



Privacy Impact Assessment (PIA)

For: Travel Document Issuance System (TDIS)

Version 04.03.01

Last Updated: July 17, 2015

1. Contact Information

<p>A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services</p>

2. System Information

- a. **Date PIA was completed:** July 17, 2015
- b. **Name of system:** Travel Document Issuance System
- c. **System acronym:** TDIS
- d. **IT Asset Baseline (ITAB) number:** # 89
- e. **System description (Briefly describe scope, purpose, and major functions):**

The Travel Document Issuance System (TDIS) processes applications for United States passports from the point of receipt of the application through the issuance (or denial) of a passport book or a passport card.

- f. **Reason for performing PIA:**

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

- g. **Explanation of modification (if applicable):**

Triennial security reauthorization requires current PIA.

- h. **Date of previous PIA (if applicable):** August 31, 2010

3. Characterization of the Information

The TDIS system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

- a. **What elements of PII are collected and maintained by the system? What are the sources of the information?**

TDIS collects and maintains records related to applications for U.S. passports.
Elements of PII that are collected and maintained by the system are:

- Birthdates
- Place of birth
- Gender
- Social Security Numbers
- Biometric IDs
- Legal and family information (collects on application but does not store)
- Phone numbers
- Mailing address and;
- Email address

Sources of the information are U.S. citizens and nationals applying for passports, other Department of State computer systems, passport acceptance agents, the Social Security Administration, the lockbox provider (CITIBANK), passport specialists, and fraud prevention managers.

The categories of record subjects in TDIS are individuals who:

- Have applied for the issuance, amendment, extension, additional visa pages or renewal of U.S. passport books and passport cards;
- Were issued U.S. passport books or cards, or had passports amended, extended, renewed, limited, or denied; or
- Have corresponded with Consular Affairs concerning various aspects of the issuance or denial of a specific applicant's U.S. passport books or cards.

b. How is the information collected?

The information is collected on several different forms:

- Form DS-11 is used for passport applications for first time applicants.
- Form DS-82 is for persons applying to replace a passport issued within the past 15 years, who are over the age of 16 when the passport was issued, and who also provide the old passport with the application form.
- Form DS-5504 is for persons replacing a passport that was issued less than a year earlier. The form may be used to replace an emergency passport with a fully valid one; to make a change to the applicant's identifying information (e.g., name change due to marriage or court order); or to correct a printing error in a passport.
- Form DS-4085 is used to add visa pages to a previously issued and currently valid passport book.
- Correspondence between the applicant and Consular Affairs regarding the applicant's passport application.

The above forms may be completed by the applicant on published paper forms available at many government office locations or may be completed online using web forms at the Department of State's public website. If web forms are used, the applicant must still print the form and submit it as a hardcopy with supporting documents.

c. Why is the information collected and maintained?

Information is collected in TDIS to process passport applications to determine if a passport may be issued or denied. The U.S. passport identifies the bearer as a U.S. citizen or national. It is a request to foreign governments to permit travel or temporary residence in their territories and access to all lawful local aid and protection. It also allows bearers access to U.S. consular services, assistance while abroad, and re-entry into the U.S.

TDIS collects and maintains only information that is directly relevant to the lawful issuance of passports and the protection of the integrity of the U.S. passport as proof of U.S. citizenship at home and around the world. Information collected and maintained in TDIS is used only for those purposes.

d. How will the information be checked for accuracy?

Accuracy of the information on a passport application and submission of citizenship evidence is the responsibility of the passport applicant. Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The following authorities provide for the administration of the program supported by TDIS:

- 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 (Passports)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Given the inherent risks involved with collecting and storing PII, only the minimum amount of PII necessary to establish an applicant's identity and citizenship status is collected by TDIS. TDIS is determined to have a moderate "confidentiality impact level" due to the amount of potential harm that could result to the subject individuals and the organization if the PII in this system were exposed and/or misused. With the collection of passport data, TDIS has high data element sensitivity and high data subject distinguishability. These factors are mitigated through a very specific context of use, in that TDIS uses passport information for specific passport book or card production, and through a statutorily mandated obligation to protect confidentiality. Therefore, the confidentiality impact level is moderate.

