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) Date of completion of this PIA: November 2022
(b) Name of system: Consular Consolidated Database
(c) System acronym: CCD
(d) Bureau: CA/CST
(e) iMatrix Asset ID Number: 9
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

CCD is a data warehouse that stores current and archived data from all 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, providing database solutions for centralized visa and American citizen services.

The data is transmitted and replicated from post databases to central CCD databases and serves as a backup for the 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 supports data delivery to applications and agencies via the Consular Affairs Enterprise Service Bus (CAESB), which provides users easy-to-use data entry interfaces and allows emergency recovery of post databases. Authenticated Department of State employees and other authorized government agency personnel use CCD to view the centralized data through various reports, and to gain access to other CA and interagency applications.

As part of the visa adjudication process, visa applications generate biographic and biometric checks that are replicated to the CCD databases. CCD 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 CCD and for interagency vetting. External agencies provide responses to CCD, and 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 Opinions (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, legal permanent residents, foreign nationals (such as passport applicants), U.S. citizen services, and non-immigrant and immigrant visa applicants. Hereafter, U.S. citizens and legal permanent residents will be referred to as "U.S. persons" and foreign nationals as "non-U.S. persons." PII in CCD includes, but is not limited to:

Data Collected	Non-U.S. Persons: Non-	U.S. Persons

	Immigrant & Immigrant Visa Applicants	
Name (first and last)	X	X
Home Address	X	X
Date of Birth	X	X
Place of Birth	X	X
Citizenship	X	X
Gender	X	X
Home Phone Number	X	X
Race		X
Personal Email Address	X	X
Biometrics (facial recognition and fingerprint)	X	X
Social Security Numbers		X
National Identification Numbers	X	
Passport Information	X	X
Educational Information	X	X
Nationality	X	X
Driver's License Information	X	X
Work Phone Number	X	X
Mobile Phone Number	X	X
Delivery Address (if address differs from home address)	X	X
Business Address	X	X
Financial Account Information	X	X

Personnel/Employment Information (Business Contact Information)	X	X
Family Information	X	X
Medical Information	X	X
Photos	X	X
Legal Information	X	X
Arrests/Convictions	X	X
Social Media Indicators	X	
Mother's Maiden Name	X	X
Other substantive Individual Information (hair color, height, marriage/divorce information, etc.)	X	X
Substantive family information	X	X
Substantive medical information	X	X
Petitioners/legal representation	X	

Petitioners/lawyers assisting applicants in applying for Consular services may be U.S. citizens, where the PII consist of names, titles, emails, phone numbers and addresses.

Note: CCD also contains Department of State Consular employee business information, such as name, title, general schedule grade, post information, email, and phone number.

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

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 22 U.S.C 2651a (Organization of Department of State)
- 22U.S.C. 211a (Authority to Grant, Issue and Verify Passports)
- 22 U.S.C. 3904 (Functions of Service)

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

☒Yes, provide:

- SORN Name and Number: Passport Records, STATE-26
  SORN publication date: March 24, 2015

- SORN Name and Number: Overseas Citizens Service Records and Other Overseas Records, STATE-05
  SORN publication date: September 8, 2016

- SORN Name and Number: Visa Records, STATE-39
  SORN publication date: November 8, 2021

☐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 Office 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 (Consolidate as much as possible):

Schedule number: A-15-001-001
Disposition Authority Number: NC1-059-77-28, item 1
Length of time the information is retained in the system: Permanent. Retire to the Records Schedule Center when 5 years old. Transfer to the National Archives when 15 years old.
Type of information retained in the system: 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.

Schedule number: A-15-001-03
Disposition Authority Number: N1-059-09-40, item2
Length of time the information is retained in the system: TEMPORARY. Cut off when case closed/abandoned. Destroy 20 years after cut off or when no longer needed, whichever is later.
Type of information retained in the system: Case files covering the following 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. Case level data includes biographic information, case information, and case activity log.

