PRIVACY IMPACT ASSESSMENT

Consular Data Information Transfer System (CDITS) PIA

1. Contact Information

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

2. System Information

(a) Name of system: Consular Data Information Transfer System (CDITS)

(b) Bureau: Consular Affairs

(c) System acronym: CDITS

(d) iMatrix Asset ID Number: #964

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

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 CDITS Authorization to Operate (ATO) is planned to be received by Winter 2020.

(c) Describe the purpose of the system:

CDITS is a communication infrastructure system used to exchange data/information in support of Consular Affairs (CA). CDITS is a General Support System (GSS) composed of several connections that assist with the transfer of visa, passport and other information on individuals from external agencies to the Department of State. CDITS provides a reliable, secure, and high-performance connectivity for transferring lookout, passport, visa and drug enforcement related information between the Department of State and external agencies for dissemination to internal CA systems to assist in processing passports and visas. All CDITS communications are encrypted using either hardware encryption, software encryption, or in some cases, both. CDITS does not have any end users.

Only connections that handle personally identifiable information (PII) of U.S. citizens are addressed after this section in this PIA. The CDITS connections with the following entities are used to transfer data:

- **The Bank** -Passport application data is gathered by the commercial bank (referred to as "the Bank"), which processes paper passport applications and the associated application fees. The Bank Lockbox Connection (referred to as the "Lockbox") then transfers this application data to the CDITS servers. The passport application data is then transferred via the State Department intranet in a secure manner to the Travel Document Issuance System (TDIS) to be maintained as a final record.

- **Government Printing Office (GPO)** - CDITS allows the GPO to transmit passport book shipment and product data to Department of State passport agencies and centers over a server-to-server Secure File Transfer Protocol (SFTP) connection. The data transferred via this connection does not contain PII and will not be discussed after Section 3.

- **United States Postal Service (USPS)** - CDITS allows passport agencies and centers to transmit a file containing a manifest of used tracking numbers to USPS over the internet. The USPS responds with an audit file indicating receipt of the manifest. Data is encrypted using Secure Shell File Transfer Protocol (SFTP). The data transferred via this connection does not contain PII and will not be discussed after Section 3.

- **Drug Enforcement Agency (DEA)** - The Drug Enforcement Agency (DEA) is a Department of Justice (DOJ) entity. CDITS receives a daily file with visa additions, updates and deletions. The File Transfer Protocol (FTP) server in the demilitarized zone (DMZ) uses virtual directories to get the file. The FTP client in OpenNet pulls the file from the DMZ FTP server on a daily basis. The Bureau of Information and Resource Management (IRM) controls all of the network equipment at both ends, up to the router at DOJ. This connection goes through the Other Government Agency (OGA) firewall and a DMZ switch.

- **Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC)** – The FBI is a Department of Justice entity. NCIC sends a daily file containing passport information to CDITS via FTP over encrypted network data links. CDITS then routes the file to the State Department namecheck application. The communication between CDITS and the FBI is protected using Federal Information Processing Standards (FIPS) 140-2 compliant hardware encryption devices.

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

- **The Bank** – CDITS securely transfers passport application biometric data and PII, including names, sex, date and place of birth, mailing addresses, email addresses, telephone numbers, financial information, most recent passport book and card numbers, date and place of any name change, height, hair color, occupation, name of employer, Social Security Number (SSN), and the name, address, and phone number of an emergency contact from the Bank to the CDITS servers and then to the State Department Travel Document Issuance System (TDIS) for further processing. The data is located in a "lockbox" (electronic location secured). While there is no established scheduled on either side, CDITS is continually checking, typically once an hour, for data to collect.

- **Drug Enforcement Agency (DEA)** – CDITS receives a daily flat file with visa additions, updates and deletions. This information includes qualifying records from the Narcotics and Dangerous Drugs Information System (NADDIS) database: name, date of birth, gender, country of birth, occupation, alias name(s), physical description (height, weight, race, eye color, and hair color), biometrics, armed-dangerous indicator, and comments (including significant information about the relevant drug case).

- **Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC) -** NCIC sends a daily email containing a "Loss of Nationality" file which includes names and SSNs.

