PRIVACY IMPACT ASSESSMENT

Consular Consolidated Database (CCD)

1. Contact Information

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

2. System Information

(a) Name of system: Consular Consolidated Database (CCD)

(b) Bureau: Consular Affairs (CA)

(c) System acronym: CA CCD

(d) iMatrix Asset ID Number: 9

(e) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
CCD is currently undergoing an Assessment and Authorization (A&A) to renew its Authorization to Operate (ATO) status. The estimated ATO date is Winter 2018.

(c) Describe the purpose of the system:

CCD is a data warehouse that stores current and archived data from all of the Consular Affairs (CA) post databases around the world. CCD provides CA a near real-time aggregate of consular transaction activity collected domestically and at post databases worldwide.

CCD provides a database solution for centralized visa and American citizen services. The data is replicated from post databases to central CCD databases, and serves as a backup for post's

transaction activity. In addition, the data provides authorized CCD users the ability to create advanced metrics such as workload statistics and trend analysis.

CCD provides users with easy-to-use interfaces via the CCD web portal, and allows emergency recovery of post databases. Authorized Department of State and interagency users utilize the CCD Web Portal to view centralized data through various reports and to gain access to other CA and interagency applications.

CCD is the consolidated storage for the Bureau of Consular Affairs' visa and passport data. 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 (VO) is the main user of VOIS for creating Security Advisory Opinions (SAOs) and Advisory Opinions (AOs) for visa applicants. VOIS does not collect data from individuals, but accesses information contained within the CCD.

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 process.

As part of the visa adjudication process, visa applications generate biographic and biometric checks that are replicated to the central CCD databases. Central CCD then processes the checks or routes them to other agencies. Biometric checks include facial recognition and fingerprint checks. Biographic data is used for namechecks against data within central CCD and for interagency vetting. External agencies provide responses to central CCD, and central CCD returns the results to submitting posts.

CCD is used by internal and the external users/systems for the following purposes:

- Automated screening of applicants in the Consular Lookout and Support System (CLASS)
- Automated checking of applicant fingerprints
- Registration of applicant images for Facial Recognition (FR)
- Reports requesting data on a particular applicant or post, or data from multiple applicants or posts
- Reports that provide reference information for Department of State users, such as post codes and post directory information
- Supervisor and administrator reports to track work or review applicant data
- Distributing data to interagency partners for visa and passport vetting
- Reports which display the status of post databases and post upgrades
- Security Advisory Opinion (SAO)/Improvement Project (IP) processing by outside agencies

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

The CCD stores information about U.S. citizens and legal permanent residents (hereafter "U.S. persons"), as well as foreign nationals (hereafter "non-U.S. persons") such as nonimmigrant and immigrant visa applicants. The PII in CCD includes, but is not limited to:

- Names
- Home/business addresses
- Birthdates
- Biometric data (fingerprints and facial images)
- Phone numbers
- Email address
- Financial information
- Race
- Gender
- Identification numbers (e.g. social security numbers and alien registration numbers)
- Personnel Information
- Nationality
- Passport information
- Medical information (DS-2054, DS-3025, DS-3026, DS-3030)
- Legal information
- Education information
- Family information
- Arrests and convictions
- Social media indicators

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

- 5 U.S.C. 552a (Privacy Act of 1974 as amended);
- 8 U.S.C. 1101-1537 (Immigration and Nationality Act of 1952, as amended (INA)), including 8 U.S.C. 1104 (Powers and Duties of the Secretary of State) and 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens); and selected non-INA sections of Title 8 as listed in the Appendix to Bender's Immigration and Nationality Act Pamphlet, 2018 edition);
- Omnibus Consolidated Appropriations Act, 1997, PL 104-208, September 30, 1996
- Illegal Immigration Reform and Immigration Responsibility Act, PL 104-208, Div. C, September 30, 1996

