Consular ***Data Information Transfer System (CDITS)***

1. Contact Information

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

2. System Information

(a) Date PIA was completed: January 19, 2010

(b) Name of system: Consular Data Information Transfer System

(c) System acronym: CDITS

(d) IT Asset Baseline (ITAB) number: 964

(e) System description:

CDITS is a communication infrastructure used to exchange data/information in support of the Bureau of Consular Affairs (CA). CDITS is a General Support System (GSS) composed of several connections that assist with the transfer of visa and passport information via several servers. Out of the several connections used within CDITS there is only connection that is covered by this Privacy Impact Assessment (PIA). It is the connection referred to as the "Citibank Lockbox Connection" ("Lockbox"). Because non-US citizens are not covered by the provisions of the Privacy Act or E-Government Act, none of the connections that handle Visa information are covered in this PIA.

Only this Lockbox connection collects and maintains personally identifiable information (PII). Initially, passport application data is gathered by Citibank, to process the application fee. The Lockbox connection then transfers this application data to the Department of State servers. Finally, the passport application data is transferred via CA OpenNet in a secure manner to the Travel Document Issuance System (TDIS) to be maintained as a final record.

(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): N/A

(h) Date of previous PIA (if applicable): April 23, 2009

3. Characterization of the Information

The system:

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

☒ does contain PII. If this is the case, you must complete the entire template.

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

CDITS temporarily collects elements of PII, but only for the CDITS Lockbox connection. This connection is used strictly as a means of transferring the Lockbox passport data (passport and biometric information from passport applications) to TDIS for further processing. This information comes from the Citibank contractor that gathers the passport data that is securely transferred to the department and further on to TDIS.

b. How is the information collected?

Citibank provides lockbox services for passport application processing. Citibank receives passport applications by mail daily. Passport applications are received in paper format and are accompanied with a form of payment covering the processing fee (when applicable) and supporting documentation.

Information transferred by CDITS is collected directly from passport applicants. The information contained in the passport application is entered into CDITS by Citibank upon processing the passport application fee. No changes to the data are made at the collection.

CDITS collects the information by using a secure and controlled inter-enterprise circuit that requires a redundant path to transfer at 99.999% reliability level to avoid delaying passport issuance and idling of CA staff. Lockbox data is pulled from Citibank servers to CA/CST servers using Connect: Direct Secure+ data transmission software (Sterling Commerce, Inc.) that is installed on each of the CA and Citibank servers. Once CA has pulled lockbox data to CA servers located at SA-26 and HST and decrypted by Secure+ it will be scanned using Norton Anti Virus software and re-distributed by CA to TDIS, which will disburse the data to the Passport Agencies and Centers as appropriate via OpenNet. No information is stored on the CDITS network, nor can it be accessed by CA personnel while en route.

c. Why is the information collected and maintained?

This information is collected and maintained for the purpose of transferring electronic passport applications to CA. This secure and controlled inter-enterprise connectivity requires a redundant path to transfer at 99.999% reliability level to avoid delaying passport issuance and idling of CA staff.

d. How will the information be checked for accuracy?

Information is not checked for accuracy within CDITS, as it is a transfer mechanism from Citibank to the Department of State. Passport application information is reviewed and checked for accuracy during the passport issuance process, utilizing the system TDIS.

CDITS does not contain any end users, therefore, only System administrators have rights to logon to make sure CDITS hardware is functioning correctly and is transferring the Lockbox information collected from Citibank. This information cannot be unencrypted until it arrives at TDIS, so nothing is verified at this stage.

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

- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)

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

CDITS is a necessary interface between Citibank and the Department of State's Travel Document Issuance System during the passport application process. CDITS transfers high levels of sensitive PII to TDIS at regular intervals. To mitigate privacy risk, strict security and access controls are in place to ensure the confidentiality and integrity of the personally identifiable information.

An Interconnection Security Agreement (ISA) helps to protect and cover privacy risks between the interconnection between Citibank's lockbox servers and CA's Consular Data Information Transfer System (CDITS) servers.

Applications processing is performed as per Service Level Agreement. Applications are processed, batched, scanned, reviewed, and have data entry performed on them. Once all processing is completed and financial data has been released to Financial Management Services (FMS), the application data is ready to be retrieved by Department of State and privacy risks follow under an Information Security Agreement between Citibank and the Department of State.

The Citibank to CA data transfer involves CA's monitoring of specific directories at the Citibank site. These directories are automatically configured to receive the passport image and data files. As the passport application and photo images files become available, CA will initiate the file transfer from the Citibank server to one of two CA servers. As Citibank will not have access to any Department servers or networks, CA will be pulling the data from the Citibank servers. This is securely protected by Connect: Direct and Secure +, which follows the FIPS 140-2 security requirement.

4. Uses of the Information

a. Describe all uses of the information.

CDITS is a communication infrastructure used to transfer passport application data and imagery from Citibank to the centralized Travel Document Issuance System (TDIS) for maintenance and further processing.

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

The data is not analyzed. No new information is produced.

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

CDITS does not use any commercial or publicly available information.

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

CDITS is a government owned system. The only users are government personnel. These users are CA Department System administrators who are allowed to monitor the directories that pick up the Citibank information. There are no end-users of CDITS. Contractors are only involved with the design and development of the system. All System administrators are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements.

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.

Appropriate use of the information is regulated by automated security controls in the CDITS system. The CDITS system does not provide a flexibility of features that might initiate a functional vulnerability creep or threat. CDITS is only used as a transfer mechanism from passport intake authorities to TDIS, and does not have any end users. Several security controls are described as such:

IRM/OPS/ENM installs, operates and manages FIPS 140-2 compliant VPN Nortel 2750 encryption devices and PKI on the lockbox transmission paths between Department datacenters (SA-26 and HST) and Citibank datacenters (MD and TX). IRM (IRM/OPS/MSO/EML/NCC) also installs, operates and manages a stateful inspection firewall (StoneSoft) and a proxy/application layer firewall (McAfee) to provide port and application proxy layer access controls.

