

PRIVACY IMPACT ASSESSMENT

Passport Support Systems (PaSS)

1. Contact Information

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

2. System Information

- (a) Name of system: Passport Support Systems
- (b) Bureau: Consular Affairs
- (c) System acronym: PaSS
- (d) iMatrix Asset ID Number: PaSS 258780; 2DB 897; OPSS 898; PRISM 896; TDIS 89; TRIP 2677, VRS 4391
- (e) Reason for performing PIA:
 - New system – Logical Consolidated Boundary
 - 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) in order to receive an Authorization to Operate (ATO) status. PaSS is expected to receive an ATO by the Spring 2018.
- (c) Describe the purpose of the system:

PaSS is a logical business grouping of application systems that maintain travel document data on applicants requesting new and renewed passports. It consists of Electronic Passport Application Form (2DB), Online Passport Status Service (OPSS), Passport Records Imaging Systems Management (PRISM), Travel Document Issuance System (TDIS), Tracking Responses and Inquiries for Passports (TRIP), and Visa Request System (VRS).

2DB-Electronic Passport Application Form 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 and then prints the application and mails the application to the passport office. The following Department of State forms apply:

- 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”

OPSS supports the Bureau of Consular Affairs’ mission requirements to permit U.S. citizens who have applied for a passport but not yet received it to utilize the Internet and a standard browser to check the status of the passport application via a link from the travel.state.gov website. The OPSS application effectively provides U.S. citizens with quick and easy 24 hours access to their application status. As a result, the National Passport Information Center (NPIC) resources are more available to address questions that require specialized knowledge. The system requests identifying information from the applicant, retrieves the latest status of the passport application (i.e., received, working, approved, mailed) and returns this information to the user. The OPSS system receives status information from the Travel Document Issuance System (TDIS) repository server. The data that OPSS returns to applicants provides some assurance as to when their passports will be produced and when they are likely to be mailed. OPSS also enables U.S. citizens to submit an email address to receive electronic status updates via email generated from the OpenNet.

PRISM tracks issued applications after they have been shipped back to CA Passport Services, Bureau of Information Resource Management, Records Management (CA/PPT/IML/R) for records processing, and in support of the Bureau of Consular Affairs’ mission requirements for tracking the images attached to each application for a U. S. passport. The PRISM application is deployed at two enterprise centers, in thirty (30) agencies, and in select passport centers across the country with identical security mechanisms and functions.

TDIS supports the Bureau of Consular Affairs’ mission requirements to numerous U.S. Citizens who apply for passports domestically. TDIS was developed to provide assurance that applications for passports are processed in a timely manner; and that the production and issuance of machine-readable passports are properly managed in accordance with established Department of State (State Department) rules and regulations. TDIS is an integrated system utilizing both

commercial-off-the-shelf (COTS) and customized hardware and software that is used via OpenNet by authorized Department employees at passport agencies and centers . TDIS is the key application used for passport application/renewal processing at various passport agencies and processing centers around the country.

TRIP supports the Bureau of Consular Affairs mission requirements that allow Customer Service Representatives (CSR) to keep records of every contact and transaction with customers who contact the National Passport Information Center (NPIC) to inquire about the status of their passport application.

VRS produces letters that the Bureau of Consular Affairs Passport Services Directorate, Special Issuance Agency (CA/PPT/SIA) uses to help obtain visas from foreign embassies and/or consulates for official U.S. government travel. In all cases, SIA uses the Visa Request System (VRS) to generate a formal letter to the foreign embassy or consulate requesting the issuance of a diplomatic or official visa. In some cases, SIA provides the letter to the employing agency which interacts with the embassy itself. In other cases, SIA submits the completed visa application package, including the visa request letter, directly to the foreign embassy/consulate. As part of the process, SIA uses VRS to track and monitor the letters and visa applications sent to and collected from the respective foreign embassies/consulates.

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

2DB - U.S. Citizen: name, birthdate, Social Security number, phone number, personal address, email address.

OPSS - U.S. Citizen: name, birthdate, Social Security number, phone number, personal address, email address.

PRISM - U.S. Citizen: name, birthdate, Social Security number, phone number, personal address, email address, business address, images or biometric identifiers, substantive individual legal information, substantive individual personnel information, substantive individual family information.

TDIS - U.S. Citizen: name, birthdate, Social Security number, phone number, personal address, email address, business address, images or biometric identifiers, substantive individual legal information, substantive individual family information.

TRIP - U.S. Citizen: name, birthdate, Social Security number, phone number, personal address, email address.

