PRIVACY IMPACT ASSESSMENT

ConsularOne Database Infrastructure (CA CDI)

1. Contact Information

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

2. System Information

(a) Name of system: ConsularOne Database Infrastructure

(b) Bureau: Consular Affairs (CA)

(c) System acronym: CA CDI

(d) iMatrix Asset ID Number: 253145

(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?

The initial Assessment and Authorization process is underway and CA CDI is expected to receive an Authorization-To-Operate by Summer 2018.

(c) Describe the purpose of the system:

ConsularOne is a major system that supports modernization efforts intended to replace outdated legacy applications. This modernized system moves paper-based services to be processed electronically (online), allowing citizens and non-citizens to request services from Consular Affairs (CA). Using a Service Oriented Architecture (SOA), the system decouples service capability to improve performance, scalability, and speed-to-market.

The purpose of CA CDI is to store much of the data related to ongoing ConsularOne operations. CA CDI stores data associated with processing of visa, passport, and citizen services, including pictures, fingerprints, case documents, and photos. In addition, CA CDI stores administrative files related to backups and logs. The CA CDI system stores all data entered into the CA ConsularOne Application and Data (CAD) system. CA CAD provides the interface to the end user requesting services. Data processed by CA CAD is stored in CA CDI. All data is transmitted database-to-database.

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

The PII collected by the system is based on information requirements supporting ConsularOne modernization effort.

General PII categories include:

- Names
- Birthdates
- Financial account numbers
- Social Security Numbers
- Phone number(s)
- Home Address
- E-mail address(es) of individuals
- Images or biometric identifiers
- Medical information
- Financial information
- Legal information
- Family information
- Educational information

(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 et seq., Immigration and Nationality Act of 1952, as amended, including 8 U.S.C. 1104 Powers and duties of Secretary of State and 8 U.S.C. 1185, Travel Documentation of Aliens and Citizens;
- 22 U.S.C 2651a (Organization of 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);

- 8 U.S.C. 1401, 1408, and 1409 (Citizens and nationals of the United States by birth);
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries);
- 22 U.S.C. 211a et seq. (Passport application and issuance);
- 22 U.S.C. 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- 22 U.S.C. 2705 (U.S. Passports and Consular Reports of Birth Abroad);
- 8 U.S.C. 1501–1504 (Adjudication of possible loss of nationality and cancellation of U.S. passports and CRBAs);
- 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);
- 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);
- 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. 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, 4194; 22 U.S.C. 4205–4207; 46 U.S.C. 10318 (Merchant seamen protection and relief);
- 22 U.S.C. 4193 (Receiving protests or declarations of U.S. citizen passengers, merchants in foreign ports);
- 46 U.S.C. 10701–10705 (Responsibility for deceased seamen and their effects);
- 22 U.S.C. 2715a (Responsibility to inform victims and their families regarding crimes against U.S. citizens abroad);
- 22 U.S.C. 4215, 4221 (Administration of oaths, affidavits, and other notarial acts);
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 28 U.S.C. 1740, 1741 (Authentication of documents);

- 28 U.S.C. 1781–1785 (Judicial Assistance to U.S. and foreign courts and litigants);
- 42 U.S.C. 14901–14954(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);
- Intercountry Adoption Act of 2000, (Assistance with intercountry adoptions under the Hague Intercountry Adoption Convention, maintenance of related records);
- 22 U.S.C. 9001–9011, 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. 9101, 9111–9114, 9121–9125, 9141, International Child Abduction Prevention and Return Act of 2014 (Reporting requirements, prevention measures, and other assistance on international parental child abduction cases);
- 22 U.S.C. 4802 (overseas evacuations);
- 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 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)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1185 (2010) (Travel Control of Citizens)
- 8 U.S.C. 1401-1503 (2010) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality Use of U.S. Passport)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, 2651a, 2705 (2010)
- 22 U.S.C. 2651a (Organization of Department of State), Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 U.S.C. § 3927 (Chief of Mission)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. 6039E (Information Concerning Residence Status

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

☒Yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

  State-05 Overseas Citizens Services Records and Other Overseas Records, September 8, 2016
  State-26 Passport Records, March 24, 2015

☐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: (obtain info from http://infoaccess.state.gov/recordsmgt/recdispsched.asp)
(If the list is long – name only the top level and indicate length of time as variable based on document and detailed info is at the link)

- Schedule number (e.g., (XX-587-XX-XXX)):
- Length of time the information is retained in the system:
- Type of information retained in the system:

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.

