Consular Consolidated Database (CCD) Privacy Impact Assessment (PIA)

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:** March 22, 2010

b. **Name of system:** Consular Consolidated Database

c. **System acronym:** CCD

d. **IT Asset Baseline (ITAB) number:** 9

e. **System description (scope, purpose, and major functions):**

The Consular Consolidated Database (CCD) is one of the largest Oracle based data warehouses in the world that holds current and archived data from the Consular Affairs (CA) domestic and post databases around the world. As of December 2009, it contains over 100 million visa cases and 75 million photographs, utilizing billions of rows of data, and has a current growth rate of approximately 35 thousand visa cases every day. It was created to provide CA a near real-time aggregate of the consular transaction activity collected domestically and at post databases worldwide. The CCD is the IT implementation that provides for a set of centralized visa and American citizen services supporting consular posts and back office functions.

Three chief functions, among the many performed by CCD, are to support data delivery to approved applications via industry-standard Web Service queries, provide users with easy-to-use data entry interfaces to CCD, and allow emergency recovery of post databases. Authenticated Department of State and other authorized government agency users utilize the CCD Portal to view the centralized data through a rich set of reports as well as to gain access to other applications. The CCD serves as a gateway to IDENT and IAFIS fingerprint checking databases, the Department of State Facial Recognition system, and the NameCheck system.

During the course of consular processing activities at posts, applications generate requests for information to CCD, which are handled as queries and routed by the CCD system to the appropriate internal or external data source. When CCD receives a reply from the data source, it generates a response to the requesting post application.

Data in the CCD is presented to users (specific communities of interest) via parameter driven reports. To enable timely browsing and reporting on that data, data marts have been created to organize the data. The data marts within CCD have been designed to improve the performance of searches against the vast data held in the CCD system. When users run reports on the CCD Portal using their Internet Explorer browser, they are accessing the CCD data through a Web Server to the appropriate data mart. In the event additional information is needed to satisfy the report requirements, the data will then be accessed from the aggregate database (SAN Storage Unit).

The CCD has become an invaluable tool for users in providing a one stop access point to data and in preventing and tracking fraud.

f. **Reason for performing PIA:**

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

☐ PIA Information Review

g. **Explanation of modification (if applicable):** N/A

h. **Date of previous PIA (if applicable):** December 2008

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?

The following PII elements are collected and maintained by CCD:

The CCD stores information about US persons (US citizens and lawful permanent residents), as well as foreign nationals (non-US persons) such as Immigrant Visa applicants and Non-Immigrant Visa applicants. This information includes, but is not limited to, names, addresses, birthdates, biometric data (fingerprints and facial images), race, identification numbers (e.g. social security numbers & alien registration numbers) and country of origin.

The main sources of the information are:

The CCD database, located in the Washington, D.C., area, holds current and archived data from Consular Affairs domestic and post databases around the world. The CCD provides access to passport data in Travel Document Issuance System (TDIS), Passport Lookout Tracking System (PLOTS), and Passport Information Electronic Records System (PIERS).

With respect to data collected and stored in CCD that is provided by foreign national visa applicants, such information is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

Because visa applicants themselves are not U.S. persons (that is, U.S. citizens or lawful permanent residents), they are not covered by the provisions of the Privacy Act or E-Government Act. Therefore the remainder of this PIA addresses the PII collected and maintained by the CCD on U.S. persons only.

b. How is the information collected?

All data is voluntarily provided by the applicants for Visas, Passports, and American Citizen Services. The data is stored on the respective systems that collect it. Through the CCD replication process, a copy of the data from the Consular systems domestically, at posts, and from external government agencies is stored in the CCD databases. The data, collected from domestic and post applications, is replicated from the systems' databases to the CCD database.

c. Why is the information collected and maintained?

