PRIVACY IMPACT ASSESSMENT

ConsularOne Applications and Data (CA CAD)

1. Contact Information

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

2. System Information

(a) **Name of system:** ConsularOne Applications and Data

(b) **Bureau:** Consular Affairs (CA)

(c) **System acronym:** CA CAD

(d) **iMatrix Asset ID Number:** 253139

(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):**

No modification

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 – in routing for approval

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

The system is currently undergoing its initial Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO). CA CAD is expected to receive an ATO in Summer 2018.

(c) Describe the purpose of the system:

ConsularOne Application Data (CA CAD)

The purpose of ConsularOne Applications and Data (CA CAD) is to function as a logical boundary that includes any customized/developed software, “glue” code, configuration files, database instances, schema, and dictionaries that are part of ConsularOne.

ConsularOne Applications and Data (CA CAD) will eventually cover all of ConsularOne capabilities for citizens and non-citizens to request passport, visa, and overseas citizen services from Consular Affairs. ConsularOne Applications and Data will also be the system that Consular Affairs end users/employees use to conduct their work, including adjudicating travel documents, providing U.S. citizens services overseas, as well as conducting budget planning, execution, and contract functions.

Currently, The CA CAD system includes the following services addressed herein:

- MyTravelGov Account Management Service
- Electronic Application for Consular Report of Birth Aboard, Department of State Form 2029, Electronic Consular Report of Birth Abroad (DS-2029 eCRBA,)

Service: MyTravelGov Account Management – for Public Users (Customers) only

To apply electronically, customers must first register for a MyTravelGov account. To access the account creation page, the customer will access a link on a web site external to this system.

Service: Electronic Consular Report of Birth Abroad (eCRBA)

The eCRBA service is for any person who wishes to electronically complete the DS-2029 Application for Consular Report of Birth Abroad, (https://eforms.state.gov/Forms/ds2029.PDF). The DS-2029 states "A Consular Report of Birth Abroad may be issued for any U.S. citizen child under the age of 18 who was born abroad and who acquired U.S. citizenship at birth. Only the child's parent(s), legal guardian, person acting in loco parentis or the child may apply on the child's behalf. The application generally must be signed before a U.S. consular officer, a consular agent, or, in the case of children born in U.S. military hospitals, a designated military official. A Consular Report of Birth Abroad is proof of U.S. citizenship; however, it does not take the place of a passport for travel purposes."

The Consular Report of Birth Abroad (CRBA) is a formal document (DS-2029) certifying the acquisition of U.S. citizenship or nationality at birth of a person born abroad to a U.S. citizen parent or parents. The purpose of issuing a CRBA is to provide a record of the acquisition of citizenship by a person born in a foreign state that the citizen can use throughout life.

(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 of the DS-2029 Application for Consular Report of Birth Abroad (https://eforms.state.gov/Forms/ds2029.PDF). It includes information about the applicant as well as the parents or guardians of the application. General PII categories include:

- Names of individuals
- Birthdates of individuals
- Financial account numbers of individuals
- Social Security numbers
- Phone number(s) of individuals
- Personal address
- E-mail address (es) of individuals
- Images or Biometric IDs
- Substantive individual medical information
- Substantive individual financial information
- Substantive individual family information
- Substantive individual 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)

(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-26 Passport Records 24Mar2015
STATE-05 Overseas Citizens Services Records and Other Overseas Records 8Sep2016

☐No, explain how the information is retrieved without a personal identifier.
Enter Text if applicable

(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 9397, November 22, 1943; Executive Order 13478, November 18, 2008.

(c) How is the information collected?

Data is collected when Public users apply for a Consular Report of Birth Abroad using the system. The request begins with the public users filling out the application for a CRBA (DS-2029) and submitting it electronically. The system guides the user to provide only the required information for each applicant.

(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?

The accuracy of the application information is the responsibility of the Public users. Quality checks (to include completeness and accuracy) are conducted against the submitted documentation at every stage and administrative policies minimize instances of inaccurate data.

Public users upload supporting documents required for a CRBA application, including but not limited to the following:

- Affidavit of birth
- Child's birth certificate
- Proof of citizenship
- Death certificate
- Divorce decree
- Proof of identity
- Marriage certificate

These documents may be used by internal users to determine if information is accurate.

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

During the adjudication process of the CRBA application, information is kept current by Internal users who aid in the decision making process, such as face-to-face interviews, checking against uploaded supporting justification and via correspondence. After a case is completed, information is not changed as it is important for the case to preserve the information reviewed at the time of the decision.

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

The system does not use information from commercial sources or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes, the Department of State's Privacy Act Statement (PAS) is clearly displayed at the collection point for the DS 2029 and applicants must click to certify that they have read the PAS before being allowed to proceed to the rest of the application.

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

Before starting the application process, the Public user is presented with the Privacy Act statement and must check a box indicating it has been read. The applicant is made aware by the PAS that failure to provide information requested may result in the denial of a service that they are seeking to acquire.

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

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

The PII items listed in Question 3d of this PIA are the minimum necessary to fully adjudicate a request for a CRBA as documented in the DS-2029 form.

5. Use of information

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

The information will be used to certify the acquisition of U.S. citizenship or nationality at birth of a person born abroad to a U.S. citizen parent or parents.

(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 CAD system's stated purpose to allow citizens and non-citizens to request passport, visa, and overseas citizen services from Consular Affairs.

