



## **Privacy Impact Assessment (PIA)**

**For: Consular Electronic Application Center  
(CEAC)**

**Version 01.01.01**

**Last Updated: June 19, 2015**

## 1. Contact Information

<p><b>A/GIS/IPS Director</b> Bureau of Administration Global Information Services Office of Information Programs and Services</p>
---

## 2. System Information

- a. **Date PIA was completed:** June 19, 2015
- 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) is a website supporting a number of web application components that form an Internet-based, full-service Immigrant Visa (IV) and Non Immigrant Visa (NIV) application service center. Immigrant Visa and Non Immigrant Visa applicants use the CEAC components to complete and submit applications, pay consular service fees, submit photos and biometric information with applications, and track application status. The user base varies by component, but overall the system is used by the public as well as domestic and overseas consular posts.

The CEAC components that are currently in use and operating today include:

### **General Nonimmigrant Visa (GENNIV)**

The GENNIV application data collection component, also referred to as the DS-160 form, allows users to complete and electronically submit a DS-160 application to posts worldwide.

### **A-Class/G-Class Non Immigrant Visa/North Atlantic Treaty Organization (AGNATO)**

The AGNATO application data collection component, also referred to as the DS-1648, allows users to complete and electronically submit a DS-1648 application online.

### **Consular Tracking (CTRAC)**

CTRAC is a fee invoice component that allows users to view their consular fee invoices and select those 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.

### **Payment Processing System (PPS)**

The PPS component is utilized when a user chooses to pay a fee from CTRAC.

### **Remote Data Collection (RDC)**

The RDC component is used by third party vendors to collect biometric information (i.e. fingerprints, photos) of applicants who have completed any one of the CEAC applications so they can be sent to posts for additional processing.

**Image Quality over the Web (IQOTW)**

As part of the electronic submission of NIV applications and medical forms, 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.

**Consular Electronic Application Center Web (CEAC Web)**

CEAC Web is a reporting application used by OpenNet users at posts that displays the data collected from AGNATO, GENNIV, IV Agent, and IV App.

**CEAC Status Check (VSC)**

CEAC status check is used by applicants worldwide to check the status of their Non-Immigrant Visa (NIV) or Immigrant Visa (IVO) cases.

**Electronic Immigrant Visa Application forms (IV App)**

The IV Application data collection component is accessible through the existing CEAC. The IV Application component, also referred to as the DS-260 form: Immigrant Visa and Alien Registration Application, allows users to complete and electronically submit an Immigrant Visa and Alien Registration application through the Internet to the National Visa Center for processing. The DS-260 form is the online version of the DS-230 form.

**Electronic Agent of Choice Application (IV Agent)**

The IV Agent data collection component is accessible through the existing 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 the NVC for processing. The DS-261 form is the online version of the DS-3032 form.

**f. Reason for performing PIA:**

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

**g. Explanation of modification (if applicable):**

Not applicable

**h. Date of previous PIA (if applicable):** September 01, 2010

### 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?**

CEAC primarily collects data on foreign nationals as part of the U.S. visa application process. This information can include but is not limited to the following:

- Name
- Birth Date
- Birthplace
- Gender
- Present Country of Residence
- Prior Country of Residence
- U.S. Consul (City/Country)
- Passport Number
- Alien (Case) Number
- Fingerprint
- Photos
- Home/Mailing Address
- Email address
- Bank routing number
- Bank account number
- Marital Status
- Employer Name/Information
- Driver's License Information (if applicant has held a U.S. Driver's License)

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 lawful permanent residents (LPRs)), 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 LPRs . This PII data may include the following:

- U.S. sponsor/petitioner
- U.S. employer
- Names
- Telephone numbers
- Email addresses
- Other contact information

In addition to the PII collected on U.S. citizens associated with visa applicants, the CEAC components that support passport services will also collect PII information on U.S. citizens. This PII data may include the following:

- Name
- Date of Birth
- SSN
- Place of Birth
- Gender
- Employer Name/Information
- Mailing Address
- Email Address
- Contact Phone Number
- Passport Book or Passport Card Information

The sources of the information are the individuals applying for consular services.