The information that is collected serves as a backup for each system's transaction activity and allows CA management the ability to apply advanced metrics against the data – identifying peak load periods at consular facilities, utilization rates for post consumables, trend analysis, manpower analysis, re-supply management, and personnel rotation scheduling. In addition, the aggregated data may be filtered by transaction type for specific areas of interest and "pushed" out to other databases within the CCD system that are streamlined and optimized to support reporting against a large collection of data. These "data marts" have been designed to improve the performance of searches against the data stored in the CCD system.

d. How will the information be checked for accuracy?

Accuracy is the responsibility of the government agency that collected the data originally.

A Data Engineering team monitors the databases to insure exact duplicate replications and consistent accuracy. Identical software is installed on all databases and configuration management controls are in place. To verify accuracy, all data updates are compared against existing data prior to being applied and any discrepancies are reported and investigated.

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

- 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).
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705
- Executive Order 11295 (August 5, 1966)
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1185 (Travel Control of Citizens)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State);

- 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);
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries);
- 22 U.S.C. 2705 (Preparation of Consular Reports of Birth Abroad);
- 8 U.S.C. 1501 (Adjudication of possible loss of nationality);
- 22 U.S.C. 2671(b)(2)(B)(Repatriation loan for destitute U.S. Citizens abroad);
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance);
- 22 U.S.C. 2151n–1 (Assistance to arrested citizens) (Repealed, but applicable to past records);
- 42 U.S.C. 1973ff–1973ff–6 (Overseas absentee voting);
- 42 U.S.C. 402 (Social Security benefits payments);
- Sec. 599C of Public Law 101–513, 104 Stat. 1979, as amended (Claims to benefits by virtue of hostage status);
- 50 U.S.C. App. 453, 454, Presidential Proclamation No. 4771, July 2, 1980 as amended by Presidential Proclamation 7275, February 22, 2000 (Selective Service registration);
- 22 U.S.C. 5501–5513 (Aviation disaster and security assistance abroad; mandatory availability of airline passengers manifest);
- 22 U.S.C. 4196; (22 U.S.C. 4195, repealed, but applicable to past records) (Official notification of death of U.S. citizens in foreign countries; transmission of inventory of effects);
- 22 U.S.C. 2715b (notification of next of kin of death of U.S. citizens in foreign countries);
- 22 U.S.C. 4197 (Assistance with disposition of estates of U.S. citizens upon death in a foreign country);
- 22 U.S.C. 4193, 4194; 22 U.S.C. 4205–4207; 46 U.S.C. 10318 (Merchant seamen protection and relief);
- 22 U.S.C. 4193 (Receiving protests or declarations of U.S. citizen passengers, merchants in foreign ports);
- 46 U.S.C. 10701–10705 (Responsibility for deceased seamen and their effects);
- 22 U.S.C. 2715a (Responsibility to inform victims and their families regarding crimes against U.S. citizens abroad);
- 22 U.S.C. 4215, 4221 (Administration of oaths, affidavits, and other notarial acts);
- 28 U.S.C. 1740, 1741 (Authentication of documents);
- 28 U.S.C. 1781–1783 (Judicial Assistance to U.S. and foreign courts and litigants);
- 42 U.S.C. 14901–14954; Intercountry Adoption Act of 2000, (Assistance with Intercountry adoptions under the Hague Intercountry Adoption Convention, maintenance of related records);
- 42 U.S.C. 11601–11610, International Child Abduction Remedies Act (Assistance to applicants in the location and return of children wrongfully removed or retained or for securing effective exercise of rights of access);
- 22 U.S.C. 4802 (overseas evacuations).

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

Due to the strict security controls required by all Department of State systems before system operation commences, privacy risks are limited as follows. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft:

- **Device theft or loss** Lost or stolen laptops and other devices such as removable drives may contain SBU information.

- **Portable Devices** PII is at the fingertips of every staff member who has email, database and Web access at work. The growing use of removable media such as USB drives, CDs/DVDs and portable Mp3 players brings new risk into the picture by making PII easily transportable on devices that aren't always properly secured.

