PRIVACY IMPACT ASSESSMENT

Consular Electronic Application Center (CEAC)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: 5/2021
(b) Name of system: Consular Electronic Application Center
(c) System acronym: CEAC
(d) Bureau: Consular Affairs
(e) iMatrix Asset ID Number: 2712
(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:

The Consular Electronic Application Center (CEAC) supports an internet-based, full-service application service center where applicants for nonimmigrant visa or immigrant visa services may complete and submit an application. Immigrant visa applicants can make payments and attach documents to their case; nonimmigrant visa applicants can attach photos. Both nonimmigrant and immigrant visa applicants can track their application status. The system is designed, developed, and implemented to be used by the public, posts, and the Bureau of Consular Affairs' users in several phases of the application process.

The following CEAC web applications are currently accessible via the internet for use by public users:

CEAC Landing Page: Visa applicants can access a splash page that allows the applicant to navigate to the various CEAC forms without typing in a specific URL for a specific form.

General Nonimmigrant Visa (GENNIV) (Nonimmigrant visa applicants):
The GENNIV application data collection component, also referred to as the DS-160 (Online Nonimmigrant Visa Application form), allows users to complete and electronically submit a DS-160 application to posts worldwide. Nonimmigrant applicants provide U.S. point of contact information via Form DS-160.

A-Class/G-Class Non Immigrant Visa/North Atlantic Treaty Organization (AGNATO) (Nonimmigrant application customers): The AGNATO application data collection component, also referred to as the DS-1648 (Application for A, G, or NATO Visa form), allows users to complete and electronically submit a DS-1648 application online.

Consular Tracking (CTRAC) (Immigrant visa applicants): CTRAC is a fee invoice component that allows immigrant visa applicants to view their consular fee invoices and select the unpaid fees which they would like to pay. Once payment is initiated, the component presents the user with a receipt and allows the user to print and/or email the receipt to one or more specified recipients. CTRAC collects immigrant data only.

Payment Processing System (PPS) (Immigrant visa applicants): The PPS payment screen allows users to input the specific information required by Pay.gov to make a payment for services. Information includes the payer's name, email address, bank routing number, account number, check type, and account type. After entering this information, the system submits the payment online to Pay.gov via the Electronic Payment System (EPS). Bank account information, as listed above, is not retained or stored by the system.

Remote Data Collection (RDC) (Immigrant and nonimmigrant visa applicants):
The RDC component is used to collect biometric information (i.e. fingerprints, photos) of applicants who have completed any one of the CEAC applications requiring the biometric information, so they can be sent to posts for additional processing. RDC collects immigrant and nonimmigrant data.

Image Quality Over the Web (IQOTW) (Nonimmigrant visa applicants): As part of the electronic submission of NIV applications, applicants are asked to provide an electronic copy of a facial photo for use in the travel document. The photo must meet quality requirements for photo submission. The IQOTW component provides photo submission and quality assessment functionality of the facial photo images submitted by applicants.

CEAC Visa Status Check (Immigrant and nonimmigrant visa applicants): CEAC status check is used by applicants worldwide to check the status of their nonimmigrant visa (NIV) or immigrant visa (IVO) cases. No U.S. citizen data is involved in the CEAC status check.

Electronic Immigrant Visa Application forms (IV App) (Immigrant and diversity visa applicants): The IV applicant uses the IV App to complete, sign and submit the DS-260 form online for submission to Department posts. The IV App data collection component is accessible through CEAC. The IV App component also referred to as the DS-260 form: Immigrant Visa and Alien Registration Application. The DS-260 form collects immigrant data and information on the IV applicant's petitioner (i.e., a U.S. person).

Electronic Agent of Choice Application (IV Agent) (Immigrant visa applicants): The IV Agent data collection component is accessible through CEAC. The IV Agent component, also referred to as the DS-261 form: Choice of Address and Agent for immigrant visa applicants, allows IV applicants to complete, sign, and submit the (DS-261) form online through the internet to Department posts for processing. The DS-261 form is the online version of DS -261 (Choice of Address and Agent form) and collects immigrant data and data on U.S. persons, if the applicant's agent is a U.S. person.

