



Privacy Impact Assessment (PIA)

Consular Consolidated Database (CCD)

Version 04.00.00

Last Updated: July 17, 2015

1. Contact Information

A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** July 17, 2015
- 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 data warehouse that holds current and archived data from the Bureau of Consular Affairs (CA) domestic and post databases. It was created to provide CA a near real-time aggregate of the consular transaction activity collected domestically and at post databases. CCD is the information technology (IT) implementation that provides for a set of centralized visa and American citizen services supporting consular posts and back office functions.

The three primary functions performed by CCD are: 1) supporting data delivery to approved applications via industry-standard Web Service queries, 2) providing users with easy-to-use data entry interfaces to CCD, and 3) emergency recovery/restoration of post databases. Authorized 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. CCD serves as a gateway to the Automated Biometric Identification System (IDENT). IDENT is DHS' implementation of Commercial Off The Shelf (COTS) technology providing automated fingerprint checking in addition to integration with other Federal biometric systems. The CCD also serves as a gateway to the Department of State Facial Recognition system.

During the course of consular processing activities at posts, applications generate queries to CCD that are routed 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 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 Storage Area Network (SAN) Storage Unit.

The CCD has become an invaluable tool for users as a one-stop access point to data and to prevent and track fraud.

f. Reason for performing PIA:

- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

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

h. Date of previous PIA (if applicable): May 28, 2010

3. Characterization of the Information

The CCD 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 legal permanent residents), as well as foreign nationals (non-US persons) such as Immigrant Visa applicants and Non-Immigrant Visa applicants. This information includes names, addresses, birthdates, biometric data (fingerprints and facial images), race, identification numbers (e.g. social security numbers and alien registration numbers) and country of origin.

The CCD holds current and archived data collected from Consular Affairs domestic and post databases around the world. The CCD provides the central consolidated storage facility for much of the Bureau of Consular Affairs, including the data systems for American Citizens Services (ACS), Passport services, and Visa processing. The CCD uses Visa Opinion Information Service (VOIS) as a Graphical User Interface (GUI) for simplified access to visa data stored within the CCD. The Visa Office is the main user of VOIS for creating Security Advisory Opinions (SAOs) and Advisory Opinions (AOs) for visa applicants. VOIS does not collect data but accesses information contained within the CCD. The CCD is also the repository of data flows between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), and other federal agencies that provide input into the visa and passport review and approval systems.

Visa and passport data provided by foreign nationals or U.S. citizens respectively is covered under the Immigration and Nationality Act or the Privacy Act and therefore subject to confidentiality requirements.

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. The data, collected from domestic and post applications, is replicated from the systems' databases to the CCD.

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 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?

A Service Operations (SO) team monitors the databases to insure exact duplicate replications and consistent accuracy. The configuration management procedures and extensive monitoring and analysis utilities provide daily updates on the data and related software both within the CCD and the systems at posts.

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

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1101-1537 (Immigration and Nationality Act of 1952, as amended (INA) and selected non-INA sections of Title 8 as listed in the Appendix to Bender's Immigration and Nationality Act Pamphlet, 2014).
- 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);
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Citizenship, passport and visa crimes)
- 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)
- 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);
- 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 notary 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; Inter-country Adoption Act of 2000, (Assistance with Inter-country adoptions under the Hague Inter-country 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).
- Title 8 of the Code of Federal Regulations (Aliens and Nationality)
- Title 22 of the Code of Federal Regulations, Parts 1-299 (Foreign Relations)

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

Strict security controls are required by all Department of State systems that are authorized and approved to operate. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft are listed below:

- **Device Theft or Loss**
Lost or stolen laptops and other devices such as removable drives may contain Sensitive But Unclassified (SBU) information. This vulnerability is mitigated by the ban on personal computers, implementation of Web (virtual) technology to maintain data storage within the CCD, and extensive inventory control of removable drives.
- **Removable Media**
Removable media such as USB drives, CDs, DVDs, and MP3 players are prohibited on State Department networks.
- **Insider threat**
Disgruntled employees seeking revenge or inadvertent human error may release SBU information over the internet.

CCD collects, stores, and transmits the minimal amount of PII required to accomplish another Consular Affairs (CA) System request. Job roles/functions permit only the required task to be completed (i.e., the principle of least privilege is implemented to reduce the risk of PII falling into the wrong hands).

4. Uses of the Information

a. Describe all uses of the information.

The information contained in the 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
- Department of State access to outside databases (e.g. United States Citizenship and Immigration Services (USCIS) records)

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 and/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 the 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.

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. This is referred to as a multilayered approach. Monitoring occurs from the moment an authorized user attempts to authenticate to the network. From that point on any changes (authorized or not) that occur to data are recorded. 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 till the time they signed off.. Ultimately it is very difficult to totally prevent an incident from occurring but by implementing a multilayered approach, risk can be greatly reduced.

Database Administrators' (DBA) 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.

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, users are required to sign non-disclosure, acceptable use, conflict-of-interest, and rules of behavior agreements before they can access the Department's internal unclassified intranet (OpenNet) or any CA/CST system.

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. CCD roles determine what a user can do on the CCD. Domestic users, with appropriate access levels and work requirements, can view data for all the posts.

The System Owner 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 the 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 "Secret" level 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 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 SBU paper. 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. Do not access this information in anything other than an official capacity, and do not share it without the permission of the Department of State."

5. Retention

a. How long is information retained?

Record retention depends upon the kind of record involved and is as specified in the U.S. Department of State Records Disposition Schedules, approved by the National Archives and Records Administration. As CCD is a repository for information from various systems, the retention schedules for each record are listed in the Privacy Impact Assessments for the feeder systems listed in 6a.