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107–56, October 26, 2001
- Enhanced Border Security and Visa Entry Reform Act of 2002, PL 107-174, May 14, 2002
- Child Status Protection Act of 2002, PL 107–208, August 6, 2002 (an Act to amend the Immigration and Nationality Act of 1952);
- 18 U.S.C. 911, 1001, 1541–1546 (Citizenship, passport and visa crimes);
- 22 U.S.C. 2651a (Organization of the Department of State);
- 22 U.S.C. 3927 (Chief of Mission);
- 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 providing assistance to other agencies);
- 22 U.S.C. 211a et seq.(U.S. Passports);
- 22 U.S.C. 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number);
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries);
- 22 U.S.C. 2705 (U.S. Passports and Consular Reports of Birth Abroad);
- 22 U.S.C. 2671(b)(2)(A)-(B) and (d) (Evacuation assistance and repatriation loans 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);
- 22 U.S.C. 5501–5513 (Aviation disaster and security assistance abroad; mandatory availability of airline passenger's manifest);
- 22 U.S.C. 4195, 4196; (Official notification of death of U.S. citizens in foreign countries; transmission of inventory of effects) (22 U.S.C. 4195, repealed, but applicable to past records);
- 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 (Receiving protests or declarations of U.S. citizen passengers, merchants in foreign ports);
- 22 U.S.C. 4194 (Lists and returns of seamen and vessels);
- 22 U.S.C. 4205–4207 (Services to American vessels or seamen, prohibitions);
- 46 U.S.C. 10318 (Wages on discharge of seaman in foreign port);
- 46 U.S.C. 10701-10711 (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);
- 22 U.S.C. 4802 (Responsibility for security and protective functions of U.S. missions abroad and domestic Department of State offices);
- 26 U.S.C. 6039E (Information concerning resident status);
- 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. 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)(Benefits ended, but applicable to past records);
- 42 U.S.C. 14901–14954; Inter-country Adoption Act of 2000, as amended (Implementing legislation for the Convention on Protection of Children and Co-operation in Respect of Intercountry Adoption, done at The Hague on May 29, 1993);
- 22 U.S.C. 9001-9011, International Child Abduction Remedies Act (implementing legislation for the Convention on the Civil Aspects of International Child Abduction, done at The Hague October 25, 1980; 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. 9101, 9111–9114, 9121–9125, 9141, International Child Abduction Prevention and Return (implementing legislation for the Convention on the Civil Aspects of International Child Abduction, done at The Hague October 25, 1980; reporting requirements, prevention measures, and other assistance on international parental child abduction cases);
- 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);
- Executive Order 11295, of August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. Passports);22 C.F.R. Part 22 (Schedule of Fees for Consular Services –Department of State and Foreign Service);
- 22 C.F.R. Parts 40-42, and 46 (Visas);
- 22 C.F.R. Parts 50, 51 and 52 (Nationality Procedures and Passports);
- 22 C.F.R. Part 71 (Protection and Welfare of Citizens and Their Property);
- 22 C.F.R. Part 72 (Deaths and Estates);
- 22 C.F.R. Part 92 (Notarial and Related Services);
- 22 C.F.R. Part 93 (Service on Foreign State);
- 22 C.F.R. Parts 96 -99 (Intercountry Adoptions)

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

STATE-26, Passport Records, March 24, 2015
STATE-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016
STATE-39, Visa Records; June 15, 2018
STATE -77, Country Clearance Records, October 3, 2011

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number:

A-15-001-01 Consular Services Policy File
Description: Consists of correspondence and reports which document the development and implementation of policies, procedures, agreements, regulations, and legislation pertaining to the provision of consular services. Excludes material regarding routine operational and administrative activities and material concerning matters for which other offices have primary responsibility
Disposition: Permanent. Retire to the RSC when 5 years old. Transfer to the National Archives when 15 years old.
DispAuthNo: NC1-059-77-28, item 1

A-15-001-02 American Citizens Services (ACS) system
Description: The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts. ACS records include case level data on the following types of citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases;

lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Record level data includes· biographic information, case information, and case activity log.
Disposition Temporary: Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is later.
DispAuthNo: N1-059-09-40, item 1

A-15-002-01 General Policy Files (Abduction and Adoption) - Arrange by subject
Description: Memorandums, correspondence, telegrams, court decisions, briefing papers, and other material relating to matters handled by the Office of Children's Affairs.
Disposition Temporary: Permanent. Cut off files when 10 years old and transfer to RSC for transfer to WNRC. Transfer to the National Archives when 25 years old
DispAuthNo: N1-059-97-14, item 1

