PRIVACY IMPACT ASSESSMENT

Consular Electronic Application Center (CEAC)

1. Contact Information

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

2. System Information

(a) Name of system: Consular Electronic Application Center

(b) Bureau: Consular Affairs (CA)

(c) System acronym: CEAC

(d) iMatrix Asset ID Number: # 2712

(e) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The system is currently undergoing an Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO) status. CEAC is expected to receive an ATO by Spring 2018.

(c) Describe the purpose of the system:
The Consular Electronic Application Center (CEAC) is a website supporting a number of web application components (listed below) 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) (Nonimmigrant application customers)
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. Nonimmigrant applicants provide U.S. point of contact information via Form DS-160.

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

Consular Tracking (CTRAC) (Immigrant Visa Applicants)
CTRAC is a fee invoice component that allows immigrant Visa applicants to view their consular fee invoices and select 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.CTRAC collects Immigrant data only.

Payment Processing System (PPS) (Immigrant Visa applicants)
The PPS component is utilized when a user chooses to pay a fee from CTRAC. PPS collects immigrant data only.

Remote Data Collection (RDC) (Immigrant and Non Immigrant customers)
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. RDC collects immigrant and nonimmigrant data.

Image Quality over the Web (IQOTW) (Nonimmigrant Visa application customers)
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. IQOTW collects nonimmigrant data only.

Consular Electronic Application Center Web (CEAC Web) (Immigrant and nonimmigrant applicants)
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 WEB can have information about immigrant, nonimmigrant and U.S. persons, if information is provided by the applicant.

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

Electronic Immigrant Visa Application forms (IV App) (Immigrant and Diversity applicants)
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. DS 230 form collects immigrant data and information on the IV applicant's petitioner (ie., a U.S. person).

Electronic Agent of Choice Application (IV Agent) (Immigrant applicants)
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. DS 3032 form collects immigrant data and data on U.S. persons, if the applicant's agent is a U.S. person.

CEAC IV Summary (Immigrant customer data)
The IV Summary page is the login page of CEAC and the page that is displayed upon successful login. It displays links to the forms required for processing (i.e. DS-260 and DS-261), links to the fee payment (i.e. CTRAC), links to messages, and links to the document upload functionality (i.e. CEAC Docs). In addition, depending on the visa class of the case, users can also access other optional functionality such as the ability to Add Applicant, Remove Applicant, Add Joint Sponsor, Add Household member, and to change the travel status of a dependent on the case. CEAC IV Summary contains only summary information on immigrant applicants.

CEAC Messages
The National Visa Center and post have the ability to send one-way messages to the applicant via CEAC. The messages are displayed on the CEAC Messages page, which is accessed by a link from the CEAC IV Summary page. At this time, applicants are not able to respond to messages through CEAC.

CEAC Document (CEAC Docs) (Immigrant and nonimmigrant data customer data)
The CEAC Docs component allows users to upload supporting documentation to their case and electronically sends the documentation to the NVC or post for review and processing. The CEAC Docs component consists of two pages: Affidavit of Support (AoS) Documents, which is the page where applicants would upload AoS documentation or financial forms/evidence, and the Civil Documents page, which is the page where applicants would upload civil documents that are required to support their visa application. The immigrant and nonimmigrant applicants can provide information about their petitioner (a U.S. person) in the uploaded supporting documentation provided to process their visa requests.

Virus Detection Service (VDS)
VDS is a customizable service-oriented architecture (SOA) restful web service application to perform virus scanning. It is to be used by CA/CST applications, such as CEAC, that require files or documents to be scanned for viruses before they are saved to minimize or eliminate virus infection or corruption in DMZ databases, which if the data is pulled into the OpenNet, could also contaminate the CCD. The application leverages the commercial product Symantec Protection Engine for the purpose of scanning files and providing the results, and uses an Oracle database to log the activity.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates: CEAC primarily collects data on foreign nationals as part of the U.S. visa application process. This information includes:

- Name
- Birth Date
- Birthplace

- Gender
- Present Country of Residence
- Prior Country of Residence
- U.S. Consul (City/Country)
- Passport Number
- Alien (Case) information
- Fingerprint
- Photos/Biometric ID
- Home/Mailing Address
- Phone numbers
- Email address
- Substantial financial information
- 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)
- Policy Certificate
- Marriage Certificate
- Financial Documents (i.e. tax filing)
- Birth Certificate
- Criminal Incarceration
- Substantive individual family information
- Substantive individual personnel information
- Substantive medical information