- **Insider threat** Disgruntled employees seeking revenge or inadvertent human error to send SBU information over the internet.

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

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

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports. In addition, these controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application. Only authorized users with a need to know are granted access to CCD.

4. Uses of the Information

a. Describe all uses of the information.

The information contained in CCD is used for the following purposes:

- Automated screening of applicants
- Automated checking of applicant fingerprints
- Registration of applicant facial images for Facial Recognition
- Reports with data on a particular applicant or post, or data from multiple applicants or posts
- Reports with reference information for authorized users, such as post codes and post directory information
- Reports for supervisors and administrators to track work or review applicant data
- External information sharing with other authorized government agencies to enable them to receive information on post applicants and provide timely responses
- Reports with the status of post databases and post upgrades
- Access by outside federal agencies

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

The following methods are used to analyze the data:

Since there is a vast amount of data contained in the CCD, the CCD data is not accessed directly. To enable timely browsing and reporting on that data, data marts have been created to organize the data.

A data mart is a database that is created and optimized to support reporting against the data collected in an operational database such as the CCD. The data marts are designed to improve the performance of searches against the vast holdings of data in the CCD. Reports run on the Consular Affairs Portal Service access the CCD data through a data mart.

The following new information is produced:

From the CCD data, statistical reports are generated and analyzed to create metrics based on country, type of request, biographic and biometric checks.

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

Some U.S. Citizen information stored in the CCD, such as names, addresses, birth dates, race, identification numbers (e.g. social security numbers) and country of origin, is obtained through commercial databases and public records. This data is used by analysts to support national security, U.S. border security, official government business or federal law enforcement.

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

The CCD is a government owned system. Government personnel are primary users of CCD. Contractors are involved with the design and development of the system.

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 categorization of information and help define distribution restrictions for some reports.

All users, including external Agency users, are screened prior to their employment with the Department or their respective Agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police and credit records, and a fingerprint check, and may include a personal interview if warranted. In addition, before given access to the OpenNet and any CA/CST system, including CCD, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

It is mandatory for all Department of State employees and contractors to pass 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.

Each domestic organization has at least one Certifying Authority who is responsible for managing the users within the organization. Certifying Authorities are government employees who use the CCD to approve account requests and assign CCD roles appropriate for each user’s job requirement. CCD roles determine what a user can do on the CCD. Domestic users can view data for all the posts.

The Certifying Authority determines the access level needed by a user (including managers) to ensure it correlates to the user’s particular job function and level of clearance. Contractors who support CCD are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors involved in the development and/or maintenance of CCD hardware and software must have a level “Secret” security clearance. Once the highest-level background investigation required has been completed, cleared technical personnel (government and contractors) will be allowed to access the server rooms housing the CCD.

The CA post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that is SBU. In addition, all CCD visa record reports are subject to INA 222(f) confidentiality requirements, and are marked with the following header that describes the output handling and retention requirements to the user:

Sensitive But Unclassified (SBU)* - *Information Protected under INA 222(f) and 9 FAM 40.4: This information "shall be considered confidential" per Section 222(f) of the Immigration and Nationality Act (INA) [8 U.S.C. Section 1202]. Access to and use of such information must be solely for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States under INA 222(f) and 9 FAM 40.4.

5. Retention

a. How long is information retained?

Record retention depends upon the kind of record involved. The complete disposition schedule for passport records is specified in the U.S. Department of State Records Disposition Schedule, approved by the National Archives and Records Administration.

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

To prevent the loss of the data retained in CCD, regular backups are performed and recovery procedures are in place. All physical records containing personally identifiable information are maintained in secured file cabinets or in restricted areas, with limited access to authorized personnel only. Access to electronic information is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately handled in accordance with appropriate National Archive and Records Administration (NARA) rules.