VRS: US Citizen: passport number, book control number, passport type, issue date, expiration date, names, birthdate, birthplace, phone number(s), job title, country to visit, travel dates, human resource records, family information, such as spouse and child information, genealogical records, family assets, and foreign family members.

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

- 5 U.S.C. 552a (Privacy Act of 1974 as amended)
- 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 C.F.R. Parts 40-42, and 46 (Visas)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 22 U.S.C. Sec. 211a-218, 2651a, 2705 (Passport Application and Issuance)
- 22 U.S.C. 3927 (Chief of Mission)
- 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)
- 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

STATE-26, Passport Records, March 24, 2015

STATE-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016

STATE-39, Visa Records; October 25, 2012

Re: 2DB only. This 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 any personal identifier can be accomplished in this system.

The other systems will search by a personal identifier.

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

(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 .)

Schedule number Department of State Records Disposition Schedule:

A-13-001a,b,c & 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.

DispAuthNo: NC1-059-79-12, N1-059-04-02, N1-059-96-05 respectively.

A-13-001-21a,b, c&d Travel Document Issuance System (TDIS)

Description: TDIS is a computerized system used to process passport applications at Passport Agencies in the United States.

DispAuthNo: N1-059-96-05

A-13-001-23 - Routine Passport Application Status Check and Expedite Fee Upgrades E-mail

Description: Email messages regarding the status of passport applications and requests for expedited service.

Disposition Temporary: Destroy/delete when 25 days old

DispAuthNo: N1-059-98-03, item 1

A-13-002-02 Requests for Passports

Description: Copies of documents relating to selected passport requests.

Disposition: Temporary: Cut off at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 2

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-13-002-06 Visa Request System

Description: The Visa Request System (VR) is a system used to track and monitor the application process of obtaining visas from foreign embassies and/or consulates for official U.S. government travelers.

Disposition: Temporary: Cut off at issuance Destroy five (5) years after cutoff.

DispAuthNo: N1-059-09-25, item 1a

A-13-002-06a Intermediary Records

Description: The Visa Request System (VR) is a tracking system used to track and monitor the application process of obtaining visas from foreign embassies and/or consulates for official U.S. government travelers. Records include:

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

Type of information retained in the system:

Records related to passport processing for U.S. citizens

It should be noted that prior to 1999, records of some data were stored in microfilm or silver halide. Records in the systems are files associated with a U.S. citizen applying for and receiving, or being denied, a U.S. passport.

4. Characterization of the Information

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

- Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)
- U.S. Government/Federal employees or Contractor employees
- Other (are not 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 and

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?

2DB - Information 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 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).

OPSS - receives information by two methods:

- (1) From a system - Passport status information from the Travel Document Issuance System (TDIS) repository server. OPSS pulls the status information from TDIS to the OPSS database.
- (2) From the applicant - Once the status information exists in the database, U.S. Passport applicants can use the public-facing website to inquire about the status of their passport application. OPSS collects the last four digits of the applicant's Social Security number (SSN).

PRISM - Information is collected by various means i.e., entered by hand and scanned directly from the paper-based application packages for document preparation, and quality control prior to being archived.

TDIS – receives information by two methods:

- 1) From a system - Department of State computer systems, passport acceptance agents, the Social Security Administration, the lockbox provider (CITIBANK) system, passport specialists, and fraud prevention managers.
- 2) From the applicant –The applicant may complete a form and take it to the agency or center where government employees then input the data into TDIS.

TRIP - The information in TRIP is collected from the applicant (over the phone) and input by the NPIC Customer Service Representative (CSR).

VRS: The data in VRS is collected from a combination of

- 1) The traveler's diplomatic or official passport,
- 2) U.S. government travel orders and/or an official memorandum from the traveler's employing agency, and/or
- 3) Country-specific visa applications completed by the traveler or the employing agency.

All foreign visa requests processed through this system require official notification from the State Department that the traveler/employee is going on official travel to represent the U.S. government. This notification is created through VRS which generates cover letters that accompany visa request packages. The letters generated by VRS are considered ancillary in our process, but several foreign countries now consider them to be an essential step in providing visas in diplomatic and official passports.

(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?

2DB - 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.

OPSS - Pulls passport application status information from the Travel Document Issuance System (TDIS) repository server; thus, erroneous data/information is cross-referenced with the TDIS data repository which is also owned and operated by CA. Information input by applicants to check the status of their passports is also validated against stored information.

PRISM - Developed in order to scan and track the application and images attached to each application for a U. S. passport. Scanning is done only after the application has been completely processed; the passport application must already have undergone adjudication, and the passport book printed and delivered to the customer, or the application must have been denied. 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.