The collection of passport data is the minimum amount of PII necessary to fulfill the statutory purposes of the system. Any remaining privacy risks inherent in the sources or methods of collection are mitigated by appropriate privacy and security controls detailed throughout this privacy impact assessment.

Specifically, there are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). The TDIS application data is protected by multiple layers of security controls including OpenNet security, TDIS application security, regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, firewalls, intrusion detection systems, antivirus software, and audit reports. If these controls were not in place, there would be an increased risk that individuals' PII could be accessed by unauthorized individuals.

4. Uses of the Information

a. Describe all uses of the information.

TDIS collects and maintains only information that is directly relevant to the lawful issuance of passports. The information is used only for that purpose. The term “passports” may refer to either the passport book or the passport card, which has been available since July 2008. The passport card facilitates entry and expedites document processing at U.S. land and sea ports-of-entry when arriving from Canada, Mexico, the Caribbean, and Bermuda. The card may not be used to travel by air. Otherwise, the card carries the rights and privileges of the passport book and is adjudicated applying the same standards.

Consular Affairs issues the passport card in response to the needs of border resident communities for a less expensive and more portable alternative to the traditional passport book. A previous passport book holder, eligible to use Form DS-82, may apply for a passport card as a “renewal.” First time applicants for a U.S. passport, and those not eligible to use the DS-82, must apply for a passport card using Form DS-11. A U.S. citizen may hold a book passport and a passport card at the same time.

An individual’s record is retrieved in TDIS by his or her name, Social Security Number, passport application number, passport book and/or card number, date of birth, or place of birth. Because records are retrieved by name and/or other unique identifiers, the system constitutes a Privacy Act system of records.

No technology or capability exists in the system to identify, monitor, track, or locate individuals in “real time.” Address and contact information of passport applicants is collected on their application or supporting documents. The information may reflect locations where the individual has interacted with a passport agency or center. Address and contact information is used only to contact or correspond with the applicant regarding his or her case, or by law enforcement under the authority of a routine use described in the System of Records Notice (SORN), for Passport Records, STATE-26.

b. What types of methods are used to analyze the data? What new information may be produced?

The passport number for the issued document is collected by TDIS when the application is finally approved. This passport number uniquely relates to a specific passport. TDIS also uses an

application number, separate from the passport number, to facilitate processing by passport specialists and other users or personnel working to process the passport.

Since August 2007, all domestic passport agencies and centers issue only electronic passport books, commonly called the “e-passport.” An e-passport is the same as a traditional passport with the addition of a small integrated circuit (or “chip”) embedded in the back cover. The chip stores:

- The same data visually displayed on the data page of the passport;
- A biometric identifier in the form of a digital image of the passport photograph, which will facilitate the use of facial recognition technology at ports-of-entry;
- The unique chip identification number; and
- A digital signature to protect the stored data from alteration.

The Department of State has taken extensive measures to prevent a third-party from reading or accessing the information on the chip without the passport holder’s knowledge. This includes safeguards against such nefarious acts as “skimming” data from the chip, “eavesdropping” on communications between the chip and reader, “tracking” passport holders, and “cloning” the passport chip in order to facilitate identity theft crimes. These safeguards are described in detail on the Department of State website, www.travel.state.gov.

The passport card contains a vicinity-read radio frequency identification (RFID) chip to meet operational needs of the Department of Homeland Security at land borders of the United States. This chip points to a stored record in secure government databases. No personal information is written to the RFID chip itself.

Checks against information in other Consular Affairs systems, particularly the Passport Information Electronic Retrieval System (PIERS), the Consular Lookout and Support System (CLASS), the Consular Lost and Stolen Passport (CLASP) Database, the In Process database (IPDB), Vital Passport Record Repository (ViPRR) and the Facial Recognition System, are performed by passport adjudicators to assist in determining whether or not to issue a passport. Administrative policies, based on approvals and quality checks, are established to minimize instances of faulty adverse determinations.

TDIS, and the personal information collected and maintained by TDIS, are not ingredients in any data mining activity as defined by federal law.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

The Social Security number provided by the applicant is checked against Social Security Administration (SSA) records (obtained via a feed from SSA) to determine the authenticity of the number.

d. Are contractors involved in the uses of the PII?