6. Internal Sharing and Disclosure

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

The following internal Department of State system(s) are connected electronically to CCD. They fall under the purview of the Department's Designated Approval Authority. CA does not require Memorandums of Understanding (MOU), Memorandums of Agreement (MOA), or Service Level Agreement (SLA) for CA owned systems connected to CCD via OpenNet. Controls built in the OpenNet GSS, including Firewalls and NIDS, provide network level controls that limit the risk of unauthorized access.

#	System Name, Acronym, and ITAB number	Type of connection	Type of data and how it is shared
1.	Adoption Tracking Service (ATS) ITAB#: 720	Bi-directional	Visa data replicated from posts to the CCD. ATS has an interface with the CCD Web Services (CCDWS) web server. The CCDWS accepts a series of predefined requests from ATS and returns the results from the CCD repository of IVO and IVIS data.
2.	American Citizen Services (ACS) ITAB#: 818	Bi-directional	Post ACS databases provide inventory of all open services and previous services. All subjects, cases, and services are replicated from each Post through the ACS data replication

#	System Name, Acronym, and ITAB number	Type of connection	Type of data and how it is shared
			server to the CCD. The ACS domestic application server interfaces with the CCD to retrieve ACS data in the form of reports and sends this data to the requesting ACS workstations at Posts.
3.	Automated Biometric Identification System (ABIS) a.k.a FR System ITAB#: 877	Bi-directional	Fraud Watchlist data / Photo Identification data Users at post submit one of the following requests: add, delete or search for a Visa applicant photo to CCD. CCD queues the request on the CCD stage database server. The request is then pushed to the ABIS stage application server (SAS) using a service account where it is processed. After processing, the results/request are queued and pushed back to the CCD stage database server. The CCD returns the results to post.
4.	Automated Cash Register System (ACRS) ITAB#: 554	One way	Consular Fee Transaction data Data from ACRS database tables is replicated via an encrypted SSL network connection to the CA CCD.
5.	**Consular Electronic Application Center Portal** **(CEAC)** **ITAB#: 2712**	**Bi-directional**	**Visa data.** **CEAC data is pulled into the CCD database cluster at HST with backup in BIMC. The CEACP web component on the OpenNet accesses data from CCD database clusters via Web Services for reporting purposes.**
	CEAC Case Tracking (CTRAC) ITAB#: 4551	Bi-directional	Tracking of immigrant visa fee invoice and payment information
	CEAC Payment Processing Service (PPS) ITAB#: 4556	Bi-directional	Visa payment data
	Remote Data Collection (RDC) ITAB#: 4555	Bi-directional	NIV biometric and image data
6.	Consular Lookout and Support System (CLASS) ITAB#: 558	Bi-directional	Visa data. CCD populates Namecheck Issuance database with Visa CCD data. When a query is submitted to the CCD, the CLASS web service drops the file to the CLASS name check, waits for the response, then returns the response back to the CCD.
7.	Consular Shared Tables	Bi-directional	System Login IDs and Reference Table