CEAC IV Summary (Immigrant visa applicant): The internet-based IV application uses the CEAC IV Summary to sign into CEAC, to view dynamic instructional text, to access the DS-261 and DS-260 forms and to access the fee payment component (PPS).

CEAC Web Application Reports: CEAC provides various reporting capabilities to manage the visa application process that are accessible only by Consular Consolidated Database (CCD) or NVC users. The reporting application displays the data collected from AGNATO, GENNIV, IV Agent, and IV Application. CEAC web may contain information about immigrant, nonimmigrants, and U.S. persons, if information is provided by the applicant.

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

CEAC primarily collects data on foreign nationals as part of the U.S. visa application process.

PII may also be provided on U.S. Citizens, which can consist of: name, address, phone number, social security number, email address, petitioner company/work information, and affiliation to applicant.

Immigrant/nonimmigrant PII includes:
Name
Birth Date
Birthplace
Gender
Present Country of Residence
Prior Country of Residence
Passport Number
Alien (Case) information
Fingerprint
Photos/Biometric ID
Home/Mailing Address
Phone numbers
Email address
Financial information
Banking information
Marital Status
Employer Name/Information
Social media handles
Driver's License Information (if applicant has held a U.S. Driver's License)
Marriage Certificate
Financial Documents (i.e., tax filing)
Birth Certificate
Criminal Incarceration
Individual family information
Individual personnel information
Medical information

The information provided by the visa applicant is considered a visa record subject to the confidentiality provisions of section 222(f) of the Immigration and Nationality Act (INA).

Because visa applicants themselves are not U.S. persons (that is, U.S. citizens or lawful permanent residents (LPRs)), they are not covered by the provisions of the Privacy Act 1974.

(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. 1151-1363 (Title II of the Immigration and Nationality Act of 1952, as amended)

8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
22 U.S.C. 2651a (Organization of Department of State)
22 U.S.C. § 3927 (Chief of Mission)
26 U.S.C. 6039E (Information Concerning Residence Status)
22 C.F.R. Parts 40-42, and 46 (Visas)

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

☒Yes, provide:
SORN Name and Number: Visa Records, STATE-39
SORN publication date: June 15, 2018

☐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-14-001-02a Visa Case Files on Individual Aliens**
  Disposition Authority Number: N1-059-86-2, item 1a
  Length of time the information is retained in the system: Destroy 6 months after issuance.
  Type of information retained in the system:
  Case files on individual aliens issued an immigrant visa.

- **Schedule number: A-14-001-02b Visa Case Files on Individual Aliens**
  Disposition Authority Number: N1-059-86-2, item 2b
  Length of time the information is retained in the system: Destroy 1 year after issuance.
  Type of information retained in the system:
  Case files on individual aliens issued a non-immigrant visa.

- **Schedule number: A-14-001-02c(1)(a) Visa Case Files on Individual Aliens**
  Disposition Authority Number: N1-059-91-28-2, item 1c(1)(a)
  Length of time the information is retained in the system: Retain until alien is 90 years of age or older, provide there has been no visa activity for the past 10 years, at which time destroy. (ref. NC1-59-86-2, item 3c1(a) and c1(c)).

Type of information retained in the system:
Case files on individual aliens refused a visa.
(1) Cases of living visa applicants.
(a) Cases of applicants refused or presumed ineligible on the basis of Sections 212(a) (1), (2), (3), (4), (5), (9), (10), (12), (13), (19), (22), (23), (27), (28), (29), (31), and (34) of the Immigration and Nationality Act.

- **Schedule number A-14-001-02c(1)(b) Visa Case Files on Individual Aliens**
  Disposition Authority Number: N1-059-91-17, item 1
  Length of time the information is retained in the system: Retain until alien is 100 years of age, then destroy**.** (ref. NC1-59-86-2, item 2c1(b))
  Type of information retained in the system:
  Cases of applicants refused or presumed ineligible under Section 212(a)(33) of the Immigration and Nationality Act.

