1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: October 7, 2010

(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 together form an Internet-based, full-service immigrant visa and nonimmigrant visa application service center. Immigrant visa (IV) and nonimmigrant visa (NIV) 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 and the system is used by the public as well as domestic and overseas consular posts. In the future CEAC will support passport services for U.S. citizens in addition to the currently supported NIV/IV applicants.

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 Form DS-160, allows users to complete and electronically submit a Form DS-160 application to posts worldwide.

CEAC GENNIV, or the Form DS-160, includes questions/fields that were once asked in the following paper forms:

DS-156: Nonimmigrant Visa Application

DS-156E: Nonimmigrant Treaty Trader / Investor Application

DS-156K: Nonimmigrant Fiance(e) Visa Application

DS-157: Supplemental Nonimmigrant Visa Application

DS-158: Contact Information and Work History for Nonimmigrant Visa Applicant

A-Class/G-Class Nonimmigrant Visa/North Atlantic Treaty Organization (AGNATO) – The AGNATO application data collection component, also referred to as FormDS-1648, allows users to complete and electronically submit Form 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. The user is also able to exit the component and return later to check payment status. Once the payment has cleared the bank, the user also has the option to print and/or email a document cover sheet that is required when submitting paperwork associated with some consular processes (e.g., the IV application process). The component currently provides the opportunity for users to view and select payment invoices for Affidavit of Support (AOS) and IV application fees. Eventually, the component also will be used to handle invoices for Nonimmigrant Visa (NIV) and passport fees as well.

Payment Processing System (PPS) –The PPS component is invoked when a user chooses to pay a fee from CTRAC. PPS receives a limited amount of payment information (e.g., service type code, fee amount, etc.) from CTRAC and presents users with a data entry screen that allows them to enter payment information which is submitted, along with the data from the invoice, to the Department of Treasury website Pay.gov via the Automated Cash Register System (ACRS).

Remote Data Collection (RDC) - The RDC component is used by third party vendors to collect biometric information (i.e. fingerprints, photos) of applications 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 posts that displays the data collected from AGNATO, GENNIV, IV Agent, and IV App. It also includes 10 reports to be used by NVC in processing the DS-260 and DS-261 applications.

Future CEAC components include:

CEAC Medical – The CEAC Medical component allows eligible users (i.e., select overseas panel physicians) to complete and electronically submit the required sub-set of the six medical forms that may be required of Immigrant Visa or Refugee applicants. These forms include:

CEAC DS-2053 - Medical Examination for Immigrant or Refugee Applicant

CEAC DS-2054 - Medical Examination for Immigrant or Refugee Applicant

CEAC DS-3024 - Chest X-Ray and Classification Worksheet

CEAC DS-3030 - Chest X-Ray and Classification Worksheet

CEAC DS-3026 - Medical History of Physical Examination Worksheet

CEAC DS-3025 - Vaccination Documentation Worksheet

Electronic Immigrant Visa Application forms (IV App) – The IV App data collection component will be accessible through the existing CEAC. The IV App component, also referred to as Form DS-260: 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 (NVC) for processing. Form DS-260 is the online version of Form DS-230.

Electronic Agent of Choice Application (IV Agent) – The IV Agent data collection component will be accessible through the existing CEAC. The IV Agent component, also referred to as FormDS-261: Choice of Address and Agent for Immigrant Visa Applicants will allow IV applicants to complete, sign, and submit the (DS-261) form online through the Internet to the NVC for processing. Form DS-261 is the online version of FormDS-3032.

Online Application for Passport Card (OAPC) – The OAPC system is an online application for passport cards designed for qualified U.S. passport book holders who meet all requirements of Form DS-82. OAPC allows qualified passport card applicants to complete the application form, upload passport photo, pay applicable fees, and submit the application online.

(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): The CEAC PIA is being updated to include the CEAC Medical forms component.

(h) Date of previous PIA (if applicable): December 29, 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?

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
- Sex
- Present country of residence
- Prior country
- U.S. Consul (city/country)
- Passport number
- Alien (case) number
- Fingerprint
- Photos
- Home/Mailing address
- Medical information (CEAC Medical)

- 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 legal permanent residents (LPR's)), 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 personally identifiable information (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
- Sex
- Employer name/information
- Occupation (OAPC Specific)
- Height, hair and eye color (OAPC Specific)
- Trip information (OAPC Specific)
- Marital history (OAPC Specific)
- Mailing address
- Email address
- Contact phone number
- Passport book or passport card information

b. How is the information collected?