#	System Name, Acronym, and ITAB number	Type of connection	Type of data and how it is shared
	(CST) ITAB#: 559		Repository Data CST uses CCD user and role information stored in the CST tables on the CCD to verify role assignment.
8.	Datashare ITAB#: 901	Bi-directional	Visa and Passport data
9.	Diversity Immigrant Visa Information System (DVIS) ITAB#: 17	One way	Diversity Visa data DVIS production data is replication to CCD.
10.	Consular Data Information Transfer System (CDITS) ITAB#: 964	One way	Images and data from passport applications are sent in bundles from CDITS to the CCD
11.	Immigrant Visa Allocation Management System (IVAMS) ITAB#: 97	One way	Visa Allocation Data. IVAMS production data is replicated to CCD.
12.	Immigrant Visa Allocation Management System Web (IVAMS WEB) ITAB#: 753	One way	User ID and Password Identification and Authentication (I&A) to IVAMS WEB is provided by the CCD. The user must first login to the CCD portal for authentication of user ID and password. Next the user selects the IVAMS WEB from the CCD menu to get routed to the web page.
13.	Immigrant Visa Information System (IVIS) ITAB#: 49	Bi-directional	Immigrant Visa data IVIS' connection with CCD is for the purpose of database replication via a one way database link.
14.	International Parental Child Abduction (IPCA) ITAB#: 39	Bi-directional	Information related to international abduction and potential abduction cases Export data from IPCA is replicated to the CCD. This data is used to generate reports for use by the Office of Children’s Issues.
15.	Internet-Based Registration Service/Consular Task Force (IBRS)/(CTF) ITAB#: 27	Bi-directional	IBRS: Travel registration data of US Citizens. Consular Users access the IBRS consular staff web pages, and reports are under the ACS tab of the CCD. CTF: When a crisis occurs overseas, the Department of State calls up a series of task forces, including one to manage the incoming inquiries from the public regarding American citizens that are potentially involved in a crisis.

#	System Name, Acronym, and ITAB number	Type of connection	Type of data and how it is shared
			This data is captured in the Consular Task Force (CTF) application on the Consular Consolidated Database (CCD) that allows task force workers to collect data about potential subjects, related subjects, and contacts, and share that information with other groups and posts overseas for case work.
16.	**Overseas Consular Section Support Applications (OCSSA)** **ITAB#: 4656**		
	Immigrant Visa Overseas (IVO) ITAB#: 817	Bi-directional	Immigrant Visa data, Petition data, Visa Allocation data A copy of IVO data from all posts is replicated to the CCD. IVO provides a link to CCD applicant reports and sends requests for CCD search.
	Non-Immigrant Visa (NIV) ITAB#: 65	Bi-directional	Non-Immigrant Visa data, Visa refusal data A copy of NIV data from all posts is replicated to the CCD. NIV provides a link to CCD applicant reports and sends requests for CCD search.
	Ten Print Live Scan (TPLS) ITAB#: 829	One way	Biographical data is entered into the TPLS application. The fingerprint image and biographical data are stored locally in the Post's database. The Post database replicates this data to the CCD.
17.	Online Passport Lost & Stolen System (OPLSS) ITAB#: 2751	Bi-directional	U.S. Citizens lost or stolen passport data
18.	Online Passport Renewal Service (OPRS) ITAB#: 2736	Bi-directional	The U.S. Passport and Passport Card Renewal application (DS-82) data
19.	Online Passport Status Service (OPSS) ITAB#: 898	Bi-directional	The U.S. Passport and status inquires
20.	Passport Information Electronic Records System (PIERS) ITAB#: 85	One way	Passport records CCD provides access to PIERS for users not on OpenNet.
21.	Passport Lookout Tracking System (PLOTS)	One way	Passport issuance data

#	System Name, Acronym, and ITAB number	Type of connection	Type of data and how it is shared
	ITAB#: 346		
22.	Petition Information Management System (PIMS) ITAB#: TBD	Bi-directional	Visa petition data
23.	Travel Document Issuance System (TDIS) ITAB#: 89	One way	Passport data CCD forwards passport application data to TDIS. Passport agencies and centers retrieve the data files in TDIS for processing
24.	Visa Opinion Information System (VOIS) ITAB#: 875	Bi-directional	Visa data used in support of SAO/AO VOIS is a front-end application to the CCD; VOIS can only be accessed by way of the CCD. CCD handles the primary logon. VOIS uses CCD reporting capability. No data is stored directly in VOIS; it is strictly an interface to CCD data.
25.	Waiver Request System (WRS) ITAB#: 415	Bi-directional	Visa applicant data WRS uses CCD for its data stores. WRS also uses subsets of the NIV and IVO data tables within the CCD to cross check applicant names and visa application numbers.

Table 1: Connection

The following are Department of State interconnected system(s) to CCD.

