DataShare

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Information Sharing Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: February 2, 2009

(b) Name of system: DataShare

(c) System acronym: DS

(d) IT Asset Baseline (ITAB) number: 561

(e) System description:

The Department of State (DoS) manages the visa process necessary for foreign citizens to visit or immigrate to the United States of America. In pursuit of this mission, DoS must communicate with a number of external agencies to share information about visa applicants for the safety and security of all American citizens. This communication has become more important following September 11, 2001, with increased scrutiny and publicity placed on the U.S. Visitor and Immigrant Status Indicator Technology System (US VISIT). US VISIT is an automated entry/exit system used to capture two finger prints which are run through a database to verify identity and ensure the foreign visitor is eligible to enter the United States, and provides a digital photograph of foreign visitor upon entry to the United States.

The mission of the DataShare system is to provide reliable, secure, high-performance connectivity between DoS and Department of Homeland Security (DHS) to support interagency exchanges of passport and visa data. Visa data originates at either an overseas post or at the National Visa Center (NVC) and is reformatted to meet DHS system requirements. DataShare transfers the data to DHS's Interagency Border Inspection System\Treasury Enforcement Control System (IBIS\TECS), the US VISIT system and the Computer Linked Application Information Management System 3 Mainframe (CLAIMS MF).

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): Annual Assessment

(h) Date of previous PIA (if applicable): May 27, 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII.

☒ does contain PII.

a. What elements of PII are collected and maintained by the system?

DataShare manages the transmission of PII between systems, but does not collect any information. DataShare transmits PII from visa applicants, including the various types of Immigrant Visas (IV), Non-Immigrant Visas (NIV), and Student Exchange Visas (SEVIS). DataShare also covers passport data, which consists of personal information of the passport holder and passport document information, and is collected at the regional passport agencies and transferred to the DHS/CBP.

b. What are the sources of the information?

DataShare receives data from the Consular Consolidated Database (CCD) and/or US VISIT systems from DHS. Visa data originates at either an overseas post or at the National Visa Center (NVC) and is reformatted within CCD to meet DHS system requirements. DataShare transfers the data to DHS's Interagency Border Inspection System\Treasury Enforcement Control System (IBIS\TECS), the US VISIT system (IDENT) and the Computer Linked Application Information Management System 3 Mainframe (CLAIMS MF). Additionally, a DHS/ICE system called SEVIS also sends data to the CCD.

c. How is the information collected?

Information in the DataShare is collected directly from individual visa and passport applicants and supplemented with data from DHS systems. The DataShare software was designed to be a transport mechanism for data between the Bureau of Consular Affairs (CA) and offices within DHS, not a front-end user interface for accepting data from any individual.

d. Why is the information collected and maintained?

DataShare exchanges current passport and visa data with various organizations within DHS to enhance security at immigration points around the world. The DataShare initiative bears responsibility to ensure reliable, secure, high-performance connectivity between DoS and DHS.

e. How will the information be checked for accuracy?

At collection, it is the responsibility of the data subject to provide accurate data when applying for a visa or passport. When sharing with DHS, DataShare verifies the format and field validity of the information being sent through the connection that is initiated with DHS.

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

- The Patriot Act and the Enhanced Border Security Act;
- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports);
- 8 U.S.C. 1101-1503 (Immigration and Nationality Act of 1952, as amended);
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports);
- 8 U.S.C. 1185 (Travel Control of Citizens);
- 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and assistance to other agencies); and
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries).

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

The personally identifiable information (PII) collected and maintained within DataShare is the minimum amount of data required to perform its unique and critical mission to national security. The large amount of PII contained within DataShare requires a heightened level of security and access controls, which have been met by assigning a security categorization level of “High” to the system.

Only authorized users with a “need to know” are granted access to the application. Users are periodically reminded by both the Department and the Bureau of Diplomatic Security (DS) of their responsibilities in the protection of the data in the DataShare application.

Controls built into the Department of State’s intranet, OpenNet GSS, including routers and Network Intrusion Detection Systems (NIDS), limit the risk of unauthorized access from all Internet Protocol (IP) segment CA systems that interface with the DataShare . This prevents the risk of cyber crime such as hacking and disallows the loss of data that could be compromised and used for criminal intent to cross borders or commit false identity when using a passport or visa.

4. Uses of the Information

a. Describe all uses of the information.

DataShare exchanges current passport and visa data with various organizations (entry Points in the United States and Canada) within DHS to enhance security at immigration points around the world. No data analysis is preformed on the DataShare side.

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

DataShare is the mid-level mechanism for transporting data between the CCD and DHS. The data is checked through application coding verifying the format and field validity of the information being sent through the connection. No new information will be produced.

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

Visa and passport applicant data provided by applicants and/or foreign authorities is used to effectively identify the applicant. No publicly available information is used.

d. Is the system a contractor used and owned system?

DataShare is a government off the shelf (GOTS) product and is not owned by contractors. Data will not be accessed in the DataShare system as it only transmits packages. There are no end users of the DataShare system. Only contract operational support personnel have the ability to access the data packages contained within DataShare if necessary.

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.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are 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. The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for the NIV application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

5. Retention

a. How long is information retained?

DataShare only serves as a transport system between DHS and DoS applications and does not retain data, except for what is replicated into the CCD. In this regards the CCD retention can be found in the CCD Privacy Impact Assessment.

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

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

Information is shared by secure transmission methods permitted under the Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. DataShare backup information is protected from unauthorized modification

by the physical security and access controls in place at several locations at State Annex 1 (SA-1). Only cleared technical personnel (government and contractors) are allowed to access the server room housing DataShare servers, and no one is allowed to access the system until the appropriate background screening has been completed.