- **Schedule number: A-14-001-02c(1)(c) Visa Case Files on Individual Aliens**
  Disposition Authority Number: N1-059-86-2, item 6d
  Length of time the information is retained in the system: Destroy 2 years after date of refusal.
  Type of information retained in the system: Cases of applicants refused or presumed ineligible under Section 212(a)(33) of the Immigration and Nationality Act.
  Case files on individual aliens refused a visa.
  (1) Cases of living visa applicants.
  (c) Cases of applicants refused or presumed ineligible under all other Sections of Section 212(a), (Category II), and Section 212(e) of the Immigration and Nationality Act

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?

26 U.S.C. 6039E (Information Concerning Residence Status)

(d) How is the PII collected?

The information is obtained directly from individuals' applications for nonimmigrant visa or immigrant visa services. The data are submitted via the internet where it is electronically stored within the CEAC database. It is then replicated to the CCD system on OpenNet. A scheduled database procedure pulls the data from the Demilitarized Zone (DMZ) to the OpenNet environment where it is accessed in the CCD by consular officers at post and/or domestic agencies.

(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?

It is the responsibility of the applicant to ensure that the information entered is accurate. Also, CEAC has built-in functionality to perform validation on fields to ensure that data input meets certain criteria. During the interview phase, the staff at posts and/or the Washington Visa Office screen the database records prior to and during the applicant's interview.

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

Yes, the information is current to the maximum extent possible. Information provided by applicants and stored in Department information systems can be amended or revalidated by the applicant during the interview/adjudication process.

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

CEAC does not use commercial information or publicly available information.

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

The PII listed in 3d are the minimum necessary to perform the actions required by this system. Concerns 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.

5. Use of information

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

The information collected by the CEAC visa components is used to determine the eligibility of foreign nationals who apply for a U.S. visa. The CEAC components themselves do not determine the eligibility of applicants who are applying for a U.S. visa, but collect the personal information necessary to complete an online visa application form. The visa issuance process determines the eligibility of the applicant. When an applicant completes the appropriate CEAC form, it is transferred to the local database at post. The Consular officer at post initiates the visa process using the information in the Non-Immigrant Visa (NIV) application or the Immigrant Visa Overseas (IVO) application to adjudicate the applicant's eligibility for a U.S. visa.

(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 PII is used to validate eligibility and to process applications for visa consular services.

(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: CA/CST’s Consular Consolidated Database (CCD); Enterprise Payment System (EPS); Ten Print Live Scan (TPLS); Non-Immigrant Visa (NIV); Immigrant Visa Overseas (IVO); Immigrant Visa Information system (IVIS); Pre IVO Technology (PIVOT).

External: CEAC does not connect/share with external entities. However, CEAC information is shared in the form of reports via the CCD system with the Departments of Homeland Security, Commerce, Defense, Treasury, Energy, and the Federal Bureau of Investigation. This sharing is accounted for in the CCD PIA.

(b) What information will be shared?

Internal: PII in 3d is shared with the CA systems listed in paragraph 6a.

External: N/A

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

Internal: The information is shared internally to validate applicant eligibility, and to process immigrant and nonimmigrant visa applications. Specifically, CCD connects to CEAC for the purpose of production data replication to the NVC, consular posts, and reporting via CEAC Web. The CEAC PPS component connects to EPS to send payment information to Pay.gov to verify payment information is received. The CEAC RDC component interfaces with TPLS to capture the applicant's biometric information in order to verify it. The NIV and IVO applications allow Consular officers to use the information to determine eligibility for a visa. NVC staff reviews CEAC information displays on CEAC Web and updates the IVIS application for visa processing. CEAC IV Application data updates the PIVOT application, which is used by the National Visa Center (NVC) to process immigrant visa cases before transmission to post.

External: N/A

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

Internal: Information is shared database to database by Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information. Electronic files are PIV/PIN or password protected and access is controlled by system managers. Audit trails track and monitor usage and access.