External Agency/Entity & System	Information Flow Description	Trigger	Frequency	Data Transfer / Communications Mechanism	Security (Authentication Mechanism)
Department of State Office of Logistics Management (A/LM)	Inbound: ILMS	Push	Nightly	Web Service	CCD Authentication
Department of State Bureau of Nonproliferation (NP) Formerly INR	Inbound: Clearance response	Push	Every 5 minutes	CCD Forms	CCD Authentication
Department of State Bureau of Nonproliferation (NP) Formerly INR	Outbound: Security Advisory Opinion (SAO) request for namecheck	Pull	Every 5 minutes	CCD Forms	CCD Authentication

Table 2: Department of State Interconnections

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

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. An Interface Control Document (ICD) defines and discloses transmission format via OpenNet. The Department of State systems that interface with the CCD are strictly controlled by Firewall and NIDS rules sets that limit ingress and egress to the CCD. All changes are requested from the Firewall Advisor Board (FAB) using a Universal Trouble Ticket (UTT). Each UTT is vetted by technical personnel and management prior to the change being implemented.

For more details on how information is transmitted, see question 6a Table 1 & 2 above.

The following safeguards are in place for each sharing arrangement:

All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. 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.

To reduce the privacy risks, access to information is controlled by application access controls. Every server on CA OpenNet has NetIQ Security Manager installed and it is used to monitor server activity. 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 Department of State 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?

The table below lists all the external organizations which CCD shares information with, the type of information being shared, the medium used to share the information, and the security mechanism used to control the shared information.

The purpose for sharing information between agencies is to ensure accuracy and efficiency while conducting federal business.

External Agency/Entity & System	Information Flow Description	Data Transfer / Communications Mechanism	Security (Authentication Mechanism)
Department of Homeland Security (DHS) USVISIT	Inbound: Encounters with matching fingerprints Avg. response size – 80,000 bytes	Partial T3 – SA1	Oracle DB Authentication USER ID/Password (use for DBMS jobs)
Department of Homeland Security (DHS) USVISIT	Outbound: Notification of visa issuances Avg. size 25,000 bytes-	Partial T3 – SA1	DB Authentication USER ID/Password (use for DBMS jobs)
Department of Homeland Security (DHS) USVISIT	Outbound: Request for fingerprint encounters Avg. request size – 360,000 bytes	Partial T3 – SA1	DB Authentication USER ID/Password (use for DBMS jobs)
Department of Homeland Security/ Customs and Border Protection (DHS/CBP)	Outbound: Lost and stolen visas Avg size 300 bytes	Intelink-U	DB Authentication USER ID/Password (use for DBMS jobs)
Department of Homeland Security/ Customs and Border Protection (DHS/CBP)	Outbound: visa applicant refusals Avg size 23,000 bytes	Intelink-U	DB Authentication USER ID/Password (use for DBMS jobs)
Department of Defense Intelligence and Security Command (DOD INSCOM)	Outbound: Security Advisory Opinion (SAO) data	Intelink-U	DB Authentication USER ID/Password (use for DBMS jobs)
Federal Bureau of Investigation (FBI)	Outbound: IVO application	Intelink-U	DB Authentication USER ID/Password (use for DBMS jobs)
Federal Bureau of Investigation (FBI)	Outbound: NIV application	Intelink-U	DB Authentication USER ID/Password (use for DBMS jobs)
Federal Bureau of Investigation (FBI) Analysts	Outbound: Security Advisory Opinion (SAO) data and visa applicant data	Intelink-U	DB Authentication USER ID/Password (use for DBMS jobs)
Federal Bureau of	Inbound: Clearance	Partial T3 – SA1	DB Authentication