The information provided by the visa applicant is considered a visa record subject to the confidentiality provisions of section 222(f) of the Immigration and Nationality Act (INA). Because visa applicants themselves are not U.S. persons (that is, U.S. citizens or lawful permanent residents (LPRs)), they are not covered by the provisions of the Privacy Act 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 U.S. sponsor/petitioner; such as:

- U.S. employer
- Names
- Home addresses
- Social security numbers
- Telephone numbers
- Email addresses
- Other contact information

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

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

22 U.S.C. § 3927 (Chief of Mission)

8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
22 U.S.C. 211a-218, (Passports)
22 U.S.C. 2651a (Organization of Department of State)
8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
26 U.S.C. 6039E (Information Concerning Residence Status)
8 U.S.C. 1151-1363 (Title II of the Immigration and Nationality Act of 1952, as amended)
22 C.F.R. Parts 40-42, and 46 (Visas)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
- SORN Name and Number: STATE-39, VISA Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): October 25, 2012

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX))
  Length of time the information is retained in the system
  Type of information retained in the system:

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.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)
☐ U.S. Government/Federal employees or Contractor employees
☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?
26 U.S.C. 6039E (Information Concerning Residence Status)

(c) 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.

(d) Where is the information housed?
☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.

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

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Yes, the information is current to the maximum extent possible. Information collected from individuals and stored in Department information systems can be amended or revalidated by the subject of the record. When an individual utilizes a particular external facing Consular Affairs information system to create his/her own record, he/she can modify or amend the record by accessing the record directly on the website or contacting the relevant departmental office to amend the record in accordance with the procedures stated in the SORN.

(g) Does the system use information from commercial sources? Is the information publicly available?
CEAC does not use commercial information, publicly available information, or information from other Federal agency databases.

(h) Is notice provided to the individual prior to the collection of his or her information?

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

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

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

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.

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

Additionally, the CEAC site displays a disclaimer which informs the applicant: "For information on the Department of State's privacy policy regarding the nature, purpose, use, and sharing of any Personally Identifiable Information (PII) collected via this website please click here. For disclaimer and notices associated with a specific information collection please click on that information collection. Our privacy policy explains our information practices when you provide PII to us, whether collected online, or when you visit us online to browse, obtain information, or conduct a transaction. PII may include: your name, email, mailing and/or home address, phone numbers, or other information that identifies you personally." An address to the Public Communication Division is also provided for applicants to contact if they have questions.

- If no, why are individuals not allowed to provide consent?

NA

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII items listed in Question 3d are the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were cogitated during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

(a) What is/are the intended use(s) for the 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, it is transferred to the local database at post. The Consular officer at post initiates the visa process using the information in the Non-Immigrant Visa (NIV) application or the Immigrant Visa Overseas (IVO) application to adjudicate the applicant's eligibility for a U.S. visa.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?
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 Consular Consolidated Database (CCD). CEAC Web retrieves the submitted data and displays it in a report format on the webpage.

(2) Does the analysis result in new information?
No, the analysis only results in reports. 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.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☒No – the reports display the same information that is in the online form.

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

INTERNALLY

CA/CST's Consular Consolidated Database (CCD)
CA/CST's Automated Cash Register System (ACRS)
CA/CST's Ten Print Live Scan (TPLS)
CA/CST's Non-Immigrant Visa (NIV)
CA/CST's Immigrant Visa Overseas (IVO)
CA/CST's Immigrant Visa Information system (IVIS)
CA/CST's Pre IVO Technology (PIVOT)
CA/CST's electronic Diversity Visa (eDP)
CA/CST's Diversity Visa Information (DVIS)

EXTERNALLY

CEAC information is shared with the Departments of Homeland Security, Commerce, Defense, Treasury, Energy, and the Federal Bureau of Investigation.

(b) What information will be shared?

PII detailed in section 3d, as well as the following PII, may be shared with the other CA sytems listed above:

- Reporting and Information,
- Collections and Receivables
- Appointment information
- Alias name
- Nationality
- refusal code
- date of U.S. arrival
- Income information for Joint Sponsors
- Petitioner Country of Birth
- Petitioner Date of Birth
- U.S. driver's license number
- U.S. taxpayer ID
- Student exchange visitor information system identification (SEVIS ID)
- Barcode number associated with the CEAC application
- Applicants' previous visa class information
- Visa class associated wth current applicant case

EXTERNALLY

Information is shared in the form of reports from CEAC Web with the above external organizations listed in paragraph 6(a). These organizations have access to applicant information contained within the DS-1648, DS-160, DS-261, and DS-260 forms.