A-15-002-02 Child Custody/Abduction Case Files
Description: Cases reflect applications filed for the return of children abducted to countries that are party and not party to the Hague Abduction Convention. Included are requests for assistance in locating children taken by the other parent, legal proceedings, information of available courses of action, monitoring the welfare of a child, information on child custody laws and procedures in the host country, and related correspondence.
Disposition: Cases reflect applications filed for the return of children abducted to countries that are party and not party to the Hague Abduction Convention. Included are requests for assistance in locating children taken by the other parent, legal proceedings, information of available courses of action, monitoring the welfare of a child, information on child custody laws and procedures in the host country, and related correspondence.
DispAuthNo: N1-059-97-14, item 2

A-15-002-03 Adoptions Tracking Service (ATS)
Description: ATS records include the following types of information: unique identifier, case status and tracking information, application information, adoptive parent information. child information, Hague Convention documentation, inquiry and complaint information, and adoption agency information.
Disposition: Temporary. Cut off at end of calendar year when adoption case closes. Destroy 75 years after adoption case closed.
Disposition: N1-059-09-09, item 1

A-13-001-16 Passport Lookout Master
Description: This online information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have

been denied passports, or those who are not entitled to the issuance of full validity passport and those whose existing files must be reviewed prior to issuance.
Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)
DispAuthNo: N1-059-04-2, item 16

A-13-001-23 Routine Passport Application Status Check and Expedite Fee Upgrades Email
Description: Email messages regarding the status of passport applications and requests for expedited service.
Disposition Temporary: Destroy/delete when 25 days old
DispAuthNo: N1-059-98-03, item 1

A-13-002-02 Requests for Passports
Description: Copies of documents relating to selected passport requests.
Disposition: Temporary: Cutoff at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty five (25) years old.
DispAuthNo: N1-059-05-11, item 2

A-13-002-03 Tracking/Issuance System
Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition: Permanent: Delete when twenty five (25) years old.
DispAuthNo: N1-059-05-11, item 3

A-14-001-03 thru A-14-001-24 Tracking/Issuance System
Description: Visa records on Aliens.
Disposition/DispAuthNo: Permanent or as depicted by the specific record item disposition authority.

B-09-001-01a thru B-0900-10 Passport and Citizenship Case Files, Correspondence and Citizenship Requests
Description: These records pertain to American citizens abroad who have applied to overseas posts for passports, the renewal, amendment or extension of passports, or for registration and other citizenship services; and files pertaining to American citizens who have applied to territorial governments for passport services. Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition/DispAuthNo: The length of time the record will be kept is dependent on the specific item and the applicable disposition rules in B-09-001-01a -10.

B-09-002-01a Immigrant Visas Issuances (Consular Consolidated Database
Description: Information obtained from issued immigrant visa application forms (DS-23, 260, and related forms) and supporting documentation. Immigrant visa case records potentially include the following types of case level data: unique identifier; applicant personal and biographical data; adjudication data; visa class information; visa clearance and name check data; case summary data; case status data; and notes

Disposition: Temporary. Cutoff at end of calendar year when issued. Destroy 11 years after issuance.
DispAuthNo: N1-084-02-02, item 1a

4. Characterization of the Information

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

☒ Members of the Public (are U.S. citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?

26 USC§ 6039E – Information Concerning Resident Status
Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008

(c) How is the information collected?

All data is voluntarily provided by applicants upon completion of applications from the system in which services are being requested. The data is stored on the respective systems that collect it. Through the CCD replication process, a copy of the data is stored in the CCD from the consular systems domestically, at posts, and from external government agencies. The data collected from domestic and post applications are replicated from the systems' databases to the CCD.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

CA's Consular Systems and Technology (CST) teams monitor the databases to ensure replication from post to central is consistent and accurate. 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.

No data is collected by CCD from applicants. Information accuracy is managed in accordance with the system's procedures where the end user is submitting an application for services.

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

Data is replicated from post databases to the CCD database approximately every 60 seconds. Requests go directly from the post database server to the Local Traffic Manager server, which sends the request to the CCD database cluster for storage.

Ensuring posts'/federal agency information is current is a process managed in accordance with the system where the end user is submitting an application requesting services.

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

Some information stored in the CCD, such as names, addresses, birth dates, race, social media indicators, and country of origin, submitted by federal agencies may come from commercial databases and/or public records. This data is used by analysts to support national security, U.S. border security, official government business and/or federal law enforcement.