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

- 22 U.S.C 2651a (Organization of Department of State)
- 8 U.S.C. 1101-1105a; 1151-1363a; and 1401-1504 (Titles I, II and 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)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 22 C.F.R. Parts 50 and 51 Subchapter F (Nationality and Passports)

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

☒Yes, provide:

- SORN Name and Number:

STATE-05 Overseas Citizens Records and Other Overseas Records, September 8, 2016
STATE-26 Passport Records, March 24, 2015
STATE-39 Visa Records, June 15, 2018

Although the system was not designed nor is used for searches, the capability is there during the approximately 30 minutes that data resides in the system.

☐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 .)

CDITS provides data transport services and stores no data.

If yes provide:
Schedule number, Length of time the information is retained in the system, and Type of information retained in the system:

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☐ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

CDITS does not collect social security numbers. SSN information in CDITS is acquired from other external systems. PII is maintained (temporarily) for dissemination to Consular Affairs (CA) information systems for use by CA personnel. CDITS routes data to other State Department CA systems for use in processing visa and passport applications. The system does not perform any processing of the data.

- If yes, under what authorization?

(c) How is the information collected?
No information is entered into CDITS by the public. The data collection methods from each source are as follows:

- **The Bank** - The Bank provides lockbox services for passport application processing. The bank enters information where it is held in an electronic, secured lockbox, which CDITS monitors for data and electronically pulls.

- **DEA** - DEA sends a daily flat file with visa additions, updates and deletions to CDITS.

- **FBI NCIC** - NCIC sends electronic files containing passport and visa information through CDITS that is transferred to the Diplomatic Security Office via CA systems.

(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?

CDITS does not utilize a process to determine if the information collected is accurate because CDITS itself does not collect the information. That process is done outside of CDITS' scope by the respective agencies listed in 4(c) managing their own data collection.

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

CDITS does not utilize a process to determine if the information collected is current because CDITS itself does not collect the information. That process is done outside of CDITS' scope by the respective agencies listed in 4(c) managing their own data collection.

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

No, the system does not acquire or use information from commercial sources nor is the information publicly available. CDITS is an internal "routing" mechanism to disseminate information to Consular Affairs systems from external systems outlined in paragraph 3(c).

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

CDITS does not provide notice to an individual prior to the collection of Personally Identifiable Information (PII) because individuals do not interface with or provide CDITS with PII; that would be the responsibility of the specific system collecting the information which is managed by the external organizations listed in 4(c).

(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?

- If no, why are individuals not allowed to provide consent?

Individuals are not provided the opportunity to consent within CDITS (the information system) because CDITS does not collect information from individuals. However, the external systems that utilize CDITS do collect information from individuals and it would be the responsibility of those systems to provide individuals with the opportunity to decline to provide the information or to consent to a particular use of information.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII handled by CDITS was taken into consideration during the design phase when determining how to preserve the confidentiality and integrity of the information. The Department of State understands the need for PII to be protected. Accordingly, the PII in CDITS is handled in accordance with federal privacy regulations regarding the transmission of PII. CDITS only collects the information necessary for the processing of passport and visa applications and purposely does not store the information for search purposes, but rather, it serves as a transport to various State Department systems responsible for the storage and use.

5. Use of information

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

CDITS routes passport and visa application PII data to other State Department systems for use in processing application request services. CDITS does not process any data.

(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, CDITS uses the information in a manner that is consistent with the purpose for which the system was designed, i.e., to acquire information from external agencies and transmit internally to CA systems to manage passport and visa operations**.** The information is not stored or used within CDITS for any other purpose.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?
(2) Does the analysis result in new information?
(3) Will the new information be placed in the individual’s record? ☐Yes ☐No
(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

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

Internally: Information identified in paragraph 3(d) is shared with the following CA systems: Consular Consolidated Database (CCD), which includes the Consular Lookout and Support System (CLASS), Travel Document Issuance System (TDIS), American Citizen Services (ACS), and Front End Processor (FEP).

Externally: Information is received from DEA, the FBI, and the bank as outlined in paragraph 3(d).

(b) What information will be shared?

Internally: The PII identified in paragraph 3(d) is shared with the CA/CST systems listed above in paragraph 6(a).