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

The information is obtained directly from individuals' applications for visas, passport books, or passport cards using an online form, or applications for refugee status in the United States. The data is submitted via the Internet where it is electronically stored within the Demilitarized Zone (DMZ). A scheduled database procedure pulls the data from the DMZ to the OpenNet environment where it is accessed by consular officers at post and/or domestic agencies.

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

Each element of collected PII is necessary to determine the eligibility of U.S. visa and passport card applicants. CEAC was created because the Bureau of Consular Affairs (CA) was tasked to develop an online visa application and data collection system that helps process applicants' data directly from an online database instead of a paper form presented at post.

CEAC simplifies the Non-Immigrant Visa (NIV) and Immigrant Visa (IV) application process because many of the NIV and IV application forms collect the same information (surname, given name, address, phone number, etc.) CEAC combines the forms into one data collection wizard so the applicant has to enter the data only once rather than multiple times on a paper forms.

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

There are two main accuracy checks:

- CEAC has built-in functionality to perform validation on fields to ensure that data input meets certain criteria.
- Staff at post and/or the Washington Visa Office screen the database records prior to the applicant's interview.

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

The following authorities provide for the administration of the program supported by CEAC:

- 8 U.S.C. 1101-1363a (Titles I and II of the Immigration and Nationality Act (INA) of 1952, as amended )
- 22 C.F.R. Subchapter E, Visas
- 22 C.F.R. Subchapter C, Part 22, Schedule of Fees for Consular Services – Department of State and Foreign Service

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

The collection of PII creates the vulnerability that Department of State employees may use the information for purposes other than those required by the Department. The potential threats to privacy include:

- **Inadequate Security by the Department of State**  
Department of State employees may create a new repository of PII that is vulnerable to unauthorized access, use, disclosure or retention.
- **Inadequate Openness and Transparency**  
Department of State may not provide sufficient details to allow applicants to understand how the information will be used.

As it relates to visa application processing, the impact could result in processing delays, denial of visas, or misuse of PII. For the applicants, misuse of PII could result in blackmail, identity theft, financial losses, physical harm, discrimination, or emotional distress. For the Department of State, the misuse of PII could result in administrative burdens, financial loss, damaged public reputation and public confidence, or civil liability. The opportunities for the misuse of PII and the serious impact that it would have on applicants, the Department of State and the integrity of CEAC makes the misuse of PII a high risk.

Department of State addresses these risks by limiting the collection and transmission of PII to the minimum CEAC business functions. Numerous management, operational, and technical security controls are in place to safeguard the information in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, firewalls, intrusion detection systems, antivirus software, and audit reports. In addition, these controls are subject to rigorous testing and the formal Assessment and Authorization (A&A) process. The Authorization To Operate is granted by the Chief Information Officer (CIO) for the Department. Security controls are reviewed annually and the system is assessed and authorized every three years or sooner if significant changes are made to the application.

These risk factors are mitigated through the use of Technical, Management, and Operational security controls. The CEAC application data is protected by multiple layers of security controls including OpenNet security, CEAC application security, Department site physical security and management security.

#### 4. Uses of the Information

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

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. The CEAC components collect the personal information as defined in Section 3(a) 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, they present the form to a Consular Officer at an overseas post. The officer at post initiates the visa process using the information in the Non-Immigrant Visa (NIV) application to adjudicate the applicant's eligibility for a U.S. visa.

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

Once an applicant submits a completed application through CEAC, the data is stored in the CEAC database in the DMZ. It is then replicated to the OpenNet. CEAC Web retrieves the submitted data and displays it in a report format on the OpenNet. Department users are able to access these reports through the Consular Consolidated Database (CCD) Web Portal. The reports display the data entered in any one of the online visa application forms. Department users can add comments, view commenters' user IDs and note that the data has been reviewed. These are the only new data elements that may be produced.

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

CEAC does not use commercial information, publicly available information, or information from other Federal agency databases.

**d. Are contractors involved in the uses of the PII?**

CEAC is a government owned system. However, contractors are involved with the design, development and maintenance of the system. Privacy Act information clauses have been inserted into all Statements of Work and become part of the signed contract. All users are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements.

**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. Security controls permit account administrators to deny access to reports or categories of information. All users, including external agency users, are screened prior to their employment with the Department of State or with their respective agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a

name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before given access to the OpenNet and any Bureau of Consular Affairs, Office of Consular Systems and Technology (CA/CST) system, including CEAC, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

Diskettes, CDs, and printouts are stored in a safe and secure manner in accordance with security requirements. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of SBU media and paper. In addition, there are technical system security controls in place as described in Section 3(f) above.