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 the CCD, regular backups are performed and recovery procedures are in place. All physical records containing personally identifiable information (PII) 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 the CCD. They fall under the purview of the Consular Affairs (CA) Department Designated Approval Authority (DAA). 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. Firewalls and Network Intrusion Detection Systems (NIDS) provide network security that prevents unauthorized access.

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

- Adoption Tracking Service (ATS),
- American Citizen Services (ACS)
- Integrated Biometric System (IBS) a.k.a Automated Biometric Identification System (ABIS) a.k.a FR System
- Automated Cash Register System (ACRS)
- Consular Electronic Application Center Portal (CEAC)
- CEAC Case Tracking (CTRAC)
- CEAC Payment Processing Service (PPS)
- Remote Data Collection (RDC)
- Consular Lookout and Support System (CLASS)
- Consular Shared Tables (CST)

- Diversity Immigrant Visa Information System (DVIS)
- Consular Data Information Transfer System (CDITS)
- Immigrant Visa Allocation Management System (IVAMS)
- Immigrant Visa Information System (IVIS)
- International Parental Child Abduction (IPCA)
- Smart Traveler Enrollment Program (STEP)
- Consular Task Force (CTF)
- Immigrant Visa Overseas (IVO)
- Non-Immigrant Visa (NIV)
- Ten Print Live Scan (TPLS)
- Online Passport Status Service (OPSS)
- Passport Information Electronic Records System (PIERS)
- Passport Lookout Tracking System (PLOTS)
- Petition Information Management System (PIMS)
- Travel Document Issuance System (TDIS)
- Visa Opinion Information System (VOIS)
- Waiver Request System (WRS)

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 rule sets that limit access to 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.

The following safeguards are in place for each sharing arrangement:

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 that PII resides on the database and or servers. Therefore various controls are implemented to reduce the risk of a breach. 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?

Listed below are all the external organizations with which CCD shares information.

The purpose for sharing information between agencies is to improve inter-agency communications and improve the various processes that occur between those agencies for the various functions each system completes.

- Department of Homeland Security (DHS) Office of Biometric Identity Management OBIM
- Department of Homeland Security/ Customs and Border Protection (DHS/CBP)
- Department of Defense (DOD)
- Federal Bureau of Investigation (FBI)
- Federal Bureau of Investigation (FBI) Analysts
- Federal Bureau of Investigation Integrated Automated Fingerprint Identification System (FBI IAFIS)
- Federal Bureau of Investigation (FBI) Namecheck
- Federal Bureau of Investigation Special Technologies and Applications Office (FBI STAO)
- Government Printing Office (GPO)
- DHS Interagency Border Inspection System\Treasury Enforcement Control System (IBIS/TECS)
- DHS Student and Exchange Visitor Information System (SEVIS)
- DHS Terrorist Screening Center (TSC)
- DHS U.S. Citizenship and Immigration Service (USCIS)

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 have various physical connections that allow for the transfer of data securely and effectively.

The following safeguards are 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 including but 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 assessment and authorization process and the security controls that are documented in the MOUs/MOAs mitigate the vulnerabilities and risk. The National Institute of Standards and Technology (NIST) recommendations are implemented in order to ensure that any risk is addressed through the user vetting and authorization process.

8. Notice

The CCD system:

- contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records.
 - Overseas Citizens Services Records-STATE-05 May 02, 2008
 - Passport Records – STATE-26 March 24, 2015
 - Visa Records – STATE-39 October 25, 2012
- does NOT contain information covered by the Privacy Act.

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

Notice is provide at the point of collection for the originating systems, prior to input into the CCD.

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

Not applicable because personal information regarding individuals is **not** collected directly by the CCD. It is received from external agencies and other Department of State systems overseas and at 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?

Not applicable because information in the CCD 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.

Not applicable because data stored in the CCD databases is merely replicated from other systems that connect to it, hence information in the CCD is **not** collected directly from individuals. This information would potentially be provided by the system that originally collected the data.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

The original source systems that populate the CCD provide the notices regarding amendment and redress procedures. It is received from external agencies and other Department of State systems overseas and at domestic posts.

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

The source systems that initially collect the PII data all provide standard notifications regarding the amendment and redress processes offered to individuals. Those processes available to individuals are reasonable based on the systems' stated purposes, uses, and 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 the CCD is limited to authorized Department of State users who 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's 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 reiterates the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Access to the 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.)

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 to access for the CCD is "Moderate," due to the number of agencies that require access to the CCD. Once the user has received access to the CCD, each specific application has the option to require additional access controls. A decentralized access management process was created which allows each post to grant authority to manage its own accounts. Therefore, no single person has access to the entire CCD access list.

11. Technologies

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

The CCD is not available to the public; portable media devices are prohibited on all State Department networks; data uploaded to the CCD from other State Department systems is transmitted via secure methods. Hence, no technologies commonly considered to elevate privacy risk are employed in the CCD.

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 the 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 the 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.

The two main technologies used by the CCD are Oracle for the database servers and SSLv3 for the web servers and the Local Traffic Manager (LTM) devices. In addition, the data uploaded to the CCD from posts is encrypted. 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 patched and fixed during the regular monitoring process.

12. Security

a. What is the security Assessment and Authorization (A&A) status of the system?

The Department of State operates the CCD in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act of 2002 (FISMA), in September 2014, the CCD received a one-year Authorization to Operate (ATO) that will expire September 30, 2015. This document was updated as part of the reauthorization of the system.