TDIS - 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.

TRIP - Information requested of phone-callers is confirmed against the information on the passport or passport application contained in Travel Document Issuance System (TDIS). Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimized instances of inaccurate data.

VRS: The data received from applicants on the application is verified primarily by a manual review and comparison of the information on

- 1) The traveler's diplomatic or official passport,
- 2) The U.S. government travel orders or an official memorandum from the traveler's employing agency, and
- 3) country-specific visa applications completed by the traveler or the employing agency.

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

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

OPSS - The applicants are responsible for ensuring that the information is current when they request the status of their passport application. After submission, the data flow of the entire Passport suite of applications takes over to verify that the data is legitimate and complete. All of the upstream CA systems for the Passport suite (TDIS, PIERS, and PRISM to include archival data for previously issued passports) are involved in adjudication and production of a passport. These systems come together in multiple layers of interaction for identity verification, including external outreaches to Social Security Administration (SSA) Live and other 'Namecheck' avenues. The passport applications are vetted thoroughly for accuracy. OPSS receives its data through these applications' "handshakes" to show correct data.

PRISM - The applicant does not access this system; it is accessible only to State Department Intranet personnel (employees with an OpenNet account). It is a repository for scanned applications and supporting documentation. The applicant is responsible for ensuring that the information is current in the application sent in for a passport. The information supplied on passport applications is assumed to be current until such time that the individual fills out a new form to update his/her passport information.

TDIS – Passport applicants are responsible for ensuring that the information is current at the time of submission. Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established for currency and accuracy of information.

TRIP - If the application appears in TRIP (which mirrors information in TDIS) and any of the information is incorrect (when the CSR verifies it with the passport applicant), the CSR will request the correct information from the passport applicant and will send a notification email to the adjudicating passport agency requesting an update to the applicant's information in TDIS.

VRS: The VRS source information is the previously issued U.S. government passport for the individual attempting to acquire a government issued travel visa. If the information on the previously issued U.S. passport becomes out of date, it is up to the individual to apply for a new U.S. passport. If the U.S. Government employee requires the services of VRS, he/she would provide the new passport information and his/her collected data would be updated by scanning the passport. VRS's main function is to provide a coversheet for the travel visa application.

VRS staff inputs data into the system to facilitate the process of receiving a travel visa; the cover sheet is printed out and provided to the traveler to verify the information on it is correct. If the traveler states that the information is correct but it is determined to be incorrect, the traveler will not receive the requested visa. The package will be returned and the traveler contacted to update information that may be inaccurate.

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

Yes, TDIS uses commercial information from CITIBANK that is transferred by CDITS (Consular Data Information Transfer System) to TDIS via the Consular Consolidated Database (CCD). The other systems do not use commercial or publicly available information.

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

2DB - 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.

OPSS – Yes, a PAS has been developed which is prominently displayed on the webpage that collects the PII.

PRISM – A Privacy Act Statement is not required for this system. It is not accessible to the public, only to State Department intranet personnel. The scanned documents in PRISM are the paper forms filled in and signed by the applicant. The paper forms contain a Privacy Act statement.

TRIP – A Privacy Act statement is not required for this system. It is not accessible to the public, only to State Department intranet personnel. Individuals are verbally briefed on the uses of their information at the beginning of the phone call, prior to collection.

TDIS– A Privacy Act statement is not required for this system. It is not accessible to the public, only to State Department intranet personnel. Each printed form associated with TDIS contains a Privacy Act statement.

VRS: A Privacy Act statement is not required for this system. Access to the system is restricted to internal Special Issuance Agency (SIA) staff (no public or other government user access). When a government employee is preparing to travel and requires a visa, the employee contacts the SIA to provide information necessary to complete the cover letter which will accompany the visa application.

The applicant is verbally briefed (phone or in person) on the required notice:

1. The purpose for which the information is required.
2. The possible uses of the information
3. How the data is protected from unauthorized/ illicit disclosure.
4. The potential consequences if the applicant declines to provide the data (i.e., that his/her visa application may be declined).

(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: The system 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.

