PRIVACY IMPACT ASSESSMENT

Electronic Consular Report of Birth Abroad

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: August 2022
(b) Name of System: Electronic Consular Report of Birth Abroad
(c) System acronym: eCRBA
(d) Bureau: Consular Affairs (CA)
(e) iMatrix Asset ID Number: 276686
(f) Child systems (if applicable) 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:

eCRBA is one of the four ConsularOne business areas that provide online web-based capabilities for local and overseas Consular Report of Birth Abroad (CRBA) services and payments. The eCRBA solution includes an end-to-end process flow that begins with filling out and submitting the Department of State Form "Application for Consular Report of Birth Abroad" (CRBA application, Form DS-2029), electronically via the web and, if approved, the applicant receives a Consular Report of Birth Abroad (CRBA, Form FS-240).

A CRBA, FS-240, is a formal document certifying the acquisition of U.S. citizenship or nationality at birth of a person born abroad to a U.S. citizen parent or parents. A Consular Report of Birth Abroad is proof of U.S. citizenship and, unlike a U.S. passport, never expires.

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

The eCRBA application collects the following PII for the person born abroad and/or their parents:

- Name
- Date of birth
- Place of birth
- Citizenship
- Phone number
- Mailing Address
- Personal e-mail address
- Social Security number
- Passport number
- Financial information
- Personnel/employment
- Family information
- Maiden name
- Previous legal name
- Biometric IDs
- Photo
- Medical information
- Other identity documents, e.g., driver's license, marriage certificate information

Non-Citizen PII only:

- National ID PII collected on non-U.S. citizens only.

Consular Staff PII:

The eCRBA application collects the name of the consular officer and the post processing the application. This information is collected for business purposes only and the remainder of this PIA will focus on the information collected as part of the CRBA application.

(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)
8 U.S.C 1401 (Nationals and Citizens of the United States at Birth
8 U.S.C. 1408 (Nationals but Not Citizens of the United States at Birth)

8 U.S.C. 1409 (Children Born Out of Wedlock)
22 U.S.C. 2651a (Organization of Department of State)
22 U.S.C. 2705 (Documentation of Citizenship)
22 C.F.R. Part 50 (Nationality Procedures)

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

☒Yes, provide:

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

SORN Name and Number: Passport Records, STATE-26
SORN publication date: 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 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-13-001-15a
Disposition Authority Number: N1-059-04-02, item 15a
Length of time the information is retained in the system: Permanent. Transfer to Washington National Records Center (WNRC) when digitally imaged. Transfer to the national Archives when 25 years old.
Type of information retained in the system:
Consists of Reports of Birth of American Citizens Abroad and supporting forms, documents and correspondence pertaining to each case; Certificates of Witness to Marriage; Certificate of Loss of Nationality; Oaths of Repatriation and Reports of Death, 1925-present. Note: Prior to 1971, some records were attached to the passport applications. (Since 1971 they are maintained in a separate file, alphabetically organized, to be kept in 10- year blocks.)

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 ☐N/A

- If yes, under what authorization?

22 CFR § 50.5 Application for registration of birth abroad.

(d) How is the PII collected?

The information in paragraph 3(d) above is collected online from the entrants using the electronic Consular Report of Birth Abroad (eCRBA) web entry. The request begins with the public users filling out the application for a Consular Report of Birth Abroad (CRBA) Form DS-2029 and submitting it electronically. The system guides the user to provide only the required information for each applicant.

(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.

eCRBA is hosted on the Federal Risk and Authorization Program (FEDRAMP) approved CA Salesforce Cloud infrastructure. There is also Department owned equipment supporting the eCRBA system.

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

The accuracy of the application information is validated during the interview phase. Also, quality checks (to include completeness and accuracy) are conducted against the submitted supporting documentation at every stage, in addition to administrative policies that 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
- Proof of identity
- Marriage certificate
- Divorce decree
- Death certificate

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

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

During the adjudication of the CRBA application, information is kept current by internal Consular Affairs personnel who aid in the decision-making process, such as face-to-face interviews, checking against uploaded supporting documents 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?

No, eCRBA does not use commercial sources of information nor is the information publicly available.

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

The PII items listed in Question 3(d) are the minimum necessary to perform the actions required by the eCRBA system. 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 considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the eCRBA system to perform the intended function of adjudicating a CRBA application.