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

Although CCD maintains and processes information with U.S. person data that is subject to the Privacy Act and non-citizen data that is subject to INA 22(f), the CCD system is not a public facing system. The data in CCD is replicated from other systems after the applicant provides documents/information to the Department of State when applying for consular services. Notification is provided by the visa and passport applications that originally collect the information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, **how** do individuals grant consent?

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

CCD information is replicated from other Department of State /Federal agency systems that provide the notice and consent at the information collection point for services requested. Consent is documented in the visa and passport applications and in case information.

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

The PII items replicated in the CCD system are the minimum necessary to perform the actions required by this system supporting visa and American citizen services. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the systems to perform the functions for which they are intended.

5. Use of information

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

The intended use of the PII in the CCD is to support the Department of State's centralized visa and American citizen services program. The information consists of current and archived data from post databases and other federal agencies to support the transaction process in reviewing and providing consular services.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information is for the management of the Department of State's centralized visa and American citizen services programs. The collection is required to make determinations for granting the various consular services being requested.

(c) Does the system analyze the information stored in it?

☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

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

Internally: Department of State users, including post users and associated systems.

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

- Adoption Tracking Service (ATS)
- American Citizen Services (ACS)
- Automatic Biometric Identification System (ABIS)
- Automated Cash Register System (ACRS)
- Consular Electronic Application Center Portal (CEAC)
- Consular Lookout and Support System (CLASS)
- Consular Shared Tables (CST)
- Diversity Immigrant Visa Information System (DVIS)
- Consular Data Information Transfer System (CDITS)
- electronic Document Processing (eDP) Web
- Immigrant Visa Allocation Management System (IVAMS)
- Immigrant Visa information System (IVIS)
- International Parental Child Abduction (IPCA)
- Internet-based Registration Service/Consular Task force (IBRS/CTF)
- Enterprise Visa Application Forms (EVAF)
- Smart Traveler Enrollment Program (STEP)
- 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)
- Passport Records Imaging Systems Management (PRISM)
- Travel Document Issuance System (TDIS)
- Visa Opinion Information System (VOIS)
- Waiver Review System (WRS)

External Federal Agencies:

- Department of Homeland Security (DHS)
- Department of Commerce
- Department of Defense (DoD)
- Department of Justice (DOJ)
- Government Printing Office (GPO)
- Office of Personnel Management (OPM)
- Federal Bureau of Investigation (FBI),
- Other Interagency Partners

Each interagency partner 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 the access to data.

(b) What information will be shared?
The various PII information listed in paragraph 3d is shared internally and externally based on the requirement.

(c) What is the purpose for sharing the information?
Sharing of information is required for the submission, processing, adjudication and approval/denial decisions of consular services.

(d) The information to be shared is transmitted or disclosed by what methods?
Information transmitted internally is via interconnected State Department systems.

Information is transmitted via interagency partners using Department of State approved secure transport layer security methods and interconnections.

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

Internal recipients, within the Department of State, must comply with U.S. government requirements for the protection and use of PII. These safeguards include but are not limited to security training and following internal Department policy for the handling and transmission of "Sensitive but Unclassified" information. In addition, all Department users are required to attend annual security awareness training to reinforce safe handling practices of information. Internal sharing requires a connection agreement and OpenNet users with privileged role-based access to manage the connection. Communication is secured using transport level security.

External agencies that share information with CCD interconnect through either the managed Multi-Protocol Label Switching (MPLS) or connection via the Department of State's extranet. CCD is not internet facing. All external agencies that share information with the CCD are required to sign a Memoranda of Understanding (MOU) with the Department of State, which generally defines a set of responsibilities and requirements. Items generally covered in the MOU 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.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to unauthorized parties: Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization, and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

b. Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal, or other.

The Department of State mitigates these risks by enforcing rules and requirements using a multifaceted approach to security requirements regarding:

- Frequent security training on information security for all users, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization, and need-to-know.

- System authorization and accreditation process along with continuous monitoring. Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared internally are encrypted as per the Department of State's Security Configuration Guides' security policies and procedures.

7. Redress and Notification

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

Individuals are unable to access their information in the CCD. CCD does not collect information directly from applicants. CCD data originates from consular affairs visa and passport systems and from interagency partner systems.

Notices to individuals on how to access their information are provided at the point of collection of information for the system where services are being requested. Procedures for notification and redress are also published in the System of Records Notice (SORN) Passport Records – STATE-26, Visa Records-STATE -39, and in rules published within 22 CFR 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

Procedures are provided to individuals at the point of data collection, prior to replication into the CCD. CCD does not collect information directly from applicants. CCD data originates from consular systems and from interagency partners.