External Agency/Entity & System	Information Flow Description	Data Transfer / Communications Mechanism	Security (Authentication Mechanism)
Investigation Integrated Automated Fingerprint Identification System (FBI IAFIS)	response		USER ID/Password (use for DBMS jobs)
Federal Bureau of Investigation Integrated Automated Fingerprint Identification System (FBI IAFIS)	Outbound: Clearance request	Partial T3 – SA1	DB Authentication USER ID/Password (use for DBMS jobs)
Federal Bureau of Investigation (FBI) Namecheck	Inbound: Clearance response	Intelink-U	CCD Authentication
Federal Bureau of Investigation (FBI) Namecheck	Outbound: Security Advisory Opinion (SAO) request for namecheck	Intelink-U	CCD Authentication
Federal Bureau of Investigation Special Technologies and Applications Office (FBI STAO)	Outbound: IVO application	Intelink-U – Web services	CCD Authentication
Federal Bureau of Investigation Special Technologies and Applications Office (FBI STAO)	Outbound: NIV application	Intelink-U – Web services	CCD Authentication
Government Printing Office (GPO)	Inbound: BCC Manifest Ingest	NT Copy (write to a Microsoft NT format file)	DB Authentication USER ID/Password (use for DBMS jobs)
DHS Interagency Border Inspection System\Treasury Enforcement Control System (IBIS/TECS)	Outbound: Notification of IVO and NIV visa issuances Avg. size 25,000 bytes	T1 – SA1	DB Authentication USER ID/Password (use for DBMS jobs)
DHS Interagency Border Inspection System\Treasury Enforcement Control System (IBIS/TECS)	Outbound: Passport data Avg. size 25,000 bytes	T1 – SA26	DB Authentication USER ID/Password (use for DBMS jobs)
Office of Foreign Missions (OFM)	Outbound: A & G visa issuances	OpenNet	DB Authentication USER ID/Password (use for DBMS jobs)
Other Partnering	Outbound: Notification of NIV applicant status	Intelink-U	DB Authentication USER ID/Password (use for DBMS jobs)
Other Partnering Analysts	Outbound: Security Advisory Opinion (SAO) data	Intelink-U	DB Authentication USER ID/Password

External Agency/Entity & System	Information Flow Description	Data Transfer / Communications Mechanism	Security (Authentication Mechanism)
			(use for DBMS jobs)
DHS Student and Exchange Visitor Information System (SEVIS)	Inbound: Notification of SEVIS status for Student and Exchange Visitor visa applicants	T1 – SA1	DB Authentication USER ID/Password
DHS Terrorist Screening Center (TSC)	Inbound: Clearance response	CCD Forms	CCD Authentication
DHS Terrorist Screening Center (TSC)	Inbound: TWPDES watchlist images	NT Copy (write to a Microsoft NT format file)	DB Authentication USER ID/Password
DHS Terrorist Screening Center (TSC)	Outbound: Security Advisory Opinion (SAO) request for namecheck	CCD Forms	CCD Authentication
DHS U.S. Citizenship and Immigration Service (USCIS)	Inbound: Hague adoption case data from SIMS	Web service	CCD Authentication

Table 3: External Interconnections

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

The following paragraph describes at a high level how CCD information is shared outside the Department:

External agencies or entities that share information with CCD connect through either the ENM managed secure T1 line and T3 line or the Intelink connection via the Department's extranet. All external interconnections are routed through the ENM managed extranet F5 Local Traffic Manager (LTM). There are two extranet F5 LTMs, one active and one standby. Even though these extranet F5 LTMs fall within CCD's system boundary they are treated like all ENM managed network-traversing devices. All changes are requested from the FAB using a UTT.

The following safeguards in place for each sharing arrangement:

All external agencies that share information with the CCD are required to sign an MOU or MOA, which generally define a set of responsibilities and requirements. Items generally covered in an MOU or MOA include but are not limited to: Trusted Behavior Expectations, User Community, Access Controls, Audit Trail Responsibility, Data Ownership, Security Parameters, Incident Handling and Reporting, AntiVirus and Security Training and Awareness.