5. Use of information

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

The eCRBA PII will be used to 1) verify and certify the acquisition of U.S. citizenship or nationality at birth of a person born abroad to a U.S. citizen parent or parents; 2) to issue a Consular Report of Birth Abroad to such person for use as proof of U.S. citizenship; and 3) to acquire payment for the CA services.

(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 use of the PII data within the eCRBA system is utilized for the purposes for which the system was designed: to validate the citizenship and identity of parent(s) of a person born abroad to determine the person's identity and whether the person acquired U.S. citizenship at birth before issuing a Consular Report of Birth Abroad to them.

(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 (Department), but external to the owning organization (referred to as "bureau" at the Department). 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 eCRBA will be shared internally with the ConsularOne Platform and Infrastructure CA (CPI), Electronic Payment System (EPS), Consular Consolidated Database, (CCD), and Consular Lookout and Support System

(CLASS), Passport Information Electronic Records System (PIERS), Front End Processor (FEP), ConsularOne Database Infrastructure (CDI), and Accountable Items (AI).

External: eCRBA does not share information directly with external agencies. However, eCBRA information is shared with EPS to process payments for consular services via Pay.gov.

(b) What information will be shared?

Internal: All the PII in paragraph 3(d) is shared with the CA systems listed in paragraph 6(a), except for EPS. Only the name, address and financial information are shared with EPS.

External: N/A

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

Internal: The Information in paragraph 3(d) is shared with CA systems in paragraph 6(a) to authenticate the eCRBA information to process the eCRBA application, and to process payments for the CA services.

External: N/A

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

Information is transmitted via secure socket layers (SSL) over hypertext transfer protocol secure (HTTPS).

Internal: All eCRBA information is shared internally database to database and is encrypted using SecureSocket Layer (SSL) and transport layer security (TLS).

External: N/A

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

Internal: The eCRBA system safeguards entail secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS)) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior outlined in the security controls for each major application, including eCRBA. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In addition, Department employees must have a Personal Identity Verification/Personal Identification Number (PIV/PIN), as well as a separate password to access eCRBA data.

External: N/A

7. Redress and Notification

(a) Is notice provided to the record subject 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 eCRBA application (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.

(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?

Before starting the application process, the public user is presented with the Privacy Act statement (PAS) 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 record subjects not allowed to provide consent?

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

All applicants can follow instructions for gaining access as stated in SORNs STATE-05 and STATE-26. The above SORNs provide information and organization points of contact regarding questions and procedures to access information.

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

☒Yes ☐No

If yes, explain the procedures.

All applicants can follow instructions for gaining access as stated in SORNs STATE-05 and STATE-26. Individuals can also update information during their interview process with the consular officer.

If no, explain why not.

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

Individuals can correct their information by following directions in the published SORNs STATE-05 and STATE-26 and during the interview process with the consular officer. The Privacy Act Statement provided to the applicants at the point of collection point to STATE-05 and STATE-26, which address the necessary procedures record subjects must follow to correct their information.

8. Security Controls

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

The eCRBA system is secured within the Department of State intranet which mitigates risk factors through 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 eCRBA information is further protected with additional access controls set at the database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer.

The eCRBA system is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable 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. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need to perform official duties. Access to the eCRBA system is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor.

(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).

Access to the eCRBA system is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. Department of State eCRBA users, Salesforce administrators, system administrators, database administrators and public users have access to eCRBA based on prescribed roles to conduct required business to support the management and execution of the eCRBA program.

Click here to enter text.

(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.

Separation of duties and least privilege access are employed; users have access to only the data that the supervisor and local Information System Security Officers (ISSOs)

approve to perform official duties. Access is role-based, and the user is granted only the role(s) required to perform officially assigned duties.

Least privileges are restrictive rights/privileges or access users need for the performance of specified tasks. The Department of State ensures through least privileges principles 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) necessary to perform their job duties. Users are uniquely identified and authenticated before accessing PII.

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

Access to data of user roles listed in 8(b) is based on the position, role, and need to perform officially assigned duties as described. Supervisors and the local ISSO must approve access to eCRBA based on the specific role and the level of security of personnel. Once personnel leave the project, their access to eCRBA is terminated.

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

The eCRBA CA System Manager and the local CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides, conduct annual control assessments (ACA) to ensure systems 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 applications for changes to the Department of State mandated security controls. Access control lists on Open-Net servers and devices along with Department of State Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures.

In accordance with Department of State 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.

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

☒Yes ☐No

The eCRBA System Security Plan (SSP) contains the procedures, controls, and responsibilities regarding access to data in the system.

(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.