(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?

Internal users analyze the data generated by the system to determine if the applicant qualifies for a CRBA through interviews with the parent(s)/guardian(s) and other parties based on the information submitted on the application.

(2) Does the analysis result in new information?

Yes, new information is derived from the compilation of the information collected. Information in various other sources is brought together as a compiled record in the system.

(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.

Enterprise Payment Service (Internal)
The system shares information with Enterprise Payment Service (EPS) to support the payment process.

Pay.gov (External)
The system shares information with Pay.gov (a service of the Department of the Treasury) to enable online payments.

Google.com/reCAPTCHA (External)
The system shares information with Google.com as a user must pass a reCAPTCHA test before completing important steps in the application process (e.g. creating an account).

(b) What information will be shared?

EPS
The fee amount and status of the payment is shared with EPS.

Pay.gov
The name and address of the main parent as well as the fee amount is shared with Pay.gov to pre-load into Pay.gov's payment web page.

Google.com/reCAPTCHA
The Public User's IP address and results of the reCATPCHA test are shared with Google.com. A link to the Google.com privacy policy is available on the reCAPTCHA web page.

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

EPS
EPS is a central CA service that facilitates communication with Pay.gov for multiple systems.

Pay.gov
The purpose for sharing this information is to ease the processing of fee payments for a Public user.

Google.com/reCAPTCHA

The purpose is to improve the ability of the reCAPTCHA service to detect bots.

(d) The information to be shared is transmitted or disclosed by what methods?
Information is transmitted both internally and externally via secure socket layers (SSL) over hypertext transfer protocol (HTTP).

(e) What safeguards are in place for each internal or external sharing arrangement?
Communications will be secured using transport and message level security.

(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: Accidental disclosures 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 whether the motivation was monetary, personal or other.

These risks 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, need-to-know, and clearance level.

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

- All communications shared with external agencies are encrypted as per the Department of State Bureau of Diplomatic Security Configuration Guides' security policies and procedures.

7. Redress and Notification

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

All applicants can follow instructions for gaining access as stated in SORNs State-26 and State-05. They may also visit the Department of State public site and/or the Department of State FOIA web site for information on how to obtain access by contacting the listed offices by phone or by mail.

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

☒Yes ☐No

If yes, explain the procedures.

U.S persons can request amendment of records about themselves that are not accurate, timely, relevant, or complete through a request for amendment to A/GIS/IPS. The individual must specify that he or she wishes the records of the Bureau of Consular Affairs to be checked. This information and additional guidance are available in the published SORNs.

If no, explain why not.

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

Individuals are notified of the procedures to correct records in these systems by a variety of methods:

1. Following directions in the published SORN
2. Following Department of State FOIA website directions
3. Being notified by an adjudicator that a correction is needed

Each method contains information on how to amend records and who/what office to communicate with as well as contact information.

8. Security Controls

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

The system is secured within Department of State networks 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 their official duties. Access to databases is further protected with additional access controls.

(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.

Personnel must be authorized users of the Department of State's unclassified network (OpenNet), which requires a background investigation and approval by the supervisor and Information System Security Officer (ISSO). 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 to OpenNet.

The system will utilize Role Based Access Control. The system has a defined list or Siebel responsibilities (similar to roles) that can be assigned to a user. The responsibilities determine access to functions and data in the system. The responsibilities are based on the standard job functions of staff.

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

The CA ISSO, in conjunction with the CA Security team, periodically scan and monitor information systems for compliance with 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.

Platform software will be used for security monitoring of eCRBA to prevent misuse of information. The provided services allow authorized users to search, analyze, and see data gathered from websites, applications, devices, etc. that comprise CA's infrastructure, to include eCRBA, to detect and respond to cybersecurity incidents or suspected cyber incidents in real time.

(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. Each user must complete the Cyber Security Awareness Training annually and pass the Privacy Act PA-459 course entitled, "Protecting Personally Identifiable Information". The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they 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 National Institute for Science and Technology (NIST) Special Publication 800-53 and Department of State Bureau of Diplomatic Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Boundary and information integrity protection including, but not limited to, firewalls, antivirus software, and access controls, are in use. System auditing procedures are implemented by the CA ISSO Security team to monitor and record deviances from required security controls.

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

The security measures listed above were implemented to secure the data in the system because PII processed by CAD/eCRBA is sensitive. 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?

There are four types of users: Public users (Customers), Internal/OpenNet Users, System Administrators (OpenNet), and Database Administrators (OpenNet).

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

Internal Users (OpenNet)

A request to access the system is made by email to the Department of State Bureau of Consular Affairs Overseas Citizen Services Directorate (CA/OCS) Government staff. If appropriate, staff will approve access to the system and provide a list of responsibilities in the system to be assigned to each user.

Public Users (Customers)

For public users, access to the system is available via the Internet. All public users have access to an unauthenticated area of the system containing general information. To proceed to the authenticated area, public users must create an account. Once the account is validated via an emailed uniform resource locator (URL) which expires in 24 hours, each public user can access the authenticated area which permits application submission. Public users can only access their own applications in the authenticated area.

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

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

No, all users will not have access to all data in the system. User access is based on the definition of the roles assigned to the user. The system will utilize Role Based Access Control (RBAC) as a means to regulate who has access to functions within the application.

(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 access 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).