Contractors that do not have access to the actual PII data and that are involved in the design, development, and maintenance of CEAC are required to have a Moderate Risk Public Trust access authorization. This includes a “National Agency Check” of the files of certain government agencies such as criminal law enforcement and homeland security for pertinent facts bearing on loyalty and trustworthiness.

Contractors that do have direct access to CEAC PII and that are involved in the development or maintenance of the hardware or software must have at least a Secret-level security clearance.

All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses and contractor owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

## 5. Retention

### a. How long is information retained?

The retention time of the visa records varies depending upon the specific kind of record. Files of closed cases are retired or destroyed in accordance with the published record schedules of the Department of State and the National Archives and Records Administration, specifically General Records Schedules GRS 20 items 2b and 2c. Some records, such as refused records, are retained until the subject is 100 years old and 10 years have passed since the last visa activity. The following information pertains to records retention schedules that are relevant to CEAC records:

A-14-001-02a Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants  
Description: a. Case files on individual aliens issued an immigrant visa.

**Disposition: Destroy 6 months after issuance.**

DispAuthNo: N1-059-86-2, item 1a

A-14-001-02b Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants  
Description: b. Case files on individual aliens issued a non-immigrant visa.

**Disposition: Destroy 1 year after issuance.**

DispAuthNo: N1-059-86-2, item 2b

A-14-001-02c(1)(a) Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Description: c. 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.

**Disposition: 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)).

DispAuthNo: N1-059-91-28, item 1c(1)(a)

A-14-001-02c(1)(b) Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Description: Cases of applicants refused or presumed ineligible under Section 212(a)(33) of the Immigration and Nationality Act.

**Disposition: Retain until alien is 100 years of age, then destroy.** (ref. NC1-59-86-2, item 2c1(b))

DispAuthNo: N1-059-91-17, item 1

A-14-001-02c(1)(c) Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Description: c. 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.

**Disposition: Destroy 2 years after date of refusal.**

DispAuthNo: N1-059-86-2, item 6d

Disposition procedures are documented at the Office of Freedom of Information, Privacy, and Classification Review and can be found at [www.foia.state.gov/Learn/RecordsDisposition.aspx](http://www.foia.state.gov/Learn/RecordsDisposition.aspx).

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

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater the risk of unauthorized use or exposure. Second, the longer the records exist, the more likely inaccuracies will develop as a consequence of aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of CEAC throughout the lifetime of the data. Accuracy of the data is dependent on the applicants providing self-identifying information or individuals providing accurate PII on behalf of the applicant. The information is retained for the duration specified in Section 5(a) above in accordance with applicable law.

Department of State OpenNet security protocols are used to ensure that the data is stored and processed in a secure environment.

All physical records containing personal information are maintained in secure file cabinets or in restricted areas which are only accessible by authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with published Department of State record schedules as approved by the National Archives and Records Administration.

## **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?**

#### **CA/CST's Consular Consolidated Database (CCD)**

Online application form data and associated documents, fee payment data and appointment information is shared with CCD. CCD connects to CEAC for the purpose of production data replication to consular posts and reporting via CEAC Web.

#### **CA/CST's Automated Cash Register System (ACRS)**

CEAC shares payment information for consular services with ACRS. The CEAC PPS component connects to ACRS to send payment information to Pay.gov to verify payment information is received.

#### **CA/CST's Ten Print Live Scan (TPLS)**

CEAC shares the applicant's biometric information with TPLS. The CEAC RDC component interfaces with TPLS to capture the applicant's biometric information in order to verify it.

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

Information is shared by Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information. Electronic files are password protected and access is controlled by system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

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

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. These vulnerabilities are mitigated by working closely with the sharing organizations to develop secure standard operating procedures for using this data. These procedures are documented in sharing agreements.

Access to information is controlled by application access controls. User training at the application level is delivered annually in accordance with internal Department of State regulations.