NOTE: ACS case records are replicated to the Consular Consolidated Database each day for long-term recordkeeping.

(Supersedes NARA Job No. NI-059-96-30, Item 1 and NARA Job No. NI-084-96-4, Item 1)

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: 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, and information on 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: Transfer to the RSC after the case is deemed closed and no action has taken place for 1 year for transfer to the WNRC. Destroy when 15 years old.

DispAuthNo: N1-059-97-14, item 2

A-15-002-03 **Adoptions Tracking Service (ATS)**

Description: ATS is an electronic information system designed to track, monitor, and report on all adoption cases involving emigration from or immigration to the U.S as mandated by the Intercountry Adoption Act of 2000 (IAA). Activities include monitoring organizations that provide inter-country adoption services, responding to adoption-related inquiries from the public and other interested stakeholders, reporting to Congressional representatives on inter-country adoptions involving U.S. citizens, producing mandatory annual reports to Congress, and communicating with all inter-country adoption stakeholders.

ATS supports the U.S. Central Authority for Inter-country Adoptions (USCA), which has inter-country adoption-related responsibilities involving U.S. citizens. The IAA designated the Department of State as U.S. Central Authority for Inter-country Adoptions under the Hague Adoption Convention. The day-to-day work of the U.S. Central Authority is the responsibility of the Bureau of Consular Affairs, Directorate of Overseas Citizens Services, Office of Children's Issues (CA/OCS/CI).

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.

DispAuthNo: N1-059-09-09, item 1

A-13-001-01a(1) **Passport Case Files - Passport and Citizenship Case Files, 1925-1970.**

Description: a. Case files containing one or more of the following types of records: passport applications; Reports of Birth of American Citizens Abroad; Certificates of Witness to Marriage; Applications for Amendment or Extension of Passport; Certificates of Loss of Nationality; and other supporting forms, documents and correspondence pertaining to each case.

(1) Reports of Birth of American Citizens Abroad, Certificates of Witness to Marriage, Certificates of Loss of Nationality, and Oaths of Repatriation.

Disposition: Permanent. Transfer to the National Archives when 50 years old.

DispAuthNo: NC1-059-79-12, item 2a

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 US 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?

Executive Order 13478, November 18, 2008.

(c) How is the information collected?

Information is collected from within the CA CAD system boundary. Users (General Public) do not have access to CA CDI systems. All data is transmitted system-to-system only. The purpose of CA CDI is to store much of the data related to ongoing ConsularOne operations.

(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?

As noted above, no data is entered into CA CDI directly. All data in CA CDI is from the CA CAD system as entered by the requestor of service. Accuracy is verified at the point of collection by the CA CAD system which then shares the information with CA CDI.

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

As noted above, no data is entered into CA CDI directly. The information is current and verified at the point of collection by the CA CAD system which then shares the information with CA CDI.

If corrections are needed to information, individuals can make changes via the system of origin (CA CAD).

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

No, the system does not use commercial or publicly available information.

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

This is not applicable because no data is entered into CA CDI directly. The notice is provided at the point of collection for the CA CAD system, in which information is entered. All data contained in the CA CDI system is from the CA CAD system.

(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?

No data is entered into CA CDI directly. As noted above, all data contained in the CA CDI system is from the CA CAD system. Individuals grant consent via the CA CAD system at the point of collection when applying for services.

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

As noted above, all data contained in the CA CDI system is from the CA CAD system. There is no information collected by CA CDI. CDI provides the common technical infrastructure supporting information across systems' storage devices to support consular services operations. The PII items listed in paragraph 3(d) are the minimum necessary to facilitate the administering and delivery of consular services.

5. Use of information.

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

The intended use of the information is to support the electronic facilitation of ongoing ConsularOne operations.

(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 PII is used according to the purpose of storing and maintaining PII to support processing of Consular One services regarding visa, passport, citizen services, pictures, fingerprints, case documents, and photos.

(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?
The system does not analyze the information; CA CDI only **stores** information.

(2) Does the analysis result in new information?
Not applicable, as per above.

(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.