Schedule number: A-15-002-01
Disposition Authority Number: N1-059-97-14, item 1
Length of time the information is retained in the system: Permanent. Cut off files when 10 years old and transfer to RSC for transfer to Washington National Records Center (WNRC). Transfer to the National Archives when 25 years old.
Type of information retained in the system: Memorandums, correspondence, telegrams, court decisions, briefing papers, and other material relating to matters handled by the Office of Children's Affairs.

Schedule number: A-15-002-02
Disposition Authority Number: N1-059-97-14, item 2
Length of time the information is retained in the system: Transfer to the RSC after the case is deemed closed and no action has taken place for 1 year for transfer to the Washington National Records Center (WNRC). Destroy when 15 years old.
Type of information retained in the system: 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.

Schedule Number: A-15-002-03
Disposition Authority Number: N1-059-09-09, item 1
Length of time the information is retained in the system: Temporary. Cut off at end of calendar year when adoption case closes. Destroy 75 years after adoption case closed.
Type of information retained in the system: Adoption Tracing Service (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.

Schedule Number: A-13-001-16
Disposition Authority Number: N1-059-04-2, item 16
Length of time the information is retained in the system: Destroy when active agency use ceases.
Type of information in the system: 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.

Schedule Number: A-13-001-23
Disposition Authority Number: N1-059-98-03, item 1
Length of time the information is retained in the system: Destroy/delete when 25 days old
Type of information in the system: Email messages regarding the status of passport applications and requests for expedited service.

Schedule Number: A-13-002-02
Disposition Authority Number: N1-059-05-11, item 2
Length of time the information is retained in the system: 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.
Type of information in the system: Copies of documents relating to selected passport requests.

Schedule Number: A-13-002-03
Disposition Authority Number: N1-059-05-11, item 3
Length of time the information is retained in the system: Permanent: Delete when twenty-five (25) years old.
Type of information in the system: Electronic database used for maintenance and control of selected duplicate passport information/documentation.

Schedule Number: A-14-001-03 thru A-14-001-24
Disposition Authority Number: Various
Length of time the information is retained in the system: Permanent or as depicted by the specific record item disposition authority.
Type of information in the system: Visa records on aliens.

Schedule Number: B-09-001-01a thru B-900-10
Disposition Authority Number: Various
Length of time the information is retained in the system: 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.
Type of information in the system: 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.

Schedule Number: B-09-002-1a
Disposition Authority Number: N1-084-02-02, item 1a
Length of time the information is retained in the system: Temporary. Cutoff at end of calendar year when issued. Destroy 11 years after issuance.
Type of information in the system: 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.

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
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) 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

(d) How is the PII collected?

All data is voluntarily provided by applicants upon completion of applications/information from various source systems (CA and other government agency systems) in which services are being requested and adjudicated. The data is collected and stored on the respective source systems and is transmitted and replicated to the CCD. Information transmitted consists of consular systems at posts, and from external government agencies. The data collected from post applications and government agencies are replicated from the source systems' databases to the CCD.

(e) 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.

(f) What process is used to determine if the PII is accurate?

The data is transmitted and replicated to CCD from various source systems. Agencies transmitting information to the CCD are responsible for the accuracy of the data. Information accuracy is managed in accordance with the source system's procedures where the end user applies for services.

CA personnel monitor the databases to ensure replication from posts to CCD 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.

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

Ensuring information is current is a process managed in accordance with the various source systems where the end user submits an application requesting consular services. Department of State data is replicated from post databases and agencies to the CCD database approximately every 60 seconds for currency. Requests go directly from the post database and government agency servers to the CCD database for storage and retrieval.

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

Yes, information is used from LexisNexis to assist Department of State Consular Affairs personnel in the adjudication of visa and passport applications in verifying renewal requester's information by detecting errors or fraudulent information. No, the information is not publicly available.

(i) How was the minimization of PII in the system considered?