External: N/A

(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. Also, the CEAC web servers reside in the Department's DMZ and the database servers reside on OpenNet and are protected by a firewall.

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. Where applicable, when the collection involves potential PII collected on U.S. citizens, there is a Privacy Act statement displayed on the form.

Non-citizen data is subject to the requirements of the Immigration and Nationality Act (INA)222(f) which are stated on the collection site.

(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?

While applicants can decline to provide PII for use in processing their application, failure to provide the information necessary to process the application may result in the application being rejected.

An applicant voluntarily elects to complete the visa application process, and all associated CEAC forms, payment, and document submission. The forms notify the applicant regarding the type of information to be collected, justification for the collection, routine uses, potential sharing arrangements, data protection measures, and the consequences of not providing the data.

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

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

Applicants can view information submitted online by entering their application ID and answering security questions, or by providing a case ID and invoice ID or principal applicant's DOB and log-in information at the CEAC site. Information submitted on themselves as well as any petitioner (U.S. persons) can be reviewed for accuracy by the applicant during this process.

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

☒Yes ☐No

If yes, explain the procedures.

Visa applicants may change their information at any time prior to final submission of the application to the consulate or embassy. Once the application has been submitted, applicants may make changes by filing a new application with the Department, requesting the Department to unlock or reopen the application for correction and resubmission, or correcting the information during the course of a visa interview.

If no, explain why not.

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

The Department informs applicants on how to correct the information during the course of their visa process. Also, emails are sent to applicants when there are inconsistencies so the applicant can provide correct information. Applicants can also follow procedures outlined in SORN STATE-39.

8. Security Controls

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

CEAC is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Access to CEAC is controlled at the system level with additional access controls at the application level. All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

CEAC is configured according to the State Department Bureau of Diplomatic 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.

(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 CEAC is role-based and the user is granted only the role(s) required to perform officially assigned duties. There are five different types of CEAC user roles:

General public users: The internet-based visa applicants use CEAC to complete, sign, and submit the required visa application forms online.

Database administrators: Database administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix applications, backups and configurations to the database.

System administrators: CEAC administrators include both government employees and contractors. System administrators are responsible for all daily maintenance, backups, and establishing access control lists (ACLs) based on supervisors' approvals of personnel.

Remote data collection (RDC) user: The RDC application is used by contract awarded personnel only to collect the biometric information of immigrant applicants who have completed a CEAC application and need to have their fingerprints and photo captured so that they can be sent to the post for additional processing.

DoS Consular Consolidated Database (CCD) users: Access is provided to CCD users to perform visa and other consular functions.

(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 CEAC is role-based and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Local Information System Security Officers (ISSO) determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function, manager's approval, and level of clearance.

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

Access to the system is role-based and restricted according to approved job responsibilities and requires managerial concurrence.

General public users: Via the internet, CEAC applicants are able to access a page that allows the applicant to navigate to the various Department of State visa application forms. Public users are restricted by the system forms being completed, to see and access only their information.

Database administrators: DBA access is controlled by the use of Access Control Lists (ACLs). The local ISSO is responsible for reviewing and approving the DBA accounts in accordance with the access approved by the supervisor. Database administrators have access to all the information in CEAC.

System administrators: The duties of system administrators require that they be granted system administrator privileges to the respective application servers. System Administrators have access to all the information in CEAC.

Remote data collection (RDC) users: The public key infrastructure (PKI) is used by RDC users, which is assigned, controlled and run by the vendor at each site. Certificates and access are controlled per site (certificate and password is required for each individual user). RDC users only have access to biometric information in CEAC.

DoS Consular Consolidated Database (CCD) users: CCD users can access CEAC via OpenNet to access various CEAC Web reports containing applicant information to view and acquire CEAC reports to perform visa and other consular functions. CCD users have access to all the CEAC Web reports containing applicant information.

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

The CEAC audit service on its servers captures many logs, access attempts, an all actions, exceeding the DoS requirements. Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information in CEAC. 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 CEAC System Security Plan includes information and procedures regarding access to data in CEAC.

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

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.