

## 1. Contact Information

**Department of State Privacy Coordinator**

Margaret P. Grafeld  
Bureau of Administration  
Information Sharing Services  
Office of Information Programs and Services

## 2. System Information

- (a) Date PIA was completed: December 29, 2008
- (b) Name of system: Consular Electronic Application Center
- (c) System acronym: CEAC
- (d) IT Asset Baseline (ITAB) number: 2712
- (e) System description (Briefly describe scope, purpose, and major functions):

The Consular Electronic Application Center (CEAC), which includes the Remote Data Collection (RDC) component, supports an Internet-based, full-service application service center where applicants for a nonimmigrant visa or, in the future, immigrant visa and passport services, may complete and submit an application, make payments, attach photo/biometrics/documents, and track their application status. The system is designed, developed and implemented to be used by the public, posts, and Bureau of Consular Affairs users in several phases.

- (f) Reason for performing PIA:

- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security re-certification

- (g) Explanation of modification (if applicable):

It is anticipated that additional components of CEAC will be implemented during the calendar year 2009. The remaining CEAC Phase I components will include the Online Passport Renewal System (OPRS) for public use. The passport forms will allow the public internet users to apply for passports and passport renewals. The passport application and passport renewal submission will also include a payment capability via a link to the Department of Treasury website, [www.pay.gov](http://www.pay.gov).

Future releases of CEAC will include the following for use by the public:

- Additional immigrant visa application forms for foreigners to supply information for immigrant visa application processing. The first immigrant visa application forms will be the on-line DS-260 and the on-line DS-261. The on-line DS-260 will collect immigrant visa application data through CEAC immigrant visa application (IVAPP) and will include biographic data about the applicant, family members and petitioner. The on-line DS-261 will collect change of address and agent designation information through CEAC IV agent of choice (IVAGENT). The DS-261 will contain name and

## **Privacy Impact Assessment: Consular Electronic Application Center (CEAC)**

address of the applicant and the name of the agent designated to serve as contact for the applicant.

- The Document Submission Component will provide public internet users with the ability to submit imaged documents with their application form. This component will provide the applicant with the ability to categorize their document, such as bank statements, court records, etc.
- The Online Passport Renewal System (OPRS) component of the Consular Electronic Application Center Portal (CEACP), Consular Electronic Application Center (CEAC) will provide American Citizens (Amcit) Internet public users with the ability to submit electronic passport application and renewal forms. OPRS will allow a user to not only electronically sign and submit their form directly to DoS, but will also allow them to pay for their passport application or renewal via [www.pay.gov](http://www.pay.gov) plus permit the electronic submission of a passport photo via a link to image Quality Over the Web (QOTW) component.

(h) Date of previous PIA (if applicable): May 2008

### **3. Characterization of the Information**

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

#### **a. What elements of PII are collected and maintained by the system? What are the sources of the information?**

*With respect to applicants for U.S. visas:* CEAC primarily collects data on foreign nationals as part of the U.S. visa application process. As such, the information provided by the visa applicant is considered a visa record subject to confidentiality requirements under 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 legal permanent residents), they are not covered by the provisions of the Privacy Act of 1974 and the E-Government Act of 2002. However, the visa portion of CEAC records may include PII about persons associated with the visa applicant who are U.S. citizens or legal permanent residents. This PII data may include the following: U.S. sponsor/petitioner; U.S. employer; names, telephone numbers, email addresses or other contact information of a U.S. person.

*With respect to applicants for U.S. passports:* CEAC primarily collects information on U.S. citizens. An applicant voluntarily elects to complete passport applications. All forms at the time of data collection contain a Privacy Statement, which indicates what information is collected, why, for what purpose the information will be routinely used, who the information will be shared with, and the consequences of not providing the data requested such as applicants social security number.

#### **b. How is the information collected?**

Visas: Visa applicants applying for services are the primary source of the information; they enter information through the on-line visa application components such as CEAC GENNIV (DS-160), A/G/NATO (DS-1648), which is an Internet-based, full-service application service

## ***Privacy Impact Assessment: Consular Electronic Application Center (CEAC)***

center whereby applicants for visa and in the future passport services, complete and submit an application. Some US Person data (name, address, phone number and email is collected on the visa applications such as petitioner, US employer, or US contact information as applicable to the type of visa for which the applicant is applying

U.S. Passport: U.S. citizen data will be collected in the process of providing passport services. For example, citizen relative information, contact information, etc, may be collected for their online passport application. U.S. citizens' Passport data will be collected via the scanning capabilities offered through the CEAC component RDC.

Other documents: Documents originated by other agencies and/or foreign local authorities such as proof of birth place, address, other identifying documents, birth documents, etc., that are provided to DoS are done through the document attachment capability.