TDIS is a government system. It is supported by contract employees, some of whom are located at contractor-owned facilities. Direct-hire U.S. government employees have the sole responsibility for adjudicating passport applications to determine if applicants are U.S. citizens and qualify for passport issuance. Contractors support government employees by entering data, printing and mailing passports, and answering customer service inquiries.

Contractors involved in the passport fulfillment process (i.e., data entry, scanning, or correction of records or the printing and mailing of passports) are subject to a background investigation by the contract employer equivalent to a “National Agency Check” of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of TDIS hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by Diplomatic Security.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Since TDIS has a very specific use, generating and tracking passport books and cards for official travel, the potential privacy risk arising from “function creep” is negligible. Furthermore, since TDIS does not perform internal analytical functions on the PII, does not internally create new information about the record subject, and does not get data from sources other than the record subject, the potential privacy risk is further decreased.

All contractors involved in the development or maintenance of TDIS hardware or software must have at least a Secret-level security clearance. This includes a “National Agency Check” of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

5. Retention

a. How long is information retained?

A-13-001-21a Travel Document Issuance System (TDIS) - TDIS is a computerized system used to process passport applications at Passport Agencies in the United States

Description: a. TDIS Database (Passport Agencies). The database consists of passport information extracted from applications received and processed during the last six months at an agency.

Disposition: Delete data when 6 months old.

DispAuthNo: N1-059-96-5, item 21a

A-13-001-02 Passport Books: Recovered, Surrendered, Unclaimed or Found

Description: These passports books were issued to individuals who have returned them on their own initiative or at the request of the Department of State or other Government agency or have been found, recovered, and/or forwarded to Passport Services (PPT/TO/RS). They include Diplomatic or other official passports issued to military personnel who are either discharged, retired or deceased during the validity period of the passport; No Fee passports issued to Peace Corps volunteers; tourist passports; and all other passports.

Disposition: Destroy after receipt has been logged into PIERS database or successor electronic database. (ref. N1-059-96-5, item 2)

DispAuthNo: N1-059-04-2, item 2

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater the risk of unauthorized use or exposure. Second, the longer the records exist, the more likely inaccuracies will develop as a consequence of aging.

The secure handling of these reports is addressed during required DS training for access to OpenNet, and in the Consular Affairs Security Awareness and Training Plan. The TDIS screen views and printed reports will be marked as Sensitive But Unclassified (SBU) because of the PII contained in the database regarding the applicants (last name, first name, middle name/initial (if applicable), date of birth, place of birth, gender, social security number, telephone number, email address and mailing address). The hardcopy applications and softcopy images of applications and supporting documents are retained for 99 years.

The Department published record schedules that specifically dictate how long information in TDIS can be retained to ensure that information is not kept longer than is necessary. These schedules are followed to mitigate the risk of undue retention.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The Bureau of Consular Affairs oversees a network of facilities that may internally share or disclose the personal information collected and maintained in TDIS. These facilities include over

a dozen regional passport agencies, a special issuance agency, three national processing facilities, the National Passport Information Center, and the Headquarters offices in Washington, DC. United States embassies and consulates abroad also accept passport applications. Information is shared within these entities only for the purpose of issuing or denying a passport in accordance with the law.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Depending on which Consular Affairs facility is the point of receipt of an application form and supporting documents, the applications are entered into TDIS one-by-one or in batches. An application is converted to computer-readable format by a combination of data transcription and hard copy scanning. Once converted to a computer-readable format, any authorized users of TDIS may view personal information as appropriate based on their duties. Information is shared among authorized users by secure transmission methods permitted under Department of State policy for the handling and transmission of Sensitive But Unclassified (SBU) information.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or a general lack of training. To combat the misuse of information by personnel, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel screening.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The information collected by TDIS is generally in use from the point of receipt of an application to the time when a passport is issued or denied. The separate Passport Information Electronic Retrieval System (PIERS) operates in tandem with TDIS and provides access to a small subset of passport-related documents, typically only the applicant's passport application form including the photograph. In complex circumstances (e.g., suspicion of fraud) additional information is accessible through PIERS. These cases represent a small percentage of all records in PIERS.