- PRISM:** The system is accessed only by Intranet personnel. Paper forms the applicant fills in have a PAS. Consent is provided when the applicant completes and submits the form.
- TRIP:** Individual callers have the option to not provide information to the Customer Service Representative, or to hang up; however, this may result in the caller not being provided the services desired.
- TDIS:** The system is accessed only by Intranet personnel. Printed paper forms have a PAS. Consent is provided when the applicant completes and submits the form.
- VRS:** The applicant is verbally briefed (by phone or in person) on the required notice to include the potential consequences if the applicant declines to provide the data (i.e., that his/her visa application may be declined).
- OPSS:** The system 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 Question 3d is the minimum necessary to perform the actions required by this system. 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 collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

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

PaSS maintains passport applicant data for those requesting first time or renewal passports and keeps a record of the decision to grant or deny. Documents in the application package are scanned and archived. Each contact the State Department has with an applicant, whether the applicant requests passport status online or calls the NPIC, is recorded and maintained in PaSS.

- (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 for which the systems were designed –to provide a business grouping of application systems that maintain travel document data on applicants to process requests for new and renewed passports.

- (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?

2DB: Does not analyze information

OPSS: Provides statistical workflow reports that do not include any PII

PRISM: Does not analyze information

TDIS: Does not analyze information

TRIP: Uses compare and contrast to verify that the caller-provided information matches what is in the system for that person, after the CSR inputs it.

VRS: Does not analyze information

(2) Does the analysis result in new information?

Yes

OPSS – Only the statistical data is new and it does not include PII.

TRIP – If the “compare and contrast” indicate discrepancies, new information about the discrepancy is created and the applicant is contacted for correction of data.

No - 2DB, PRISM, TDIS

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

Yes – TRIP discrepancy information

No – 2DB, OPSS, PRISM, TDIS

(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 - TRIP

No - 2DB, OPSS, PRISM, TDIS

6. Sharing of Information

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

INTERNALLY: The following internal Department of State systems are used within the Bureau of Consular Affairs to process passport and visa applications:

2DB - Printed Barcode with Passport Application Information will be scanned to upload into TDIS, CLASS. The information can be accessed in TDIS and CLASS by authorized users internally within the Department of State Bureau of Consular Affairs. Authorized OpenNet users are cleared Department of State personnel who have been granted access to the 2DB. OpenNet

users use Single Sign-on to access the enterprise which provides access to the 2DB application. The 2DB Reporting Tool is primarily used by management. 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.

OPSS – Passport status and email address are shared internally within the State Department with TDIS allowing the NPIC CSRs to query in response to an applicant’s passport status questions.

PRISM – Images are shared with Passport Information Electronic Records System (PIERS) and TDIS users as needed for passport processing/questions. PRISM exchanges passport applicant data with PIERS through the ViPRR (Virtual Passport Records Repository) database. PIERS provides authorized users at domestic passport agencies and overseas posts with the ability to query information pertaining to previously processed passport applications and vital record data for the purpose of adjudicating passport applications, and for confirming citizenship and eligibility of persons to receive other consular services.

TDIS – Images are shared with PRISM for passport processing. Information (Social Security number (SSN), passport application number, the applicant’s last name and date of birth) is shared with TRIP. TDIS also works in tandem with PIERS to provide a small subset of passport related documents. Complex cases may require more information obtained via PIERS.

TRIP - Information is shared between TRIP and TDIS. Social Security number (SSN), passport application number, the applicant’s last name and date of birth are shared in order for the State Department’s Consular Affairs personnel to retrieve records through TRIP in response to an applicant’s passport status inquiries.

VRS - The State Department’s Special Issuance Agency uses VRS to monitor the letters, passports, and visa applications sent to and collected from embassies and consulates.

EXTERNALLY

PRISM – Data on the scanned images - photo, name, date of birth, passport number and expiration number along with adjudicator notes are shared with the Department of Homeland Security, Customs and Border Protection (CBP). Images are viewable via PIERS and may be shared with courts or law enforcement as required by law.

TDIS - Information may be disclosed to external Federal and State 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.

2DB, OPSS, TRIP, and VRS do not share externally.

(b) What information will be shared?

Answered in (a) above.

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

Answered in (a) above.

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

2DB – Data in 2DB is not transmitted electronically. The application is printed with a barcode containing all the data. TDIS and CLASS scan the barcode to upload the data.

OPSS – Information is shared by utilizing the State Department secure internal network. The sharing is permitted based on State Department policy for the handling and transmission of sensitive but unclassified (SBU) information.

PRISM – PRISM is available only on the Department of State intranet, installed on particular CA domain workstation desktop images. All connections and data integration endpoints between passport systems is operated and maintained by CST (Consular Shared Tables). Hence, information is shared 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.

TDIS – 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.

TRIP – Information is shared between TRIP and TDIS by secure transmission methods permitted by Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

VRS - Does not share information.

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

2DB, OPSS, TRIP - 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.