### **c. Why is the information collected and maintained?**

The information is collected to determine the eligibility of persons who applied or are applying for US visas or in the future, passports.

### **d. How will the information be checked for accuracy?**

Accuracy of the information on a visa or passport application is the responsibility of the applicant and CEAC users. Ensuring the accuracy of the information on an application and the submission of citizenship evidence is the responsibility of the passport applicant. Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data.

### **e. What specific legal authorities, arrangements, and/or agreements define the collection of information?**

- The Immigration and Nationality Act (INA), 8 U.S.C. 1202, Section 222(f)
- U.S.A. PATRIOT Act
- Illegal Immigration Reform and Immigration Responsibility Act of 1996
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P..L. 107 -173)
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)

### **f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated?**

The CEAC system collects the minimum amount of information required to satisfy the statutory purposes of the system and the mission of the bureau. All of the information that is collected by CEAC is required to issue a passport or visa.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

## **4. Uses of the Information**

## ***Privacy Impact Assessment: Consular Electronic Application Center (CEAC)***

### **a. Describe all uses of the information.**

The Consular Electronic Application Center (CEAC) which includes the Remote Data Collection (RDC) component is developed to support an Internet-based, full-service application service center whereby applicants for a nonimmigrant visa or, in the future, immigrant visa and passport services, complete and submit an application, and, if needed, make payments, attach photo/ biometrics/documents, and check application status.

The information collected by the Consular Electronic Application Center is used by the Bureau of Consular Affairs Visa and Passport Offices to monitor the status of services provided.

With respect to visa applications: to create visa cases, to record and track visa applicant requests and appointments, and provide the status of an application via knowledge based shared data (case ID and petitioner information or case ID and applicant ID or case ID and applicant name). Data is routinely retrieved using case ID and petitioner information, case ID and applicant ID or case ID and applicant name in order to provide visa services.

With respect to passport applications: for the initial creation of U.S. citizen passport applications and passport renewals, to record and track passport applicant request, appointments and to provide the status of an application will be retrieved using the applicants SSN, DOB, Full Name, etc., from the Travel Document Issuance System (TDIS).

### **b. What types of methods are used to analyze the data? What new information may be produced?**

CEAC conducts error checking to ensure that all required fields are complete and the application is suitable for transmission. It also captures information for management purposes such as remarks and audit data.

### **c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.**

Visa applicant data such as photo, fingerprint, proof of birth, birth place, other identifying documents, existing passports provided by visa applicant and/or Foreign Local Authorities is used to effectively identify the visa applicant outside of the CEAC.

Passport applicant data such as photo, proof of birth, birth place, SSN, existing passport number and/or drivers' license number provided by passport applicant will be used to effectively identify the passport applicants for passport issuance or renewal.

### **d. Is the system a contractor used and owned system?**

CEAC is a government owned system. The CEAC RDC component is supported by contract employees, some of whom are located at contractor-owned facilities. Contractors are also involved with the design and development of the CEAC system and will be involved with the maintenance of the system. Privacy Act information clauses have been inserted into all Statements of Work and became part of the signed contract; this also includes other regulatory measures. Each contractor employee is required to attend mandatory briefings that cover the handling of classified and other such information prior to working on the task.

## ***Privacy Impact Assessment: Consular Electronic Application Center (CEAC)***

All employees and contractors must pass annual computer security briefing and Privacy Act briefings from DOS and/or the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

### **e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.**

User access to information is restricted according to job responsibilities and requires managerial level approvals. Users who utilize and have access to CEAC is restricted to cleared, authorized Department of State direct hire or contractor personnel. CEAC enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated.

Contractors involved in the U.S. passport fulfillment process (i.e., data entry, scanning, or correction of records or the printing and mailing of passports) are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of CEAC hardware or software must have at least a Secret-level security clearance.

## **5. Retention**

### **a. How long is information retained?**

Record retention varies depending upon the types of records. The disposition schedule for records is contained in the Department's Records Disposition Schedule for American Citizens, 13: Passport Records and Chapter 15: Overseas Citizens Services Records; and for immigrant visas, Chapter 14: Visa Records. All have various disposition timeframes depending on the data retained.

The DoS Records Disposition Schedule website is available at <http://foia.state.gov/records.asp>.

There are various procedures for the disposition of the visa and passport data at the end of the various retention timeframes based upon the data in the record/file. The U.S. Department of State Records Disposition Schedule, Chapter 13: Passport Records and Chapter 15: Overseas Citizens Services Records; and Chapter 14: Visa Records will have to be referenced for the specific disposition schedules.