The PII listed in 3d is the minimum necessary to perform the actions required by the CCD to support visa, passport, and American citizen services. Concerns about collecting and maintaining PII include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were assessed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended to serve as the CA central storage and retrieval database of CA post and federal agency consular service information.

5. Use of information

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

The intended use of the PII in the CCD is to support the Department of State's centralized visa, passport, and American citizen services program. The PII consist of current and archived data from post databases and other federal agencies to support the transaction process in reviewing and validating applicant information, such as submission of application requests for CA services, conducting namechecks, fingerprint, and facial recognition checks against CA source systems and interagency vetting.

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

Yes, the information in the CCD centralized database supports the implementation of the Department of State's visa, America citizens and passport programs. The information is required to make determinations for granting the various consular services being requested to validate applicant information and to provide centralized storage of information internally for use by posts, in addition to sharing and validating information with other government agencies.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

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

(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

(d) If the system will use test data, will it include real PII?
☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal:
The term "internal sharing" traditionally refers to the sharing of information within the Department of State, but external to the owning organization (referred to as "bureau" at Department of State). However, since the various Bureau of Consular Affairs offices

have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in CCD is shared internally with the following CA systems:

- Adoption Tracking Service (ATS)
- American Citizen Services (ACS)
- Integrated Biometric System (IBS)
- Consular Electronic Application Center Portal (CEAC)
- CA Enterprise Service Bus (CAESB)
- Consular Lookout and Support System (CLASS)
- Consular Launchpad for Enterprise Analytics and Reporting (CLEAR)
- Consular Affairs Crisis Management System (CACMS)
- 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)
- Immigrant Visa Overseas (IVO)
- Non-Immigrant Visa (NIV)
- Passport Information Electronic Records System (PIERS)
- Passport Lookout Tracking System (PLOTS)
- Travel Document Issuance System (TDIS)
- Waiver Review System (WRS)
- Online Passport Renewal (OPR)
- Smart Traveler Enrollment Program (STEP)

CCD also shares with the Department of State's Bureau of Nonproliferation (DOS/NP) and the Office of Foreign Missions (OFM).

External:
CCD shares information externally with the following agencies:

- Department of Homeland Security (DHS)
- 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?

Internal:
The PII listed in 3d is shared with the internal CA systems, DOS/NP and the OFM.

External: Information listed in 3d is shared with other government agencies listed in 6a based on what is required by that agency.

(c) What is the purpose for sharing the information?

Internal:
The PII listed in section 3d is shared with internal CA systems and DOS/NP to validate applicant information requesting consular affairs services and to provide the requested consular services to U.S. persons and non-U.S. persons.

External:
PII in the CCD is shared externally to validate information provided by individuals requesting consular affairs services in addition to sharing information in connection with fraud investigations, law enforcement requests, or counterterrorism and border security efforts to support the Department's consular affairs and federal agency missions.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
The information is shared by secured internal database to database connections with the Consular Affairs Consular Consolidated Database (CCD) system. Data in transit is encrypted and protection is implemented in accordance with Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information. Information is also shared with DOS/NP by the same methods.

External:
Agencies can receive and transmit information via CCD using the managed Multi-Protocol Label Switching and secure internet protocol security (IPsec) tunnels via the internet with all connections through the Department of State OpenNet.

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

Internal:

Safeguards in place for internal sharing arrangements include secure transmission methods such as data encryption using Hypertext Transfer Protocol Secure (HTTPS) and secure communications using Transport Layer Security and multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers. These safeguards are permitted by internal Department of State policies for handling and transmission of sensitive but unclassified (SBU) information. Electronic files are personal identity verification/personal identification number (PIV/PIN), or password protected, and access is controlled by system managers. Audit trails track and monitor usage and access of systems that reside on the Department's secure intranet network, OpenNet.