The information is obtained directly from individuals applying for a visa, passport book, or passport card using an online form, or applying for refugee status in the United States. The data is submitted online over the Internet where it is electronically stored (temporarily for OAPC) within the Demilitarized Zone (DMZ). A database procedure on OpenNet pulls the data from the DMZ to the OpenNet environment (on a scheduled basis) where it is viewable by consular officers at post and/or domestic agencies.

c. Why is the information collected and maintained?

Each element of personally identifiable information (PII) collected is necessary to determine the eligibility of persons who applied, or are applying, for a U.S. visa or U.S. passport card. The Department of State, Bureau of Consular Affairs, was tasked to develop an online visa application and data collection system that allows posts to receive applicant data directly from an online database instead of from a paper form presented by the applicant at post.

This effort was intended to significantly simplify the Nonimmigrant Visa (NIV) and Immigrant Visa (IV) application process. Many of the NIV and IV application forms collect the same information (surname, given name, address, phone number, etc.). By combining a number of forms into one data collection wizard, the applicant will only have to enter much of this data once.

Furthermore, the Bureau of Consular Affairs was tasked to develop an Online Application for Passport Card (OAPC) and data collection system that processes applicant data directly to a database rather than through paper form.

This effort is intended to be a 90 day or 20,000 applications (which ever is met first) pilot in order to demonstrate the viability of the process and to facilitate CA/PPT's ability to intake, verify, adjudicate, and archive an online application for a passport card from an applicant who currently holds a valid, 10-year U.S. passport book and meets the requirements of Form DS-82. (Reference: OAPC Business Requirements Specification)

d. How will the information be checked for accuracy?

There are two main accuracy checks:

1) CEAC has built-in functionality to perform validation on fields to ensure that data entered meets certain criteria.

2) With applicant information submitted and stored electronically, staff at the post and/or at the Visa Office in Washington perform some screening of the data prior to the applicant arriving for the interview.

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

CEAC was developed and modified to support U.S. immigration and nationality law as defined in the major legislation listed below:

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 22 U.S.C. 2651(a) (Organization of the Department of State)
- The Immigration and Nationality Act (INA) , 8 U.S.C. 1202(f) (Confidential Nature of Visa Records)
- Immigration Act of 1990
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA96)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000)
- USA Patriot Act of 2001 (HR 3162) (P.L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)
- Child Status Protection Act (HR 1209) 2002

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 personally identifiable information (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 and retention;

- Inadequate openness and transparency – Department of State may not provide sufficient details to allow applicants to understand how information will be used.

As it relates to visa and/or passport application processing, the impact of these threats could result in processing delays, possible subsequent denial of immigration to the United States, issuance of a U.S. passport based on faulty data, or misuse of PII which could result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised, and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State. The opportunities for the misuse of PII and the serious impact that it would have on applicants and the integrity of CEAC makes the misuse of PII a high risk.

The Department of State seeks to address these risks by minimizing the collection and transmission of PII to the minimum required to perform the business functions required of CEAC. To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and 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, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports. In addition, these controls are subject to rigorous testing, formal Certification and Accreditation (C&A). Authority to operate is authorized by the Chief Information Officer (CIO) for the Department. Security controls are reviewed annually, and the system is certified and accredited every three years or sooner if significant changes are made to the existing application.

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 application form used in the visa issuance process. 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 Nonimmigrant Visa (NIV) application to adjudicate the applicant's eligibility for a U.S. visa.

The information collected by the CEAC passport components, when operational, will be used to determine the eligibility of U.S. citizens who apply for a U.S. passport book or card. The CEAC components do not determine the eligibility of applicants who are applying for a U.S. passport book or card. The CEAC components allow the applicant to complete an online application form used in the passport adjudication process. The adjudication process determines the eligibility of the applicant. Adjudication is the process where applications are reviewed to verify and examine citizenship evidence. Adjudication is conducted at passport agencies after the namecheck process using the Independent Namecheck (INK) application. Adjudicators view namecheck and special namecheck results and supporting documentation required of the applicant. The Travel Document Issuance System (TDIS) is used to physically issue the passport book/card.