Externally:

- **The Bank** – Bank administrators prepare the photo and biometric data for the CDITS server pick-up. As the passport application and photo image files become available, CDITS initiates the file transfer from the bank server to the CDITS server. CDITS securely transfers passport application biometric data and PII, including names, sex, date and place of birth, mailing addresses, email addresses, telephone numbers, financial information, most recent passport book and card numbers, date and place of any name change, height, hair color, occupation, name of employer, Social Security number, and the name, address, and phone number of emergency contact.

- **DEA** – Lookout, passport and visa related PII is transferred from DEA to CDITS for the purpose of visa application processing. This includes name, date of birth, gender, country of birth, alias name(s), physical description, armed-dangerous indicator, comments (including significant information about the relevant drug case).

- **FBI NCIC** – This sharing consists of “Loss of Nationality” files that transfer personally identifiable information (PII), which include name and SSN and other PII to update State Department information for processing of Passports and Visas. NCIC also sends electronic files containing passport and visa information through CDITS that is transferred to the Diplomatic Security Office via CA systems.

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

CDITS receives information from external organizations and routes that information to the CA State Department systems identified in paragraph 6(a) for use in processing passport and visa application processing. CDITS does not directly process any data.

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

Internally:

Internal information is transferred database to database between the CA/CST systems listed in paragraph 6a. Information is transferred electronically and securely using Transmission Control Protocol/Internet Protocol (TCP/IP) and Transport Layer Security (TLS).

Externally:

The Bank – CDITS pulls data from the Bank. The data is encrypted in transit. CDITS transfers this data to other State Department systems identified in paragraph 6(a) via an FTP server over the secure State Department intranet.

DEA - Information is transferred from DEA to CDITS via File Transfer Protocol (FTP). The communication between CDITS and the DEA is protected using the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 compliant hardware encryption devices.

FBI NCIC - Information is transferred from NCIC to CDITS via File Transfer Protocol (FTP). The communication between CDITS and the FBI is protected using FIPS 140-2 compliant hardware encryption devices.

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

Internal:

Information is shared by secure transmission methods permitted by internal Department of State (DoS) policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to electronic files internally is protected by inherited security controls from the DoS domain infrastructure. All accounts are under the supervision of system managers. Audit trails track and monitor usage and access. Defense in depth is deployed as well as roles assigned based on least privilege. Finally, regularly administered security and privacy training informs authorized users of proper handling procedures.

External:

The Bank - To mitigate the risk of a privacy breach, strict security and access controls are in place to ensure the confidentiality and integrity of the PII. An Interconnection Security Agreement (ISA) is in place that specifies requirements for protection of PII transferred via the interconnection between the Bank servers and CDITS servers. Bank application processing is performed in accordance with a Service Level Agreement (SLA). This transfer is secured by national Institute of Standards Technology (NIST) Federal Processing Standard (FIPS) 140-2 compliant encryption software and hardware.

When the data is received by the CDITS servers, it is decrypted and then scanned using anti-virus software. The data is sent to CA systems addressed in paragraph 6(a) making information available to the passport agencies and centers via the State Department intranet. No information is permanently stored on the CDITS network. The data cannot be accessed by CA personnel while in transit.

DEA/FBI NCIC - Risk of modification and disclosure of the PII is mitigated by the encryption of communications between the DEA and CDITS. Within the State Department intranet, the data is protected by common enterprise security controls.

(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:

1) 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.

2) Deliberate disclosure/theft or information provided to unauthorized parties regardless whether the motivation was monetary, personal or other.

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

1) 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.

2) Strict role based access control, based on approved roles and responsibilities, authorization, need- to-know, and clearance level.

3) Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

For external organizations, there are memoranda of understanding (MOUs) in place and the data is transmitted using FIPS 140-2 encryption.

7. Redress and Notification

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

Not applicable. CDITS does not permanently store any PII therefore no access process is required.

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

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.

CDITS does not collect or store information from individuals. Individuals must follow processes of the source systems used to apply for the specific service to request correction of information.

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

CDITS does not collect information from individuals. CDITS' main function is that of transmitting information from one location to the next. Any procedures to access information provided for a specific purpose would be documented by the system that originally collected the information, not CDITS.