### **b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.**

The data retained in the information system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in the U.S. Department of State Records Disposition Schedule, Chapter 13: Passport Records and Chapter 15: Overseas Citizens Services Records; and Chapter 14: Visa Records; and little privacy risk as a result of degradation of data quality in this information system over an extended period of time.

## **6. Internal Sharing and Disclosure**

### **a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?**

CEAC will transfer data to or receive data from several CA/CST Internal systems to perform many of its functions and services. These include managing system security, obtaining visa application data, future U.S. passport data, biometrics and photos, bank fee transfer information, applicant appointment information, forgotten password management and email addresses. CEAC version 01.00.03 interfaces and/or shares information with the following systems:

- CCD – CEAC interfaces with Consular Consolidated Database (CCD) for replication of all CEAC data. The CEAC domestic application server interfaces with the CCD to retrieve CEAC detail data for replication. This system's security accreditation expires February 28, 2010.
- ACRS – CEAC visa and future passport fee payments will be submitted to ACRS to register within www.Pay.gov. This system's security accreditation expires February 28, 2010.
- Remote Data Collection (RDC) – CEAC will receive the visa applicant biometrics and photo from RDC. This system is in the process of obtaining an accreditation.
- Image Quality Over the Web (IQOW) – the IQOW server will submit the photo images to CCD for replication. This system is in the process of obtaining an accreditation.

### **b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?**

After the CEAC data is submitted to the Department of State network, data transmitted across the network is protected by the bulk encryptors.

### **c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.**

After the CEAC data is submitted to the Department of State network, data transmission across the network or to other agencies is protected by the bulk encryptors inherent within OpenNet, which encrypt the data from domestic operations and posts to the CCD database. Additionally, direct access to CEAC is limited to "Only" approved and authorized users with all required official background investigations and clearances.

## **7. External Sharing and Disclosure**

### **a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?**

The information contained in CEAC is not directly shared outside the Department of State.

### **b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?**

Not applicable. The information contained in CEAC is not directly shared with others outside the Department of State.

**c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.**

Not applicable. The information contained in CEAC is not directly shared with others outside the Department of State.

**8. Notice**

The system:

- contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit [www.state.gov/m/a/ips/c25533.htm](http://www.state.gov/m/a/ips/c25533.htm) for list of all published systems):

The corresponding Systems of Records Notices for this system are: STATE-39, Visa Records, in conjunction with STATE-26, Passport Records, and STATE-05, Overseas Citizen Service (OCS). Data is routinely retrieved using name, date of birth, and place of birth. Depending on the system used to process the applicant's record, case numbers or applicant IDs may also be used to retrieve applicant data.

- does NOT contain information covered by the Privacy Act.

**a. Is notice provided to the individual prior to collection of their information?**

*Visa applications:* The application forms provide notice of the purpose for the information collection, how the information will be used, and potential outcome of not providing information.

The application form provides a statement that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

Also, notice is provided in the System of Records Notice Visa Records, State-39.

*U.S. Passport applications:* An applicant voluntarily elects to complete a passport application. All forms at the time of data collection contain a Privacy Statement, which indicates what information is collected, why, for what purpose the information will be routinely used, who the information will be shared with, and the consequences of not providing the data requested.

**b. Do individuals have the opportunity and/or right to decline to provide information?**

An applicant voluntarily elects to complete a passport or visa application.

With respect to visa applications, individuals who voluntarily apply for a U.S. visa must supply all the requested information, and may not decline to provide part or all the information required, if they wish visa services.

## ***Privacy Impact Assessment: Consular Electronic Application Center (CEAC)***

With respect to passport applicants initial issuance and passport renewals, U.S. citizens who voluntarily apply for a U.S. Passport have the option of supplying all requested information and may decline to provide part or all of the information required if they wish to obtain a passport without penalty but with a possible delay in obtaining their passport with the exception of their SSN. If a individual has a SSN and does not supply it when the application is submitted they are clearly notified on the application that they are of risk of a fine and/or penalties from the IRS.

### **c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?**

*Visa applications:* By providing the information requested, visa applicants are consenting for the information to be used for its identified purpose. With respect to visa applications, individuals who apply for a visa are put on notice that the information may be used as consistent with INA section 222(f). They may not elect for more limited use of the information.

*U.S. Passport applications:* By providing the information requested and signing the application, U.S. citizens are consenting for the information to be used for its identified purpose as it is clearly stated on the passport application and renewal forms.

### **d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.**

*Visa applications:* With respect to visa applications, the information provided on the form and in the SORN regarding visa records fully explain how the information may be used by the Department and how it is protected under INA 222 (f).