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?

DataShare does not share information with internal DoS applications. It collects information from the Consular Consolidated Database (CCD) to prepare data for external sharing, detailed below.

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

DataShare does not share information with internal DoS applications.

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

DataShare does not share information with internal DoS applications.

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?

External information is shared with the following:

The following DoS systems share visa and passport data with DHS to assist US VISIT in verifying identities of foreign visitors to the United States, to ensure the foreign visitor is eligible to enter the United States, and to provide a digital photograph of foreign visitor upon entry to the United States.

System Release	Purpose
• Consular Affairs Transfer Server (CATS)	Consular Affairs Transfer Server (CATS) exchanges US-VISIT packages with DHS using File Transfer Protocol (FTP)
• Websphere Message Queuing	For the communication of IV, NIV, US-Visit, Class, and Passport data between DataShare and DHS, a WebSphere message queuing (MQ)/Oracle advanced queuing (AQ) solution is used.

System Release	Purpose
• Immigration Visas (IV)	Formats IV adjudication information in the case of a visa issuance into an issuance data package submissions to DHS's Interagency Border Inspection System (IBIS), Treasury Enforcement Control System (TECS
• Non-Immigrant Visas (NIV)	Formats NIV adjudication information in the case of a visa issuance into an issuance data package submissions to DHS's IBIS/TECS.
• Passport (Consular Data Information Transfer System)	Transfers Passport data between DoS and DHS

• U.S. Visitor and Immigrant Status Indicator Technology System (US VISIT) (DHS)
  • US VISIT (Issuance/Refusal)
  • US VISIT (Return Package)
  • US VISIT (Visa Applicant)
	The MAILN[?] US-VISIT Visa Applicant and Issuance/Refusal applications format adjudication information from the IV IADEG and NIV IADEG components into visa applicant package submission to DHS's US-VISIT system. The DataShare Return Package application reformats return information from DHS for replication back to Post IV and NIV systems.

• Student and Exchange Visitor Information System (SEVIS)	Receives XML files with student/exchange visitor information from DHS's SEVIS and maps the data fields to the appropriate CCD tables for further processing by IV IADEG and NIV IADEG.
• Advanced Host Monitor (Hostmon)	Hostmon provides remote monitoring for all servers and applications within the DataShare accreditation boundary.

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

Department of State OpenNet security protocols are used to ensure that the data packages are being transmitted in a secure environment through the DoS network. Outside of the DoS network DataShare employs the use of the DataShare Security Enclave.

Data collected from DHS is transmitted over a three-tiered security enclave that provides aggregated communications services over secured encrypted private frame relay circuits between the DHS components and DoS. This means there are encryptors on each side of the link to encrypt the data before it is provided to the telecommunications vendor for transmission.

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

External sharing occurs only with authorized users who are cleared U.S. government employees or contractors with work-related responsibility, specific to the access and use of the system's data. No other internal disclosures of the information/data within the State Department are made.

Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) requirements are strictly adhered to in order to ensure any risk is addressed through the user-authorization process.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

The information in this system is covered by STATE-05, Overseas Citizen Services Records, last amended May 2, 2008 at 73 FR 24342-24345.

☐ does not constitute a system of records covered by the Privacy Act.

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

Passport Records: Each published passport application form contains a Privacy Act statement in conformance with the requirements of the Act. Each form (including online web forms) exhibits an 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.

Visa Records: The information provided by the visa applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). The visa application form provides a statement explaining that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

Also, notice is provided in the System of Records Notice Overseas Citizen Services Records, STATE-05.

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

Information is given voluntarily by the applicants and with their consent, by family members and other designated agents. Individuals who voluntarily apply for a U.S. visa or passport

must supply all the requested information and may not decline to provide part or all the information required, if they wish to obtain visa or passport services.

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?

Applicants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

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 notice provided to the public by the Systems of Records Notice STATE-05 is reasonable and adequate in relation to the system's purposes and uses, its applicable legal requirements and sensitivity of the PII collected.

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?

The information in DataShare is considered a visa record subject to confidentiality requirements under INA 222(f) and passport records subject to the Privacy Act of 1974.

Visa Records: Visa applicants may change their information at any time prior to submission of the application to the consulate or embassy. Once that is done, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request and this guidance is available to the public in 9 FAM 40.4:

Formatted: Underline

i. Correspondence previously sent to or given to the applicant by the post;
ii. Civil documents presented by the applicant; and
iii. Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

Visa applicant information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a) and individuals may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Passport records: Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa 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 171.32.

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

To the extent information in DataShare may be Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements.

Therefore this category of privacy risk is appropriately mitigated in DataShare.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access?

There are no end users of the DataShare system. Only operational support personnel have the ability to access the data packages contained within DataShare if necessary.

What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The system maintains a system log of events for the backend database and operating system as well. Database and system administrators are responsible for reviewing system audit logs. Audit logs are reviewed on a bi-weekly basis.

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

All users are required to undergo computer security and privacy awareness training prior to accessing the system and must complete refresher training yearly in order to retain access.

Every user must attend a security briefing prior to receiving access to Department of State networks and a badge for facility access. This briefing is sponsored by DS/SI/IS and also includes the Privacy Act of 1974. Users must also take a Departmental information system security briefing and quiz prior to receiving access to a DoS network.

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.

Access control lists define who can access the system and at what privilege level and are regularly reviewed; inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.) Therefore, no such residual risk is anticipated.

11. Technologies

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

DataShare operates under standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or

technologies. No technologies commonly considered to elevate privacy risk are employed in DataShare.

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

No such risk is anticipated. The safeguards are described in paragraph 10 above.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates DataShare 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. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, DataShare is certified and accredited through August 31, 2011.