CA/CST operates and manages Direct: Connect Secure+ software on CA servers. It is used for adding another level of protection for lockbox data before it enters and after it has cleared the network transmission path. CA also installs and operates Norton antivirus on the servers to provide content scanning for virus and malware after data has been decrypted by Secure+ (See Section 3.0.). Connect direct is accessed by going to Programs, Sterling Commerce Connect Direct v4.4.00, and to CD Secure +CLI. It is FIPS 140-2 compliant and can be verified at the following internet link:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

5. Retention

a. How long is information retained?

No information is retained.

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

Both Citibank and Department of State are responsible for auditing application processes and user activities involving this interconnection and transfer of the Citibank files. The data that is sent onto TDIS via CDITS is almost instantaneous and does not pose a great risk for the duration of the transfer.

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?

TDIS interfaces with CDITS via Front End Processor (FEP). The TDIS request is filtered through to CDITS via FEP and the response from CDITS to TDIS is sent back via FEP for the purpose of preventing internal CA major application systems from initiating a direct and formal communication with external systems not on OpenNet.

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

Information within CDITS is transferred via FTP server from CITIBANK to TDIS and to other passport agencies. Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to electronic files is protected by passwords, and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

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

Access to information is controlled by application access controls. Management Control Reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal DoS regulations.

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?

Citibank provides lockbox services for passport application processing. Citibank receives passport applications by mail daily. Passport applications are received in paper format and are accompanied with a form of payment covering the processing fee (when applicable) and supporting documentation.

An Interconnection Security Agreement (ISA) helps to protect and cover privacy risks between the interconnection between Citibank's lockbox servers and CA's Consular Data Information Transfer System (CDITS) servers.

CDITS allows Citigroup (Citibank) to transmit passport data that is captured in the lockbox process, sent over OpenNet, and transferred to TDIS for sending to the passport agencies and centers over a secure point-to-point encrypted circuit.

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

CDITS passport data is shared by Citibank. Citibank Administrators prepare the photo and biometric data for CA server pick-up. There is a Memorandum of Understanding in place with an Information Security Agreement (ISA) that provides the guidelines for sharing of the information. CA administrators monitor the specific directories at the Citibank site that contain the passport image and data files. As the passport application and photo image files become available, CA will initiate the file transfer from the Citibank server to one of two CA servers. This information is pulled into the CA OpenNet servers and securely passed on to the Department of State servers which pick up the data and deliver it to TDIS.

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

CDITS only receives the data from Citibank and once the data is accepted it is completely processed over OpenNet at the TDIS level, therefore mitigating any privacy risk.

8. Notice

The system:

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

□ 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?

Notice is provided at the point of collection during the application process. Passport applications that collect PII directly are covered by Passport Records, STATE-26.

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

No, once information is collected by the passport issuance agencies, an individual cannot decline to provide information. CDITS is part of the “Passport Records” system of records, even though applicant data cannot be uniquely retrieved within CDITS.

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?

No, once information is collected by the passport agency, an individual does not have the right to consent to limited, special, and/or specific uses of information.

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.

Notice provided is adequate and reasonable, and is provided at the collection points of information (i.e. the passport application forms).

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?

Department notification procedures dictate that individuals who have reason to believe that the Bureau of Consular Affairs may have security/investigative records pertaining to them should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA-2, Department of State, Washington, DC 20522–6001. The individual must specify that he/she wishes the Passport Records (STATE-26) System of Records Notice to be checked. At a minimum, the individual must include: Name; date and place of birth; current mailing address and zip code; signature; and a brief description of the circumstances, which may have caused the creation of the record.

Record Access and Amendment Procedures: Individuals who wish to gain access to or amend records pertaining to them should write to the Director; Office of Information Programs and Services (address above).

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

There is no risk associated with Notification and Redress as it is a part of the SORN (Passport Records Number STATE-26).

10. Controls on Access

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

Only Department of State administrators are responsible for auditing application processes and user activities involving the CDITS servers and network devices. Activities that will be recorded include: event type, date and time of event, user identification, server identification, success or failure of access attempts, and security actions taken by system administrators or security officers.

IRM supports 24x7 Network Operations Centers that are responsible for monitoring, trouble management and escalation processes for firewalls and all the Lockbox connection network transmission path equipment. Tracking events identified are not captured entirely by a single protection device but by a combination of all of the devices in the transmission path and, most importantly, are considered DHS Trusted Internet Connection (TIC) compliant architecture. IRM policy requires that audit logs are retained for 6 months.

IRM provides 24x7 monitoring of firewall, scanning, and encryption equipment in the network transmission path on centrally managed and automated servers. Monitoring of events outside the network boundaries on CA Lockbox servers, including the use and management of Secure+ and Norton antivirus content level scanning, is the responsibility of CA. To meet this requirements, Lockbox servers are configured to comply with the all applicable Diplomatic Security configuration guide policies on auditing and in accordance with 12 FAM 652.3-4 Audit.

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

All CA administrators must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain access.

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 controls are employed to ensure that CA personnel use CDITS only in an authorized manner. The trainings and controls described above are adequate in their protection of CDITS information from unauthorized access and use.

11. Technologies

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

CDITS uses secure networks and Connect:Direct servers to transfer information. These technologies do not elevate privacy risk.

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

Since CDITS does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum satisfactory in this general support system (GSS).

12. Security

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

The system is currently going through a Certification and Accreditation process.