*U.S. Passport applications:* An applicant voluntarily elects to complete a passport application. All forms at the time of data collection contain a Privacy Statement, which indicates what information is collected, (why, for what purpose the information will be routinely used, who the information will be shared with, and the consequences of not providing the data requested). These safeguard and notification procedures are reasonable and adequate in relation to the system's purposes.

## **9. Notification and Redress**

### **a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?**

CEAC CTRAC users' access invoice data through shared data (data known to users and the system). These users will have unique user IDs and passwords assigned to them. These users will have information such as case ID and petitioner information or case ID and applicant ID or case ID and applicant name. The CEAC CTRAC, the immigrant fee payment component will allow a login based on petitioner number and case ID or case ID and applicant ID in order to access the on-line invoice for payment of applicant or AOS fees. The IVAGENT and IVAPP will use the same type of shared data access control.

*With respect to visa applications:* The data submitted in the CEAC GENNIV (on-line DS-160) and AGNATO (on-line DS-1648) can not be accessed once it is submitted, with the

## ***Privacy Impact Assessment: Consular Electronic Application Center (CEAC)***

exception of name, DOB, gender and passport number that CEAC RDC uses. RDC does not have the ability to modify this data. RDC uses PKI certificates to control access.

Visa applicants may change their information at any time prior to submission of the application to the Consulate or Embassy. Once that is done, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request and this guidance is available to the public in 9 FAM 40.4:

- (1) Correspondence previously sent to or given to the applicant by the post;
- (2) Civil documents presented by the applicant and
- (3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

Future releases will provide internet/public users with the means to create their own unique user IDs and password for access or access the system using knowledge-based data. Internet/public users will only have access to their own personal data.

*Internet/public users with accounts:* A public user completing a visa application will create a user account that would allow them to save partially completed applications and come back later to login to their account and complete it. These users may also be able to track the status of their application.

*With respect to future U.S. passport applications:* The procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

### **b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.**

To the extent information in CEAC may be Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purposes and uses and its applicable legal requirements. Therefore this category of privacy risk is appropriately mitigated in CEAC.

Additionally, internet/public users will only have access to their own personal data, and this restriction is enforced automatically by the technical access controls inherent within CEAC.

## **10. Controls on Access**

### **a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?**

CEAC supports several user groups:

## ***Privacy Impact Assessment: Consular Electronic Application Center (CEAC)***

- System, Database and Web Administrators/Users Security
- CEAC OpenNet users
- CEAC Internet/Public users
- CEAC System and Web Administrators

Internal access to CEAC is limited to authorized DOS users that have a justified need for the information in order to perform official duties. To access the system, authorized users must be an authorized user of the DOS' unclassified network. Access to CEAC requires a unique user account assigned by a supervisor. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. 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. The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for the IVO application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

CEAC Internet/Public users will acknowledge the Rules of Behavior (ROB) and online Security Awareness issued before access is given to the CEAC Internet web pages.

There are three types of Internet/Public Users:

- Internet/public users with knowledge based shared data (data known to users and the system) - these users will not have unique user IDs and passwords assigned to them. These users will have information such as case ID and petitioner information or case ID and applicant ID or case ID and applicant name. The CEAC CTRAC for immigrant fee payment component will allow a login based on petitioner number and case ID or case ID and applicant ID in order to access the on-line invoice for payment of applicant or AOS fees. The IVAGENT and IVAPP will use the same type of access control.
- Internet/public users without user accounts or shared data - these users will have access to some components to insert visa application data but will not be able to retrieve previously saved information or retrieve data on existing applications or visa cases.
- Internet/public users with accounts – In the future a public user completing a visa application will be able to create a user account that would allow them to save partially completed applications and come back later to login to their account and complete it. These users may also be able to track the status of their application. The account management component of CEAC will provide the ability for public users to create their own account and manage their own password.

**b. What privacy orientation or training for the system is provided authorized users?**

All users must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain access.

**c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.**

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.) As a result of these actions, the residual risk is low.

## **11. Technologies**

**a. What technologies are used in the system that involve privacy risk?**

CEAC operates under standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in CEAC.

**b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.**

No technologies commonly considered to elevate privacy risk are employed in CEAC.

These applications use a secure protocol (SSL) and non-secure protocol to access CA's web sites for the purpose of conducting consular business. The secure protocol (SSL) connection provides strong encryption (128-bit), and with some applications, user/client authentication is also required.

## **12. Security**

**What is the security certification and accreditation (C&A) status of the system?**

The Department of State operates CEAC in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly.

In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, CEAC's most recent date of authorization to operate

***Privacy Impact Assessment: Consular Electronic Application Center (CEAC)***

was February 26, 2008. CEAC's Authority to Operate will expire in February 28, 2011, or upon significant system change.