PRISM – Controls built into the Department of State intranet, including routers and Network Intrusion Detection Systems (NIDS), provide network level controls that limit the risk of unauthorized access from all IP (Internet Protocol) segments. CA systems that interface with PRISM are strictly controlled by routers and NIDS rule sets that limit ingress and egress to PRISM.

Safeguards in place for internal sharing arrangements are done by secure transmission methods (methods detailed at end of this section) permitted by State Department policy for the handling and transmission of sensitive but unclassified (SBU) information. Memorandums of Understanding (MOU/MOA) are in place with other government agencies. All physical 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.

Safeguards in place for external sharing arrangements with other government agencies are utilizing secure transmission methods and data shares. When data is shared with DHS, all components are required to comply with the both the Department of State's and the Department of Homeland Security's security policies and procedures. All communications shared with external agencies are encrypted.

Details of the Secure Transmission Methods

All systems like PRISM use TCP/IP (Transmission Control Protocol/Internet Protocol) to assist with its 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, systems employ the use of Hash message authentication codes to sign packets verifying that the information received by the system from the Internet is exactly the same as the information sent. The transmissions are secured using digital certificates (including web-based Secure Socket Layer (SSL) certificates),

and all cryptographic keys. The connection between all the sites that the system servers reside on is protected using SSL with 128-bit data encryption using SSLv3.1/TLSv1.

TDIS - 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.

VRS - Does not share information.

- (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:

- a. 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. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.
- 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 shared with external agencies 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?

All applicants can follow instructions for gaining access as stated in SORNs State-26 and State-05. They may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA web site for the privacy policy which includes instructions on how to obtain access by contacting the listed offices by phone or by mail.

In addition, more specific access to information in these systems is outlined below:

2DB – This system does not store any information; what was input is on the printed form.

OPSS – This system is used only to track passport status. Applicant visits the website, input requested information and can view the information.

PRISM – Applicants can contact the representative who assisted them and request to review their information.

TDIS - Applicants can contact the representative who assisted them and request to review their information.

TRIP - Applicants can contact the NPIC and request to review their information.

VRS – The applicant cannot access the system directly. The applicant is verbally briefed (by phone or in person) on how to find out what information about them is in the system and how to correct it when needed. Applicants can contact the representative who assisted them as well as refer to the above listed sites.

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

Yes No

If yes, explain the procedures.

All applicants can follow instructions for requesting changes to their information as stated in SORNs State-26 and State-05. They may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA web site for the Privacy Policy which includes instructions on how to request changes by contacting the listed offices by phone or by mail.

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

Individuals are notified of the procedures to correct records in these systems by a variety of methods:

1. During their interview; after, applicants can contact the representative who assisted them
2. Published SORNs
3. Department of State Privacy Act Website
4. Link on Web pages to Department of State Privacy Policy
5. Instructions on forms or web pages where the data was input
6. Being notified by letter or email that a correction is needed

Each method contains information on how to amend records and who/what office to get in touch with as well as providing contact information.

If no, explain why not.

8. Security Controls

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

The system 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.

Access to applications/databases is further protected with additional access controls set at the application/database level. All system accounts/access must be approved by the user's supervisor and the Information System Security Officer (ISSO). The audit vault system is used to monitor all privileged access to the system and violations are reported to senior management daily, if applicable. Data shared with other government agencies is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by authorizing officers of each agency.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable NIST 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately.

(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 system, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and 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 PIV/CAC and PIN (Personal Identity Verification/Common Access Card and Personal Identification Number) 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. 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 and CA ISSO, in conjunction with the CA 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 CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with DS Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with DS Security Configuration Guides, auditing is enabled to track the following events on the host operating systems and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

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 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 system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier,

date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

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 annual security/privacy training is required for all authorized users including regular refresher training. Each user annually must complete the Cyber Security Awareness Training and pass the Privacy Act PA-459 course entitled, “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 sign that they 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. 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?

The information collected, if exposed to unauthorized users may include inconvenience, distress, or damage to standing or reputation, financial loss, harm to State Department programs or the

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- OpenNet-based Users, System Administrators, Database Administrators
OPSS- Internet Users, OpenNet-based Users, System Administrators, Database Administrators
PRISM - PRISM Users, OpenNet-Based User, System Administrators, Database Administrators
TDIS- OpenNet-based User, System Administrators, Database Administrators
TDIS- OpenNet-based User, System Administrators, Database Administrators
VRS - System Administrators and Special Issuance Agency staff

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

Access is determined based on requests which are approved by the supervisor and 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 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 ISSO approves to perform official duties.

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

-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.