Oracle application files necessary to perform daily activities. This limit of access is controlled through the use of ACLs as established by the system administrators.

Access is determined based on position and job roles which are approved by the supervisor and local ISSO. Access is role based and user is granted only the role(s) required to perform officially assigned duties.

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

Information is documented in the 2DB System Security Plan. The Plan includes information regarding system access to data.

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

Users other than administrators will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and local ISSOs approve to perform official duties.

Public User: This access is limited to resources necessary to complete the form the applicant is completing for a specific service.

OpenNet User: Information is stored long enough to execute processes to barcode and print documents. Elements of this user group can only see information within the user directory.

Web and Database Administrators: The Web and Database administrators are the only users with direct access to the database for the purpose of performing various maintenance dutes. Accordingly, Web and Database Administrators have access to information within the directories during the execution of the barcoding and printing process of forms within a directory prior to information being deleted from 2DB.

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

- System component auditing is broken out by application, database, and system level auditing events. Audit records are generated from the various components within the system to monitor activities of individuals with access to the information. Auditing information include logon identifications associated with their name for auditing purposes. Administrators are prohibited from using their accounts for any functions not associated with their administrative duties.

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN).

-Privacy training informs users of the Rules of Behavior and warns against unauthorized browsing.