If no, explain why not.

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

Procedures are provided to individuals at the point of data collection, prior to replication into the CCD. The source system where the data originates provides notices on how to correct information.

Guidance is also outlined in SORNS STATE 26 (Passport Records) and STATE 39 (Visa Records) and in rules published at 22 CFR 171, informing the individual how to inquire about the existence of records, how to request access to records, and how to request amendment of a record.

8. Security Controls

(a) How is the information in the system secured?
The CCD system is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous

monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Applications are configured according the Department of State's Security Configuration Guides to optimize security while still providing functionality. This complies with federal regulations and the Federal Information System Management Act (FISMA). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

To access the CCD system, persons must be authorized users of the Department of State's unclassified network, which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Each authorized user must electronically agree to the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the CCD system is role based, and restricted according to job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Information System Security Officers determine the access level needed by a user to ensure it correlates to the user's particular job function and level of clearance.

Data shared with other government agencies is carefully regulated according to an MOU and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency.

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

The level of access granted to CCD restricts the data that may be viewed and the degree to which data may be modified. Administrative activity is monitored, logged, and audited.

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides and conduct annual control assessments (ACA) to ensure that all

systems/applications comply and remain compliant with Department of State and federal policies. Additionally, configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor OpenNet-connected systems that host CA's major and minor applications for any changes to security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with Department of State Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State Security Configuration Guides, auditing is enabled to track events on the host operating systems and back-end database servers.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating system (OS) level auditing is set in accordance with the Department of State Security Configuration Guides. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application log provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

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

In accordance with Department of State computer security policies, mandatory annual Cyber Security Awareness training, with a privacy component, is required for all authorized users. The Department of State's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users digitally agree to the rules and acknowledge that they must protect PII through appropriate safeguards to ensure security, privacy and integrity. All Department of State users are required to complete the mandatory FSI course, PA 459 Protecting Personally Identifiable Information.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational, and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists, are in use. System and information integrity auditing are implemented to monitor and record possible attempts of unauthorized access or data manipulation. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

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

Organizations or individuals whose PII has been breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss.

Security measures are in place to minimize that risk, and to minimize the risk of harm to Department of State programs or the public interest through an unauthorized release of sensitive information. The security measures listed above were implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

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

The following personnel have access to the CCD: Post users/OpenNet-based users, Domestic users, CCD Administrators (System, application, database, network, and web) and External Agency Users.

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

Access is determined and based on individual job functions which are approved by the supervisor and ISSO. Access is role based and the user is granted only the role(s) required to perform officially assigned duties. Interagency account access is granted by the Consular Affairs Visa Office and determined based on their mission and the Department's mission and authorities.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

☒Yes ☐No

Information is documented in the CCD System Security Plan. The plan includes information regarding roles and system access to data.

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

Users other than administrators will not have access to all data in the system. Separation of duties and least privilege is employed allowing users access to only the data required and approved by the supervisor to perform official duties.

Internal Department of State Users

Post Users/OpenNet-based Users

Post users include U.S. Citizens and local hires from the country where the U.S. embassy or consulate is located. All of these users can view CCD data, but there are restrictions to which data each user has access, based on job responsibility.

Domestic Users/OpenNet-based Users

Domestic users within the United States include both U.S. government employees and contractors. Domestic organizations are made up of groups of people who either work at the same physical location or have related job assignments or both. 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.

Administrators (System, application, database, network and web)

Administrators include both U.S. government employees and contractors. CCD System Administrators are responsible for daily CCD maintenance, including establishing access control lists, backups, managing user accounts, software upgrades, patches, database configurations and establishing, activating, modifying, reviewing, disabling, and removing accounts.

External Agency Users

In addition to the users within Department of State, CCD data is used by numerous external agencies. These agencies are able to access CCD through a web interface (CCDi) via the Department's extranet. Once in CCDi, users are permitted access to the appropriate CCD data marts based on their assigned user role.

Each external agency has at least one Certifying Authority who is responsible for managing the users within the organization.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

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

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

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Audit logs are reviewed at the Application, Database, and System level,

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN) and activities while logged in can be traced to the person that performed the activity.