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 the 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 visa or passport online application forms. Department users have user privileges that allow them to add remarks, view the User IDs of users who made remarks, and indicate that the data has undergone a cursory review. In a future version of CEAC, Department users will also be able to reopen a Form DS-260 or Form DS-160 application to allow the applicant to make corrections. These are the only new data elements that may be produced.

For CEAC Medical, once the panel physician submits the completed set of forms, 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. Users are able to access these reports through the Consular Consolidated Database (CCD) Web Portal. Selected data is replicated to the Center for Disease Control (CDC) - Electronic Data Notification (EDN) system. The reports display the data entered in the Medical forms. Department users have user privileges that allow them to add remarks, indicate that the data has been checked, and view the User IDs of users who made remarks within the report. 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 are 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. Access control lists permit categories of information and reports that are to be restricted.

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 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.

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 are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that is SBU.

In addition, there are technical system security controls in place as described in Section 3(f) above.

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 to the published record disposition schedules of the Department of State and the National Archives and Records Administration (NARA), specifically 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 retention time of the passport records varies depending upon the specific kind of record. Files of closed cases are retired or destroyed in accordance to the published record disposition schedules of the Department of State and NARA. Some records, such as case files containing passport applications, are retained permanently at NARA.

Disposition procedures are documented at the Office of Freedom of Information, Privacy, and Classification Review, Room 1239, Department of State, 2201 C Street NW, Washington, DC 20520-1239.

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 to 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 individuals providing self-identifying information or individuals providing personally identifiable information (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 secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. 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 (NARA).

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 applicant biometrics information with TPLS. The CEAC RDC component interfaces with TPLS to capture the applicant biometrics to run a bio check against applicants.

CA/CST's Panel of Physicians (POP) – Initial password to CEAC Medical is shared with POP. The user's initial password will be set by the Panel of Physicians system and then the user will have to change it upon first log-in to CEAC Medical.

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

Information is shared by secure transmission methods permitted by Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Access to electronic files is protected by passwords, and is under the supervision of 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 Department of Homeland Security (DHS), Department of Commerce (DOC), Department of Defense (DOD), Department of the Treasury(DOT), Department of Energy (DOE) and the Federal Bureau of Investigation (FBI). Information is shared in the form of reports from CEAC Web. Currently, these organizations only have access to applicant information contained within the Forms DS-1648 and DS-160. Once the IV App and IV Agent components are deployed, these organizations will have access to data contained within both Forms DS-261 and DS-260. Information is shared to help carry out the unique missions of each agency. In addition, select medical data will be shared with the Center of Disease Control (CDC) to determine entry in the United States and follow-up with state and local health departments.

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 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 Department's security policies and procedures, particularly the *DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1).* This handbook establishes a comprehensive program for DHS to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules, which are applied

to component systems, communications between component systems, and at all interfaces between component systems and external systems.

Each data sharing arrangement with federal agency partners is covered by a written agreement in the form of a memorandum of understanding (MOU) or exchange of letters as well as technical documentation including an interface control document and interagency security agreement. Data is sent through encrypted lines

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' signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

- Visa Records, State-39
- Passport Records, State-26

☐ 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 or passport application process, and therefore all associated CEAC forms. All forms indicate 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 and how it is protected.

With respect to applications for visas: the forms provide a statement that the information collected 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 personally identifiable information (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.

b. 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 his/her 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.

c. 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 System of Records Notice (SORN) State-39 and SORN State-26 to mitigate the privacy risks posed by collection and use of personally identifiable information (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 and passport records fully explain how the information may be used by the Department and how it is protected.

Further, 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 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
(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.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record.

Certain exemptions to Privacy Act provisions for notification and redress may exist for visa 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.

Future functionality will allow the Department to reopen a submitted Form DS-160 or DS-260 so that applicants can make corrections on their submitted DS-160 or DS-260 applications.

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 passport or visa.

CEAC Medical allows access to panel physicians who have been approved by the Department of State and are in the PoP application. Each user will have a username and password to log-in to the CEAC Medical application and will only have access to applicants in the country where the user is authorized as a panel physician. 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.

Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

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

d. 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.

Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed. 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 robust safeguards are determined to be at the very minimum satisfactory in this application.

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 safeguarded and protected. The Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk and implemented controls. The Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, CEAC completed the C&A process, and was granted an Authority to Operate (ATO) that will expire in February 2011. CEAC is currently undergoing a full Certification and Accreditation (C&A) that will result in a new ATO prior to the current expiration.