External:
Safeguards for external agencies sharing of information include the use of (HTTPS) encryption and secure socket layers (SSL). All external agencies that share information with the CCD are required to sign a Memoranda of Understanding (MOU)/and or an Interconnection Security Agreement (ISA) with the Department of State, which defines a set of responsibilities and requirements in the handling and sharing of information. Items generally covered in the MOU include, but are not limited to trusted behavior expectations, user community, access controls, audit trail responsibility, data ownership, securing data sharing transmission, security parameters, incident handling and reporting, antivirus and security training and awareness.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

The information in CCD is obtained from other CA systems and external agency systems. When the collection of information by the source system involves potential PII collected on U.S. persons, there is a Privacy Act Statement displayed on the form in which the applicant is seeking a consular service, such as a passport.

Non-U.S. person data is subject to the requirements of the Immigration and Nationality Act (INA)222(f) which are stated on the collection site of the source system collecting the PII.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

Consent is acquired via the source systems in which the information is originally obtained when applicants request consular services. CCD provides CA a near real-time aggregate of consular transaction activity collected where agency and post databases pull and receives information from the system

(c) What procedures allow record subjects to gain access to their information?

CCD data originates from consular affairs visa and passport systems and from interagency partner systems. Procedures are provided to individuals at the point of data collection in the source system where the applicant applies for the Consular Affairs service, prior to replication into the CCD. Procedures for access are also published in the System of Records Notices (SORNs) STATE-05, STATE-26, STATE -39, and in rules published within 22 CFR 171.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Guidance on procedures which allow a record subject to correct their information is outlined in SORNS STATE-05, STATE-26, and STATE-39, and in the rules published at 22 CFR 171, informing the individual how to inquire about the amendment of a record. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Notifications to correct records are provided via the adjudication process of the source system collecting the information from the individual requesting the specific service and housed in CCD. Individuals can also follow procedures in SORNs STATE 05, STATE-26, and STATE-39, regarding points of contacts listed for individuals wanting to correct their information. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

8. Security Controls

(a) How is all of the information in the system secured?

The system is secured within the Department of State intranet where risk factors are mitigated using 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 to perform official duties.

Access to CCD is controlled at the system level with additional access controls at the application level that requires a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN). This meets the dual authentication requirement for federal systems access that is required for logon. All accounts must be approved by the user's supervisor/manager and the local Information System Security Officer (ISSO). The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

Systems are configured according to the State Department Security Configuration Guides to optimize security while still providing functionality (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) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Department of State Internal Users:
Access to CCD is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. System administrators, database administrators, web administrators, network device administrators, and Department of State employees have access to the system to maintain the CCD, and aid in processing American citizen services, passport, and visa applications.

External Agency Users:
In addition to the users within Department of State, CCD data is used and shared with numerous external agencies to validate information of users requesting CA and or agency sponsored services.

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

Access to CCD is role-based and restricted according to job responsibilities approved by the manager/supervisor. Supervisors and the local Information System Security Officers (ISSO) determine the access level needed by a user to ensure it correlates to the user's particular job function, manager's approval, and level of clearance. Access control lists permit categories of information and reports that are restricted by roles. Local ISSOs validates the access level needed by a user to ensure it correlates to the user's particular job function and level of clearance.

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.

(d) How is access to data in the system determined for each role identified above?

In accordance with Department of State policy, CCD employs the concept of least privilege for each user by allowing only authorized access to information in the system necessary to accomplish assigned job and tasks as approved by the manager/supervisor. This is accomplished via email/ and or a form. All roles have been analyzed to determine the specific data set and corresponding functions that will be required in accordance with the person's job and level of security approved by the supervisor. Accordingly, when a user or service account is added to a particular database role, access is limited to only the approved data and functions allotted.

All interagency partners have 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 agency user's approve role based on the job requirements.

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

The CCD audit service on its servers captures many logs, access attempts, an all actions exceeding the Department of State requirements. Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information in CCD. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system.

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

☒Yes ☐No

The CCD System Security Plan includes information and procedures regarding access to data in CCD.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially. The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.