## 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?

CEAC information is shared with the Departments of Homeland Security, Commerce, Defense, Treasury, Energy, and the Federal Bureau of Investigation. Information is shared in the form of reports from CEAC Web. Currently, these organizations only have access to applicant information contained within the DS-1648 and DS-160 forms. Once the IV Application and IV Agent components are deployed, these organizations will have access to data contained within the DS-261 and DS-260 forms. Information is shared in order to facilitate the execution of each agency's unique mission.

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

CEAC allows non-Department of State user access to CEAC Web reports through the CCD Portal Service (PS)-defined user roles.

In all cases of sharing with the Department of Homeland Security (DHS), all components are required to comply with the DHS' security policies and procedures.

Each data sharing arrangement with federal agency partners is covered by a written agreement in the form of a Memorandum of Understanding or exchange of letters as well as technical documentation including an interface control document and interagency security agreement. Transmissions are encrypted.

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

Any data sharing, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. These risks to privacy are described in Section 3(f) above. These vulnerabilities are mitigated by working closely with the sharing organizations to establish formal agreements and develop secure standard operating procedures for sharing the data. The security program involves the establishment of strict rules of behavior for each major application, including CEAC. It includes a periodic assessment of physical, technical, and administrative controls designed to enhance accountability and data integrity. It also requires that all users be adequately trained in their security responsibilities. System users must participate in a security training program, and contractors and consultants must also sign non-disclosure agreements. External connections must be documented and approved with both parties' signatures in an Interconnection Security Agreement ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

## 8. Notice

The CEAC system:

- contains information covered by the Privacy Act.  
Provide number and name of each applicable system of records.  
Visa Records - STATE-39
- does NOT contain information covered by the Privacy Act.

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

An applicant voluntarily elects to complete the visa application process, and all associated CEAC forms. 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.

Visa applications display a statement that the information is protected by section 222(f) of the INA. Section 222(f) provides that records pertaining to the issuance and refusal of visas 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.

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

Yes, the applicants have the right to decline to provide PII for use in processing their application. However, failure to provide the information necessary to process the application may result in the application being rejected.

**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?**

Information is given voluntarily by the applicants or a representative. No other special uses of the information are permitted. Individuals are advised on the use of the information being collected at the time of collection.

**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.**

CEAC relies on the Visa Records Systems of Records Notice, State-39 to mitigate the privacy risks posed by collection and use of PII.

The mechanisms for notice offered to individuals are reasonable and adequate in relation to the system's purpose and uses. The information provided on the forms and in the SORN regarding visa records fully explain how the information may be used by the Department and how it is protected.

Furthermore, access to CEAC is restricted to cleared, authorized Department of State direct hires and 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.

## 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?

Information provided by an applicant for a visa is considered a visa record subject to confidentiality requirements under INA 222(f).

Visa applicants may change their information at any time prior to submission of the application to the consulate or embassy. Once the application has been submitted, 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:

- Correspondence previously sent to or given to the applicant by the post;
- Civil documents presented by the applicant;
- 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.

The Privacy Act SORN State-39 Visa Records and 22CFR 171.31 publish the procedures for notification and redress, as well as procedures for inquiries, access and amendments of records.

Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement and in the interest of national defense and foreign policy if the records have been properly classified, or 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 covered under the Privacy Act, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore, this category of privacy risk is appropriately mitigated in 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?

Internet based users of CEAC only have access to the extent necessary to complete the online forms as required to apply for a visa.

Internal access to CEAC 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. To access the system, users must be granted the status of an authorized user of the Department of State's unclassified network. 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.

The operating system interface allows the system administrator or ISSO to review audit trail information. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year. The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

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

It is mandatory for all Department of State employees and contractors to complete an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

The CA post officers/users, system administrators, and database administrators receive security awareness training to safeguard Sensitive But Unclassified data (SBU) from unauthorized users.

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Internet based users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

- 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.**

System Administrators and supervisors determine and regularly review access levels and privileges. Inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity.

## 11. Technologies

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

CEAC does not employ any technology known to elevate privacy risk.

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

Since CEAC does not use any technology known to elevate privacy risk, standard safeguards are considered sufficient to mitigate the risk.

## 12. Security

- a. What is the security assessment and authorization (A&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 on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security management Act (FISMA) of 2002, the triennial assessment and authorization of this system is underway. This document was updated as part of the triennial reauthorization of the system which is expected to be approved by July 2015.