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

The CCD information associated with visa records is shared with U.S. government agencies with a statutory requirement and in accordance with confidentiality requirements under INA section 222(f).

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

8. Notice

The system:

☐ Contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems)

☒ Does NOT contain information covered by the Privacy Act.

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

N/A, the CCD is a data warehouse to store and process data collected by other (internal and external) systems, hence, CCD is not required to provide notice of the purpose, use, and authority for collection of information.

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

N/A, personal information regarding individuals is **not** collected directly by CCD; it is received from external agencies and Department of State overseas and domestic posts.

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?

N/A, information is **not** collected directly from individuals.

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.

N/A, information is **not** collected directly from individuals.

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?

N/A, personal information regarding individuals is **not** collected directly by CCD; it is received from external agencies and Department of State overseas and domestic posts, hence, it is the responsibility of the system that replicates to CCD to provide the notice of information.

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

To the extent information collected by the Department of State overseas and domestic post may be Privacy Act-covered, the notification and redress mechanisms offered to individuals by the respective systems which collected the data are reasonable and adequate in relation to the system’s stated purposes and uses and its applicable legal requirements.

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?

Internal access to CCD is limited to authorized Department of State users that have a justified need for the information in order to perform official duties. In addition, these users must be authorized to use the Department of State’ unclassified network (OpenNet). Each authorized user must sign a user access agreement before being given an OpenNet user account. The user access agreement includes rules of behavior describing the individual’s responsibility to safeguard information and describes prohibited activities (e.g. curiosity browsing). The authorized user’s supervisor must sign the agreement certifying that access is needed to perform official duties. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning an OpenNet logon. A system use notification (“warning banner”) is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Access to CCD requires a unique user account and password. Each domestic organization appoints a Certifying Authority who is responsible for reviewing each CCD user account request and creating the CCD user account. The Certifying Authority is also responsible for periodically reviewing the user access list and disabling any user account that no longer requires access.

The CCD access for post users is controlled by CST roles granted and managed by CST administrators. Each post has a CST administrator responsible for accepting, reviewing, and creating the individual user accounts.

Once a user is properly identified and authenticated by the CCD, they are authorized to perform all functions commensurate with their CCD assigned role. The CCD employs logical access controls in accordance with the principle of least privilege and the concept of separation of duties.

Access control lists, 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 that authorized users perform--or may attempt to perform.)

Mandatory annual security/privacy training is required for all authorized users including security training and regular refresher training.

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

All users 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.

The expected residual risk related to access for CCD is due to the number of agencies that require access to CCD. A decentralized access management process was created which allow each agency to grant authority to manage their own accounts. This creates the risk that no one person at one time has knowledge of the full access list for CCD. In addition, the current authentication mechanism (user name, password, location code) used by CCD does not meet the eAuthentication Security requirement to use multiple factors authentication.

11. Technologies

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

The two main technologies used by CCD are Oracle 10g for the database servers and SSLv3 for the web servers and the LTM devices. In addition, bulk encryptors inherent within OpenNet encrypt the data from posts to the CCD database are also used. They are all Government off-the-shelf (GOTS) products and have met required security capabilities related to their design and development processes, undergone required testing and rigorous internal evaluation procedures and documentation. All known vulnerabilities identified by the industry related to these technologies have been mitigated. All new vulnerabilities identified in the future will be patch and fix during the regular monitor process.

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

Since the OpenNet is a dedicated closed network for the Department of State and the technologies used by CCD do not have any known elements that elevate privacy risk, the current CCD safeguards in place, which are described below, are satisfactory.

The Department of State operates CCD in accordance with information security requirements and procedures required by federal law and internal policy to ensure that information is appropriately safeguarded and protected. The Department of State 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.

12. Security

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

In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of CCD, its most recent date of Authorization To Operate (ATO) was February 28, 2007 for 36 months. The CCD just completed recertification and reaccreditation, and received its new ATO for another 36 months; it will expire in March 31, 2013.