8. Security Controls

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

CDITS 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 official duties.

All CDITS accounts must be approved by the user’s supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

CDITS is configured according to State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (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 and are tracked until compliant or acceptably mitigated.

(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.

Access to CDITS is role based, and restricted according to approved job responsibilities requiring managerial concurrence. Information System Security Officers determine the access level needed by a user to ensure it correlates to the user’s particular job function and level of clearance.

Access to CDITS at the network level is limited to authorized Department of State vetted system administrators who have a justified need to access network level devices, services and protocols for administrative, maintenance and troubleshooting purposes only. Databases in CDITS are limited to authorized users with accounts that allow access resources specifically designated to them. Access is approved at all levels by government supervisors.

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

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information (PII). Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State network and respective applications. From that point on, any changes (authorized or not) that occur to data is recorded. In accordance with Department of State Security Configuration Guides, CDITS auditing is also 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 CDITS audit trail is to document unintended modification or unauthorized access to the system. 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 he/she signed off. This multilayered approach to security controls greatly reduces the risk that PII transmitted by CDITS will be misused.

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

In accordance with Department of State computer security policies, Department of State government employees are required to take the one-time PA459, Protecting Personally Identifiable Information privacy training. All authorized users of DoS systems are required to take the PS800 Cyber Security Awareness training. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. The 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 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.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. All systems must comply with all guidelines published by Systems Integrity Division, in addition to all Security Configuration Guides published by Diplomatic Security. Adherence to these guides is verified during the system's Assessment and Authorization process.

CDITS uses Transmission Control Protocol/Internet Protocol TCP/IP for data transport across the network. Data in transit is encrypted. The TCP/IP suite consists of multiple layers of protocols that help ensure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary.

(f) How were the security measures above influenced by the type of information collected?

Due to the sensitive nature of the data that traverses the CDITS boundary, which includes PII of U.S. citizens and legal permanent residents, numerous security measures were implemented, including effective procedures for access authorization, identification and authentication, account housekeeping, monitoring, recording, and auditing

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

Only Department of State Passport and Visa System Administrators have access to CDITS servers and network devices for the purpose of carrying out their official duties.

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

An individual's job function determines what data can be accessed as approved by the supervisor and the Information Systems Security Officer (ISSO). Although this system primarily transfers data (as opposed to storing it), the information is still accessible by System Administrators while processing through the system. Access to this information is role based and the user is granted only the role(s) required to perform officially assigned duties such as administrative, account management, maintenance and troubleshooting duties. DoS system administrators are given access to data strictly as a part of their day to day job functions.

External users are given access to the CDITS data based on agreed upon MOUs between CA and the partner agency. The partner agency is provided with an account that will allow them to access only the data agreed to in the MOU.

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

Procedures and controls are documented in the System Security Plan. The Plan includes information and procedures regarding access to data in CDITS.

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

Access will be restricted to Department of State Visa and Passport Administrators only. Separation of duties and least privilege is employed and users have access to only the data that their supervisor and ISSO approved to perform official duties.

Both the Visa and Passport Administrators have logon identifications associated with their name that allows for user auditing.

The CDITS Visa and Passport Administrators are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configurations to the database. The CDITS Visa and Passport System Administrators are cleared personnel with the Department of State who are authorized to access CDITS for the purpose of performing daily maintenance, troubleshooting technical issues, installing software and patches, establishing access control lists (ACLs), maintaining user accounts, conducting backups, and other actions needed to keep CDITS operational. They have logon identifications associated with their name for the purpose of auditing.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data? CA CDITS information is protected by multiple layers of security controls including:

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

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

- CA CDITS Visa and Passport System Administrators have access via OpenNet from the Department of State configured workstations. Users must dual factor authenticate utilizing Personal Identification Verification /Common Access Card (PIV/CAC) and Personal Identification Number (PIN) to access data in CA CDITS.

- Least Privileges are restrictive rights/privileges or access of users for the performance of specified tasks.

- System and information integrity auditing are implemented to monitor and record unauthorized access/use of information.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Several steps are taken to reduce risk related to system and information access. Access controls, which define who can access the system, and at what privilege level, are regularly reviewed, and 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.