Under the above arrangement, PIERS, not TDIS, is more commonly the system from which passport records are disclosed to external agencies under the authority of a published routine use. However, TDIS information may also be disclosed to external agencies having information on an individual's history, nationality, or identity, to the extent necessary to obtain information relevant to adjudicating an application, or where there is reason to believe that an individual has applied for or is in possession of a U.S. passport fraudulently or has violated the law. Information may also be disclosed to attorneys representing an individual in administrative or judicial passport

proceedings when the individual to whom the information pertains is the client of the attorney making the request.

TDIS information is shared with the Department of Homeland Security (DHS), and even more specifically with DHS' Customs & Border Protection (CBP). The connections of data flow are not direct through TDIS; other passport suite applications (e.g. PIERS, FEP, Passport Archive/PDITs, etc.) are the channels through which this data flows from TDIS to that external agency. The PIAs of those applications contain the details regarding their data exchanges and interfaces.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information is shared with external agencies by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to the information by external agencies is based upon agreements with those entities as to how they will use the data and protect it in accordance with the Privacy Act.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and the use of unsecured connections are also serious threats to external sharing. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associated with external sharing and disclosure including, but not limited to, formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements (SLA), annual security training, separation of duties, least privilege and personnel screening.

8. Notice

The TDIS system:

- contains information covered by the Privacy Act.
Provide number and name of each applicable system of records.
Passport Records – STATE-26
- does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Each published form associated with TDIS contains a Privacy Act statement in conformance with the requirements of the Act. Each form (including online web forms) exhibits an Office of Management and Budget (OMB) authorization number indicating it is an approved information collection. The website that provides applicants the ability to complete an electronic application contains a tailored website privacy policy that describes the terms of use of the personal

information provided. In addition, the publication of State-26 provides notice to the public of the type of information collected in TDIS.

b. Do individuals have the opportunity and/or right to decline to provide information?

An application for a passport is a voluntary action by a record subject. No provision exists within the law for an applicant to decline to provide part or all the information required on the passport application form.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Information collected on the passport application form is used for the sole purpose of processing the application in accordance with law. Limited, special, and/or specific uses of the information do not apply to this programmatic need.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notices offered in the Passport Records SORN, as well as the Privacy Act notice on the instructions of the passport application, are reasonable and adequate in relation to the system's purpose and uses. The fact that passport applicants voluntarily provide their information on the application and then voluntarily submit that application to the Department of State in and of itself mitigates the risk that applicants are unaware that the Department is collecting their information.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

TDIS processes Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR Part 171 Subpart D. The procedures inform the individual on how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to the system is limited to authorized Department of State staff having a need for access to the system in the performance of their official duties. All authorized government users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes the rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g., curiosity browsing). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning the logon.

The level of access for the user restricts the data that may be seen and the degree to which data may be modified. Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

Various technical controls are in place to deter, detect, and defend personally identifiable information. This is referred to as a multilayered approach. Monitoring occurs from the moment an authorized user attempts to authenticate to the network. From that point on any changes (authorized or not) that occur to data are recorded. If an issue were to arise, administrators of the system would review (audit) the logs that were collected from the time a user logged on until the time they signed off.

Ultimately it is very difficult to totally prevent an incident from occurring, but by implementing a multilayered approach, the risks can be greatly reduced.

b. What privacy orientation or training for the system is provided authorized users?

All TDIS users must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access users must complete annual refresher training.

All users must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice that describe the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Strict security controls are required by all Department of State systems that are authorized and approved to operate. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft are listed below:

- **Device Theft or Loss**
Lost or stolen laptops and other devices such as removable drives may contain Sensitive But Unclassified (SBU) information. This vulnerability is mitigated by the ban on personal computers, implementation of Web (virtual) technology to maintain data storage within the CCD, and extensive inventory control of removable drives.
- **Removable Media**
Removable media such as USB drives, CDs, DVDs, and MP3 players are prohibited on State Department networks.
- **Insider threat**
Disgruntled employees seeking revenge or inadvertent human error may release SBU information over the internet.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation

11. Technologies

a. What technologies are used in the system that involve privacy risk?

TDIS operates under standard, commercially-available software products residing on a government-operated computing platform not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in TDIS.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

TDIS does not utilize any technology known to elevate privacy risk. The current TDIS safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

a. What is the security assessment and authorization (A&A) status of the system?

The Department of State operates TDIS 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 August 30, 2015. This document was updated as part of the triennial reauthorization of the system.