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

INTERNALLY

The information is shared internally in order to process immigrant and nonimmigrant visa applications. Specifically:
CCD connects to CEAC for the purpose of production data replication to the NVC, consular posts and reporting via CEAC Web.

The CEAC PPS component connects to ACRS to send payment information to Pay.gov to verify payment information is received.

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

The NIV and IVO applications allow Consular officers to use the information to determine eligibility for a visa.

NVC Staff reviews CEAC information displays on CEAC Web and updates the IVIS application for visa processing.

CEAC IV App data updates the PIVOT application, which is used by the NVC to process immigrant visa cases before transmission to post.

The eDP application allows NVC staff and post users to review documents submitted in CEAC Docs for visa processing.

KCC staff reviews CEAC Web and updates the DVIS application for DV case processing.

EXTERNALLY
CEAC information is shared with the Departments of Homeland Security, Commerce, Defense, Treasury, Energy, and the Federal Bureau of Investigation. Information is shared in order to facilitate the execution of each agency's mission pertaining to immigration and border protection.

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

EXTERNALLY
All communications are encrypted and secured using transport and message level security.

Additionally, 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 that address agreed upon security policies and procedurs.

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

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
INTERNAL/EXTERNAL
Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to non-authorized parties
b. Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, “Sensitive but Unclassified”, and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know

- System authorization and accreditation process along with continuous monitoring (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared with external agencies are encrypted as per the Department of State’s Security’s security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Applicants can view information submitted online by either entering their application ID and answering security questions, or by providing a Case ID and Invoice ID or Principal Applicant's DOB and log-in information at the CEAC site. Information on themselves as well as any petitioner (U.S. persons) information submitted can be reviewed for accuracy by the applicant during this process.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
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, request the Department to unlock or reopen the application for correction and resubmission, or correcting the information during the course of a visa interview.

If no, explain why not.
NA

(c) By what means are individuals notified of the procedures to correct their information?
The Department informs applicants on how to correct the information during the course of their visa process. 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 Title 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32. SORN State-39 (Visa records) provides guidance to individuals on how to access visa records pertaining to them and how to correct information.

8. Security Controls

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

Access to applications/databases is further protected with additional access controls set at the application/database level. All system accounts/access must be approved by the user's supervisor and the Information System Security Officer. The audit vault system is used to monitor all privileged access to the system and violations are reported to senior management daily, if applicable. Data shared with other government agencies is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable NIST 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

To access the system, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a PIV/CAC and PIN which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. 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.

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

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with DS configuration guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and Federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with DS Security Configuration guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with DS configuration guides, auditing is enabled to track the following events on the host operating systems, and back-end database servers:

Multiple logon failures;
Logons after-hours or at unusual times;
Failed attempts to execute programs or access files;
Addition, deletion, or modification of user or program access privileges; or
Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.
Operating System-Level auditing is set in accordance with the DS Security Configuration Guide. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. 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

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory security/privacy training is required for all authorized users including security training and regular refreshment training. Each user must complete the annual Cyber Security Awareness Training and pass the PA-459 course, entitled Protecting Personally Identifiable Information. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users acknowledge electronically and agree to the rules and must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?

Security measures were implemented to ensure the best protection of PII is provided and security is in place to defend from both external and internal threats. NIST 800-53 security controls are the standard for government agencies and include a family of 26 controls for PII. These controls are implemented in this system. The security measures taken meet or exceed the requirements for PII.

9. Data Access

(a) Who has access to data in the system?
System Administrators and authorized Department of State Employees with supervisor approval based on duties assigned that user have access to the data in the system. Internet based users of CEAC only have access to the extent necessary to complete the online forms as required to apply for a visa.

(b) How is access to data in the system determined?
By supervisor signature on an application for access which defines what the user requires to perform their assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
Not all users will have access to all of the data in the system. Defense in depth and separation of duties are used to restrict users to the minimum data necessary to perform their assigned duties, which matches the supervisor approval for which data can be accessed.
Sensitive documents, such as documents with applicant's financial data, are not viewable once uploaded into CEAC.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
Defense in depth and separation of duties are employed. Users are restricted to the minimum data necessary to perform their assigned duties as approved by their supervisor.