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: December 11, 2008

(b) Name of system: Consular Consolidated Database

(c) System acronym: CCD

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

(e) System description (Briefly describe scope, purpose, and major functions):

The Consular Consolidated Database (CCD) is a set of databases located in Washington, D.C. that hold and provide access to all current and archived data from all of the Consular Affairs post databases around the world. This includes the data from the Automated Biometric Identification System (ABIS), ARCS, Automated Cash Register System (ACS), Consular Lookout and Support System (CLASS), Consular Shared Tables (CST), DataShare, Diversity Visa Information System (DVIS), Immigrant Visa Information System (IVIS), Immigrant Visa Overseas (IVO), Non-Immigrant Visa (NIV), Visa Opinion Information Service (VOIS), and Waiver Review System (WRS) applications. The CCD also provides access to passport data in the Travel Document Information System (TDIS), Passport Lookout and Tracking System (PLOTS), and Passport Information Electronic Records System (PIERS). In addition to Consular Affairs data, other data from external agencies is integrated into the CCD, such as the "Master Death Database" from the Social Security Administration.

The CCD is used for many purposes and supports data delivery to approved applications via industry-standard Web Service queries, provides users with easy-to-use data entry interfaces, and allows emergency recovery of post databases. Authenticated Department of State and other authorized government agency users utilize the CCD to view the centralized data through a rich set of reports as well as to gain access to other applications. Finally, the CCD serves as a gateway to IDENT and IAFIS fingerprint checking databases as well as to the DoS Facial Recognition and NameCheck systems. The CCD has become an invaluable tool for over 20,000 users in providing a one stop access to data and in fraud prevention and tracking.

(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): April 2007

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 CCD stores information about U.S. citizens, and non-U.S. citizens such as Immigrant Visa applicants and Non-Immigrant Visa applicants; which includes, but is not limited to, names, addresses, birthdates, race, identification numbers (e.g. social security numbers & alien registration numbers) and country of origin.

However, as PII collected from non-U.S. citizens is not covered by the provisions of the Privacy Act and E-Government Act, the remainder of this PIA addresses the PII collected and maintained by CCD on U.S. persons only.

b. How is the information collected?

CCD receives data from Consular systems domestically, at posts, and from external government agencies such as the Social Security Administration.

c. Why is the information collected and maintained?

The data collected from post applications is replicated from the post database to the CCD database. Assuming there is new data to transmit, this replication occurs repeatedly on a regular schedule. As this data is aggregated in CCD, it serves as a backup for each post'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. Any errors detected by the CCD are called to the attention of the collecting-agency.

A Data Engineering team monitors the databases to insure exact duplicate replications and consistent accuracy. On all databases identical software is installed 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.

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act of 2002 and information assurance standards published by the National Institute of Standards and Technology. 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 (eg, firewalls, intrusion detection systems, antivirus software), and audit reports.

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 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
- Supervisor and administrator reports 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
- SAO/IP processing by outside agencies

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

Statistical reports are used to analyze data to create metrics based on country and type of request. Also, reports are used to analyze data for 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 by the CCD is obtained through commercial databases and public records such as names, addresses, birth dates, race, identification numbers (e.g. social security numbers) and country of origin. This data is used 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?

CCD is a government-owned system. However, development and support of CCD is provided by contract employees to DOS.

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.

CCD is a government owned system. It is supported by contract employees, who support DOS employees in the maintenance of the system.

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.

All DOS employees and contractors must pass an annual computer security briefing and Privacy Act briefing from both DOS and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

5. Retention

a. How long is information retained?

Record retention depends upon the kind of record involved. Files of closed cases are retired or destroyed in accordance with published record schedules of DOS and as 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.

Regular backups are performed and recovery procedures are in place for CCD. All physical records containing personal 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?

Name of System	Type of Data	Data Flow
ABIS (FR)	Fraud Watchlist data / Photo Identification data	Bi-directional
ACRS	Consular Fee Transaction data	Bi-directional
ACS+	American Citizen data / Personal Identity data	Bi-directional
CST	Shared Database Tables	Bi-directional
CLASS	Consular Lookout and Support System	Bi-directional

Name of System	Type of Data	Data Flow
DataShare	Visa and Passport data	Bi-directional
DVIS	Diversity Visa data	Bi-directional
IVIS	Immigrant Visa Information data	Bi-directional
IVO	Immigrant Visa data, Petition data, Visa Allocation data	Bi-directional
NIV	Non-Immigrant Visa data, Visa refusal data	Bi-directional
VOIS	Visa Opinion Information Service	Bi-directional
WRS	Waiver Request System	Bi-directional

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 under internal DOS policy for the handling and transmission of sensitive but unclassified (SBU) information. Interface Control Document (ICD) and Memo of Understanding (MOU) are used to define and disclose transmission format via the OpenNet.

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

Vulnerabilities and risk are mitigated through the system's certification process. NIST recommendations are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

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 following external agencies share information with the CCD and are allowed to connect to the CCD through a secure portal:

- Department of Homeland Security (DHS)
- Department of Commerce (DoC)
- Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)
- Office of Personnel Management (OPM)

Each of these federal agencies is required to sign an acknowledgement form that defines the manner in which they are to utilize and handle data obtained from the CCD system.

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

Other systems sharing data or having access to CCD are involved in national security; U.S. border security, official government business or federal law enforcement. The sharing of data and access is closely defined by Memorandums of Understanding (MOUs) between the agencies and/or through the connection to OpenNet and then to CCD.

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

Vulnerabilities and risk are mitigated through the system's certification process. NIST recommendations are strictly adhered to in order to ensure all appropriate data transfers and storage methods are applied.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

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

- Passport Records. STATE-26
- Overseas Citizens Services Records. STATE-05
- Visa Records. STATE-39

☐ does NOT contain information covered by the Privacy Act.

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

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-26, Passport Systems; STATE-5, Overseas Citizens Services Records; STATE-39, Visa Records.

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

Personal information regarding individuals is **not** collected directly by CCD; it is received from external agencies, and DOS 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?

Information is **not** collected directly from individuals for specific use in CCD.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's disclosed purposes and uses.

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?

CCD contains Privacy Act covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures fully inform on how to inquire about the existence of records, how to request access to records, and how to request an amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

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?

Each domestic organization appoints a Certifying Authority who is responsible for reviewing each user account request and creating the 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.

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 system, they are authorized to perform all functions commensurate with their official assigned role. The CCD employs logical access controls in accordance with the principle of least privilege and the concept of separation of duties.

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

All users are required to pass annual computer security and privacy awareness training prior to accessing the system, and must complete refresher training in order 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.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level,

are regularly reviewed, and inactive accounts are promptly terminated. Additionally, system audit trails are automatically generated that regularly analyze and review usage in order to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

11. Technologies

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

CCD is a Government off-the-shelf (GOTS) product and has met required security capabilities, design and development processes, required testing and rigorous internal evaluation procedures and documentation

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

No technologies that are known to elevate privacy risk are employed in CCD.

12. Security

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

DOS operates CCD in accordance with information security requirements and procedures required by federal law and internal policy so to ensure that information is appropriately safeguarded and protected. DOS has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, its most recent date of authorization to operate was February 09, 2007 and expires February 28, 2010 (or upon significant change to the system).