External Sharing: N/A

Internal Sharing:

Information is shared among the Consular One databases.

(b) What information will be shared?

PII listed in 3d of this PIA is shared between the Consular One databases.

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

To provide and validate information to execute Consular One services.

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

Any information shared with the CDI shall support traffic over Secure Socket Layer (SSL) or Transport Layer Security (TLS). It can support both protocols.

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

Internal sharing of PII is database to database with the CAD and Consular One databases. External sharing of CDI information is via the CAD system. CDI does not interface with external systems. Communications will be secured using Secure Socket Layer (SSL) and Transport Layer Security (TLS) for the internal sharing of information.

(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 non-authorized parties
b. Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other.

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.

These risks for accidental and deliberate disclosures are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, 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 Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

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

For CA CDI, this is not applicable because no data is entered into CA CDI directly. As noted above, all data stored in CA CDI is from CA CAD. Individual users do not have access to the system. If corrections are needed to information, individuals can make changes via the system of origin (CA CAD).

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐Yes ☒No

As noted above, all data stored in CA CDI is from the CAD system. Individual users do not have access to the CDI system. Nor is data collected from applicants by the CDI system. If corrections are needed to information, individuals can make changes via the system of origin (CA CAD).

If no, explain why not.

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

CDI does not collect information from individuals. The information maintained in CDI is from the CAD system. Procedures are provided at the point of collection in CAD to correct records:

- The STATE-26 Passport Records SORN and STATE-05, Overseas Citizens Services Records and Other Overseas Records SORN.

- The system of origin where services are being requested in the form of a privacy act statement.

- Link to the privacy policy on the Department of State website

Each method contains information on how to amend records and who/what office to get in touch with as well as providing contact information.

8. Security Controls

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

CA CDI is secured within the Department of State databases that Data Engineering and Data management (DEDM) manages in the Enterprise Server Operations Center (ESOC) West 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.

The information is further secured by limiting internal access to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties. Access to the system is secured as follows: All administrative accounts for the system must be approved by the both Government Task Manager (GTM) and Consular Affairs Information Systems Security Officer (CA ISSO).

CA Systems are configured according the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute for Science and Technology, NIST Special Publication 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.

(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.

Internal/OpenNet users:

To access the system, persons must be authorized users of the Department of State's unclassified network OpenNet, which requires a background investigation and an application approved by the supervisor. Each authorized user must sign 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 and Personal Identification Number (PIV/CAC and PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities; in addition to requiring 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 (including managers) to ensure it correlates to the user's particular job function and level of clearance.

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

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with the Bureau of Diplomatic Security (DS) 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, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

Boundary protection devices ensure that all external incoming connections are filtered for appropriate approved protocols, and routed specifically to authorized DMZ enclaves and Devices which have been approved by both Diplomatic Security (DS) Information Assurance (IA) and Operations. The boundary protection devices in the DMZ have restricted ports and protocol policy that is enforced by the Firewall devices and router interfaces.

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 DS Security Configuration Guides, auditing is 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 and to dynamically audit retrieval access to designated critical data.

Operating System (OS)-Level auditing is set in accordance with the DS Security Configuration Guide. 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 logs 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 security training, with a privacy component, is required for all authorized users including security training and regular refreshment training. Each user must complete the Cyber Security Awareness Training annually and complete privacy training entitled "Protecting Personally Identifiable Information (PA459)". The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users to acknowledge (electronically) and agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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 Special Publication 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. 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 at unauthorized access. 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?

The security measures listed above were implemented to secure the PII in the system. 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. The security measures are in place to minimize that risk, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information.

9. Data Access

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

System Administrators/Database Administrators: The System and Database Administrators include both government employees and contractors. They are responsible for the daily maintenance, upgrades, patch/hot fixes to applications, backups, and database configurations.

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

Access is determined based on requests which are approved by the supervisor. Access is role-based and the user is granted only the role(s) required to perform officially assigned duties. All administrative accounts for the system must be approved by the both Government Task Manager (GTM) and Consular Affairs Information Systems Security Officer (CA ISSO).

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

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

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

Access to the system is limited to administrative users only in accordance with their assigned roles and responsibilities. Separation of duties and least privilege is employed

and users have access to only the data that the supervisor approves to perform official duties.

(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

-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.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN).