PRIVACY IMPACT ASSESSMENT

Overseas Consular Support Applications (OCSA)

1. Contact Information

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

2. System Information

(a) Name of system: Overseas Consular Support Applications (OCSA)

(b) Bureau: Consular Affairs (CA)

(c) System acronym: OCSA

(d) iMatrix Asset ID Number: OCSA: 258562, ACRS 554, ACS 818, AI 4397/AI Web 106201, CST 559, INK 29, IVO 817, NIV 65, TPLS 829

(e) Reason for performing PIA: In addition to triennial Authorization to Operate (ATO), these systems are consolidating under OCSA

☒ New system (as a Logical Consolidated Boundary)

☐ 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?
OCSA is currently undergoing its initial Assessment and Authorization (A&A) as a logically grouped system in order to receive an ATO status. OCSA is expected to receive an ATO by summer 2018.

(c) Describe the purpose of the system:
OCSA is a logical business grouping of several immigration systems and two systems that collect information on American citizens; the American Citizen Services System (ACS) and the Automated Cash Register System (ACRS). The grouping consists of the Automated Cash Register System (ACRS), American Citizen Services (ACS), Accountable Items (AI), Accountable Items Web (AI Web), Consular Shared Tables (CST), Independent Namecheck (INK), Immigrant Visa Overseas (IVO), Non-Immigrant Visa System (NIV), and Ten Print Live Scan (TPLS).

ACRS is a computerized point of sales system that provides cash accountability by managing and monitoring consular fee receipts. This system is used by the Bureau of Consular Affairs' (CA) cashiers (generally Locally Engaged (LE) staff) at posts worldwide to collect fees for the consular services provided (e.g., passport applications, immigrant visa applications, and certain reciprocity fees), print receipts, and process refunds. It also performs end of period reconciliation tasks and prints receipts and management reports that are used by the Accountable Consular Officer (ACO) to maintain accountability of the fee collection process.

ACS supports the Bureau of Consular Affairs (CA) in providing assistance to American citizens living or traveling abroad. ACS is a collection of automated services and support functions used to record services provided to citizens, including passport issuance, tracking report of birth issuance via the Consular Consolidated Database Consular Report of Birth Abroad system (CCD CRBA), arrests, deaths, lost and stolen passports, financial assistance, and more. This is the system where CA employees keep contemporaneous "notes" of their actions on cases for individual American citizens traveling or residing abroad.

AI can be accessed via the processing systems (IVO, NIV or ACS) or a locally installed client application (on workstation) and is used to track accountable inventory. AI records the printing of foils for the Non-Immigrant Visa (NIV) and Immigrant Visa Overseas (IVO) applications at posts, Consular Report of Birth Abroad (CRBA) Certificates at the print facilities to assign CRBAs for Domestic Printing, Local Print and US Print Barcodes, Issue Foils, Supplemental Foils, and Passport Books for American Citizens Services (ACS). It is used at Department of State posts to record the receipt, storage, movement, and final disposition of consular controlled items. At post, each of the consular automated system applications (ACS, NIV, and IVO) utilizes the AI component to track inventory and usage of the controlled items associated with it and to assist Accountable Consular Officers (ACOs) to reconcile their use.

AI Web is different from the version of AI used at post; it does not directly interact with ACS, NIV or IVO. AI Web is a stand-alone, Web-based version of the application which is accessed exclusively by users at the General Services Division (GSD) warehouse. AI Web allows users at the warehouse to receive items from the controlled document suppliers/manufacturers (e.g., Government Printing Office), as well as items that are transferred to the GSD from overseas posts. Users are also able to transfer items to posts worldwide and receive confirmation of the transfer, perform and certify quarterly inventories of the CSF (Consular Supplies Facility), and, although very rare, users also have the capability to destroy items that are outdated and are no longer used. Lastly, users have the ability to transfer items to groups such as the Forensic Document and Design Integrity Coordinators Office (FDDI) for testing purposes. A number of new reports were also created for the warehouse to allow them to view historical inventory, active and historical transfers, active and historical returns, and a history of received items.

CST manages shared reference table data and is responsible for maintaining and managing the validation and lookup data approved by the Visa Office (VO) and Passport Services as well as those specific to individual post locations. It stores and manages reference information used and shared worldwide by other major Department of State (DoS) CA applications. The system also stores and manages database accounts, user roles, and privilege levels for users of CA system applications. When updates are necessary for shared data, CST reduces the need for multiple Configuration Change Requests (CCRs). CST also acts as the sole entry and deployment source for much of the Passport Services Directorate, Visa Office, and CA/Consular Systems and Technology (CA/CST) data.

INK allows posts to process namecheck queries for individuals at a post. INK was derived from the independent namecheck function that was in the Non-Immigrant Visa (NIV) system. In addition to the independent namecheck functions that are available in NIV, INK allows users to add lookouts (independent checks and queries using CLASS to check information), create category-one (CAT-1) refusal files, back scan existing CAT-1 files, extract photos from the scanned documents to store as a separate scanned image associated to an INK record, and generate reports. INK will display the namecheck results returned from the CLASS (Consular Lookout and Support System) via the TCM (Telecommunications Manager) application. Post is also able to add lookouts to the CLASS database via INK. Lookout information may come from a variety of sources including newspapers, Department of Homeland Security (DHS) forms, letters, job applications, and lists of refugees.

IVO provides automated support to the adjudication of an immigrant or a diversity visa application from individuals wishing to come to the United States with the intent to establish permanent residence. IVO provides for the administration of federal law and regulations that govern the issuance or refusal of either visa type, and is a case record and maintenance application used at overseas posts to review and complete the visa adjudication. IVO's main processes are: 1) immigrant visa (IV) case processing, name clearance (through interfaces with name check applications), fingerprint and facial recognition clearance (through interfaces with biometric applications), adjudication, visa issuance, and refusal recording and tracking; 2) visa allocation management for allocations assigned to post; 3) biometric data collection (such as fingerprints and images for facial recognition); 4) automated tracking, scheduling and reporting of applicant interviews and medical exams; 5) internal fraud control, workload statistic management for post and Fraud Prevention Program (FPP) managers; 6) waiver processing; and 7) processing of boarding foils in connection with USCIS-approved parole cases.

NIV issues non-immigrant visas to qualified applicants seeking temporary stay in the United States (U.S.) which are the type of visas most commonly sought by visitors for business, pleasure, or education. NIVs are also granted to government officials, treaty traders and treaty investors, exchange visitors, temporary workers, and fiancées of U.S. citizens. NIV supports the Bureau of

Consular Affairs mission requirements by automating and streamlining posts' capabilities for 1) processing applicant, petition, referral, and diplomatic note data, captured photos, and fingerprints; 2) viewing namecheck, fingerprint IDENT and other clearance request results; 3) recording the decision of the adjudicating officer; 4) printing the Machine Readable Visa (MRV); 5) processing Border Crossing Cards (BCC); 6) processing boarding foils in lieu of transportation letters, scanning documents, and processing clearances such as Security Advisory Opinions (SAO). As of 2004, the system no longer allows new crew list to be created in the application, although the Vessel window remains in the system allowing users to view old crew list data associated with vessels.

TPLS supports the Bureau of Consular Affairs mission requirements for travel documents and immigration documents into the United States of America. TPLS software is installed on a post workstation that is used to capture visa applicant fingerprints via a fingerprint scanner attached by a Firewire cable. Consular officers are always required to collect a complete set of fingerprints and simple biographic information for visa applicants unless exempt based on policy.

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

ACRS collects names and credit card information/account numbers from U.S. citizens applying for U.S. passports.

ACS collects names, including aliases, birthdate, birthplace, passport number, Social Security number (SSN), addresses, e-mail addresses, nationality, name of in-country contacts, information on relatives, medical information and photograph (for passport issuance) from U.S. citizens.

AI/AI Web does not collect PII; therefore, does not require a PIA.

CST collects only business related government employee information: Name, Information Technology (IT) Security info, and Security Management; therefore, does not require a Privacy Impact Assessment (PIA).

INK collects names, birthdates, individual identities from other sources, address, phone or similar information from non-US citizens/permanent residents. An INK record may contain PII about U.S. citizens or legal permanent residents who are associated with the non-U.S. citizens. This PII may include the following: employer name (whether foreign or domestic), sponsor name and address, and U.S. contact name and phone numbers.

IVO collects names, birthdates, address, phone, email, images/biometric identifiers, gender, language used, relationships, occupation, employment information, employer information, financial information, aliases, alien registration number, marital status, nationality, final U.S.

address, passport number and other passport issuance information, national identification, arrival date, and duration of stay information from non-U.S. citizens/non legal permanent residents (LPRs). Depending on what the applicant enters in the system, IVO may also collect some of this information on U.S. citizens/sponsors.

NIV collects names, birthdates, phone, personal address, email, alias, nationality, gender, birth country, passport information, national identification, SEVIS ID (Student and Exchange Visitor Information System Identification), and employer name. It also collects U.S. sponsor's name, contact information and email. If there is a referral by a U.S. citizen direct hire employee, the name of the U.S. citizen will be in NIV. Additionally, there is an open entry field where posts overseas can input additional information required, or data provided by the applicant. This field may contain PII of a U.S. citizen/LPR.

TPLS receives an individual identifier/identification from other sources, and collects fingerprint images (Biometric IDs) from non-U.S. citizens/non-LPRs who are covered by the Immigration and Nationality Act of 1952, as amended, but are not covered under the Privacy Act of 1974, as amended; therefore, a PIA is not required.

NOTE: The remainder of this document addresses the systems which require a PIA: ACRS, ACS, INK, IVO, and NIV.

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

- 5 U.S.C. 552a, Privacy Act of 1974, as amended
- 8 U.S.C. 1101-1504 (Immigration and Nationality Act of 1952, as amended, Titles I-III, General, Immigration, Nationality and Naturalization)
- 8 U.S.C. 1701 et seq., Enhanced Border Security and Visa Entry Reform Act
- 8 U.S.C. 911, 1001, 1541-1546 (Citizenship and Passport related Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, 2705, Passports and Consular Reports of Birth Abroad (CRBAs)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Department of State Authority to Issue, Deny, Limit Passports);
- 22 U.S.C. 1731 (Protection to naturalized citizens abroad)
- 22 U.S.C. 2651a (Organization of Department of State)
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance)
- 22 U.S.C. 2715 (Procedures regarding major disasters and incidents abroad affecting United States citizens)
- 8 U.S.C. 1183a note (Fees relating to Sponsor's Affidavit of Support)
- 8 U.S.C. 1351, 1351 note (Nonimmigrant Visa Fees)
- 8 U.S.C. 1713 (Machine-readable visa fees)

- 8 U.S.C. 1714, 1714 note (Surcharges related to consular services)
- 22 U.S.C. 3904 (Functions of service)
- 22 U.S.C. 4201 (Fees for certification of invoices)
- 22 U.S.C. 4215 (Notarial acts, oaths, affirmations, affidavits, and depositions; fees)
- 22 U.S.C. 4219 (Regulation of fees by President)
- Executive Order 10718, June 27, 1957, 22 FR 4632 (Delegating to the Secretary of State authority to prescribe the rates or tariffs of fees for official services at United States embassies, legations, and consulates)
- 31 U.S.C. 9701 (Fees and charges for Government services and things of value)
- Title 22 of the Code of Federal Regulations, Parts 1 to 299, Foreign Relations (various parts), including 22 CFR Subchapter C, Part 22, Schedule of Fees for Consular Services – Department of State and Foreign Service
-

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
- SORN Name and Number/SORN publication date: State-39, Visa Records 25Oct2012
- SORN Name and Number/SORN publication date: State-26, Passports 24Mar2015
- SORN Name and Number/SORN publication date: State-05, Overseas Citizen Services Records and Other Overseas Records 8Sep2016

☒No, explain how the information is retrieved without a personal identifier.

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

If yes, please notify the Privacy 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 about this question, please contact the Department's Records Officer at records@state.gov .)

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

B-09-002-01a to B-09-002-40b: Consular Records Visa Services
Description: Information obtained from issued immigrant and non-immigrant visa application forms (DS-156, 157, 158, 160, 230, 260, and INS related forms I-129B,I-129F, I-130, I-140 and I-600) and supporting documentation. Immigrant visa case records potentially include the following types of case level data: unique identifier; applicant personal and biographic data; adjudication

data; visa class information; visa clearance and name check data; case summary data; case status data; notes; and reports.
Disposition: Consular Records Visa Services records range from retaining up to 100 years to until superseded, obsolete, or no longer needed depending, on the type of record.

B-09-001-01a to B-09-001-10: Consular Records Passport Services
Description: These records pertain to American citizens abroad who have applied to overseas posts for passports, the renewal, amendment or extension of passports, or for registration and other citizenship services; and files pertaining to American citizens who have applied to territorial governments for passport services.
Disposition: Consular Records Passport Services records range from destroying when no further need for information to maintaining up to 5 years old, depending on the type of record.

A-15-001-02 to A-15-001-17: Overseas American Citizen Services Records
Description: The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts.
Disposition: Overseas American citizen service records are retained from 6 months up to 30 years, depending on the type of record.

A-13-001-05a to A-13-001-05b: Passport Accounting Records
Description: Accounting records showing money received, deposited, or refunded by Passport Services, including cash receipts and other accounting records.
Disposition: Accounting records destroy when 5 years old; cash receipts destroy when 2 years old, depending on the type of record.

The retention of records will vary based on the type of record and the assigned rules by NARA and Department of State. All information can be located in the State Department's Records Management Site: http://a.m.state.sbu/sites/gis/ips/RA/Pages/RDS.aspx

4. Characterization of the Information (collectively)

(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? (collective list)

- 8 U.S.C. 1101-1504 (Immigration and Nationality Act of 1952, as amended, Titles I-III, General, Immigration, Nationality and Naturalization)
- 22 U.S.C. 211a-218, 2705, Passports and Consular Reports of Birth Abroad (CRBAs)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Department of State Authority to Issue, Deny, Limit Passports)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 8 U.S.C. 911, 1001, 1541-1546 (Citizenship and Passport related Crimes and Criminal Procedure)
- 22 U.S.C. 2715 (Procedures regarding major disasters and incidents abroad affecting United States citizens)
- 22 U.S.C. 1731 (Protection to naturalized citizens abroad)
- 22 U.S.C. 3904 (Functions of service)
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance)
- 22 U.S.C. 4201 (Fees for certification of invoices)
- 22 U.S.C. 4215 (Notarial acts, oaths, affirmations, affidavits, and depositions; fees)
- 22 U.S.C. 4219 (Regulation of fees by President)
- Executive Order 10718, June 27, 1957, 22 FR 4632 (Delegating to the Secretary of State authority to prescribe the rates or tariffs of fees for official services at United States embassies, legations, and consulates)22 U.S.C. 6551 (References)
- 31 U.S.C. 9701 (Fees and charges for Government services and things of value)
- Anti-Drug Abuse Act of 1988, PL 100–690, November 18, 1988
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Enhanced Border Security and Visa Entry Reform Act of 2002, PL 107-174, May 14, 2002
- Title 22 of the Code of Federal Regulations, Parts 1 to 299, Foreign Relations (various parts), including 22 CFR Subchapter C, Part 22, Schedule of Fees for Consular Services Department of State and Foreign Service

(c) How is the information collected?

The information is collected from the applicant for visas, passports, and payments/fees.

ACRS-The information is collected directly from the customer who is requesting a fee-based consular service. This information is either manually entered or automatically collected when the credit card is swiped.

ACS-The information is entered into the electronic ACS system by a Department of State employee working either domestically or at the relevant post abroad, and is also collected from other databases depending on the services required by the American citizen. Registration data from STEP (Smart Traveler Enrolment Program) is automatically ingested into the ACS database and made available to post users. Post employees can populate ACS with information regarding

passport issues, and can input information provided by the citizen during the face-to-face interviews after submitting proper identification.

INK- The information is collected from various sources such as visa applications, passports, corroborating documentation and in-person interviews.

IVO- Data is collected by consular posts from visa applications, passports, corroborating documentation and in-person interviews. Some of the case data is electronically transferred from the Immigrant Visa Information System (IVIS) used domestically by the National Visa Center (NVC) or Diversity Visa Information System (DVIS) used domestically by the Kentucky Consular Center (KCC) applications. Both systems are used to process imported data or input additional information from approved immigrant visa petitions (filed by U.S. citizens with the Department of Homeland Security's U. S. Citizenship and Immigration Service (DHS/USCIS)).

NIV- The information is collected by posts overseas from visa applications in paper form or web via CEAC (Consular Electronic Application Center) application. The CEAC data (DS Forms 260, "Immigrant Visa and Alien Registration Application" and DS 261 "Choice of Address and Agent for Immigrant Visa Applicants") as well as corroborating documentation, information from in-person interviews and fingerprints are loaded into NIV.

(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?

ACRS- The accuracy of the data is the responsibility of the customer requesting services at post. Data is collected directly from the customer and entered manually in ACRS. The data is verified by Consular Cashiers or Accountable Consular Officers (ACOs) adjudication process in checking data against data in other CA systems addressed in paragraph 3.

ACS- Data provided to ACS is verified by Department of State employees during routine processing of a service request, as well as by a Department consular officer at the time of adjudication by checking existing records and other CA systems addressed in paragraph 3.

INK- Accuracy of the information is the responsibility of the INK users. Quality checks are conducted against data in other CA systems addressed in paragraph 3, for completeness, accuracy

and for inconsistencies at every stage of processing. Administrative policies are also implemented minimizing instances of inaccurate data.

IVO- Accuracy of the information on an immigrant visa application is the responsibility of the applicant and IVO users including the Department of State (DoS) employees and contractors working domestically and overseas.

Also, locally engaged (LE) staff at post will review the initial documentation and identification forms in the hard file sent by NVC against what is loaded into the IVO application from IVIS. Any new documentation or identification forms submitted by the applicant thereafter are also reviewed and verified against data in IVO. IVO also allows DoS users to conduct and annotate the results of any local and/or governmental background and identity checks. Any changes to biographical data thereafter will alert the DoS users that new checks need to be performed. In some instances, the IVO application will detect changes and will then initiate an automated check without user intervention. The final stage of review is the interview and final adjudication conducted by a Foreign Service Officer (FSO). The FSO will verify that all information is factually correct before adjudicating the visa.

NIV-Accuracy of the information in NIV is the responsibility of the applicant filling in the paper form or entering data into CEAC. The information is verified using corroborating documentation and during in-person interviews.

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

Information is validated at the point of collection. If anything changes, it is the responsibility of the applicant to inform post or the State Department of the change so that the visa or passport remains current. If a visa or passport is reissued, the information is verified prior to reissuance.

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

The Overseas Consular Support Applications (logical business grouping) do not use commercial or publicly available information.

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

U.S.Citizens: Application forms can include: DS-60 (Change of Name Form), DS-5504 (Application for a U.S. Passport – Corrections, Name Change within 1 Year of Passport Issuance), DS-82 (Application for Passport Renewal By Mail) and DS-11 (U.S. Passport Application - for changes needed after the passport was issued 15 or more years ago). These forms that are submitted by an applicant for services contain a Privacy Act Statement which explains the reason for the information collection, how the information will be used, and potential outcome of not providing information. The consular officer at post will conduct an interview and ensure the

applicant understands the privacy notices. In addition, State Department published System of Records Notices (SORNs) include the Privacy Act Notice information.

Intending Immigrants: The application forms provide a statement that the information collected is protected by section 222(f) of the Immigration and Nationality Act of 1952, as amended (INA). INA section 222(f), 8 U.S.C. 1202(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

(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?
Information is given voluntarily by the consenting applicants, by family members or designated agent. Individuals are informed that failure to provide the information necessary to process the application may result in the application being rejected.

- If no, why are individuals not allowed to provide consent?
Click here to enter text.

(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 considered 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?

ACRS-

- To collect fees for the consular services provided (e.g., passport applications, immigrant and non-immigrant visa applications, and certain reciprocity fees) print receipts, and process refunds.

ACS-

- Financial assistance: To help service trusts, repatriation loans, and Emergency Medical and Dietary Assistance (EMDA) loans.
- Citizenship services: To assist with passport, Consular Report of Birth Abroad of a U.S. Citizen (CRBA) and loss of nationality issues.
- Other services: To track information regarding arrests, traveler enrollment and the whereabouts of U.S. citizens traveling or residing abroad.

INK-

- To supply information for name checks and other searches to verify the identity of the applicant and to help determine if the applicant for a visa or refugee status is suitable for travel to the United States. Consular and refugee personnel use the information to make a determination whether to grant visa or refugee documentation.

IVO-

- IVO is used by consular officers to record information for name checks, fingerprint matching, and other searches to verify the identity of the applicant and to help determine if the applicant is eligible for travel and immigration to the United States under applicable immigration laws and regulations. Consular officers use the information to make a determination whether to grant an Immigrant Visa (IV).
- Data can be retrieved in IVO by keyword searches such as applicant name, alien registration number, case number, and/or by barcode scanning.
- Issuance and refusal information is shared with the Department of Homeland Security (DHS) including name, date of birth, gender, and visa information, such as issuance or refusal date and visa foil number.

NIV-

- NIV is used by consular officers to record information for name checks, fingerprint matching, and other searches to verify the identity of the applicant and to help determine if the applicant is eligible for travel with a visa or boarding foil to the United States under applicable immigration laws and regulations. Consular officers use the information to make a determination whether to grant a non-immigrant 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. The OCSA systems were designed to aid the Bureau of Consular Affairs in its visa, passport, and citizen services functions. The information used by the systems is necessary to fulfill those functions.

(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?

ACRS

- Runs management reports to maintain accountability of the fee collection process and batch reports to assist in reconciliation of transactions after a specific duration. ACRS also runs daily, monthly, and yearly reports to assist post in compiling consular statistics. ACRS also generates a unique "transaction number" for each transaction.

- Customers' first and last names are also collected for all transactions and stored with a corresponding user ID of the cashier capturing information which is reconciled to generate various management reports regarding fee collections and associated statistical management data.

ACS

- Produces different types of reports, depending on the service being provided, which can then be analyzed by authorized users.

INK

- Other than error checking to ensure that all required fields are complete and the data is suitable for transmission, INK performs no internal or other automated analyses of lookout records.

IVO

- IVO generates a variety of reports for statistical and management purposes. These reports include:

    - Accountability reports that contain detailed information on a specified case and its applicants such as the Case Accountability Report.

    - Management reports that are reviewed by consular management for unusual and inexplicable activity such as: Critical Fields Changed in Case/Applicant, Cases Deleted, Potential Duplicate Cases/Applicants, Outstanding FBI Clearance Applicants and Visas Returned and Not Reissued.

    - Standard reports such as: Monthly Report of Qualified Visa Applicants Returned, Visa Authorizations, Daily Appointment Schedule, Monthly Immigrant Visa Workload, Annual Report of Active Visa Applicants and Annual Report of Inactive Visa Applicants.

    - Query reports such as: Recalled Cases, Refused Applicants, and Applicants subject to Numerical Limitations Eligible for Appointments, Applicants Not subject to Numerical Limitations Eligible for Appointments, Adjudicated Special Interest Cases, Applicants with Overcome/Waived Refusals and Namecheck Hits.

NIV

- NIV generates a variety of reports for management and accountability purposes.

(2) Does the analysis result in new information?

Only ACRS analysis results in new information: It generates a unique "transaction number" for each transaction. All other results are various compilations of data entered and no new information is generated.

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

If a transaction is given a number, the number will be stored with the record to which it applies.

(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

6. Sharing of Information

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

INTERNAL SHARING

ACRS - Information within ACRS is shared with the Office of the Executive Director, Bureau of Consular Affairs (CA/EX) in reports that describe the fees collected for the consular services provided to the applicants. This information is used to perform "End-of-Day" reconciliation tasks and management reports to maintain accountability of the fee collection process only. There is no PII shared as part of this process.

ACS - Information outlined in paragraph 3d is shared with other CA systems {Travel Document Issuance System (TDIS), American Citizens Record Query (ACRQ), Enterprise Case Assessment Service (ECAS), Consular Consolidated Database (CCD), Front End Processor (FEP), Smart Traveler Enrollment Program (STEP), Consular Consolidated Database—Consular Report of Birth Abroad (CCD-CRBA), Accountable Items (AI), Message Alert System for Citizens Overseas Tool (MASCOT), Passport Information Electronic Records System (PIERS), In Process Database (IPDB), Consular Lost and Stolen Passports (CLASP), ACS-FEP Replacement Web-Service, and Cable Messaging Systems}. All data sharing is for the purposes of completing the processing of passports, CRBAs, loans, communication with citizens overseas, and other citizenship services. Data shared is comprised of records indicating the CA services for U.S. citizens abroad have been utilized.

INK - Information outlined in paragraph 3d is shared with authorized DoS consular officers and staff who may be handling a legal, technical, procedural or law enforcement question resulting from an application for a U.S. visa. Independent Namecheck (INK) application provides the

capability to conduct namecheck queries and add lookouts to CLASS for individuals who are not applying for a visa.

IVO - IVO information outlined in paragraph 3d is shared with authorized Department of State consular officers and staff who may be adjudicating a visa case or handling a legal, technical or procedural question resulting from an application for a U.S. visa. Application case data, previous case history, adoption information, visa allocations, issuance and refusal statistics, workload statistics, and lookout data are shared internally to perform immigrant visa functions and services.

TPLS- Case number information for the Immigrant Visa Overseas (IVO) and NIV are provided to TPLS for which a fingerprint capture needs to occur. TPLS returns the fingerprint scores and indicates if capture was successful. TPLS is also used to perform fingerprint verification and to display images of previously captured fingerprints.

NIV- Information outlined in paragraph 3d is shared internally with authorized Department of State consular officers and staff who may be adjudicating visa or refugee cases or handling a legal, technical or procedural question resulting from an application for a U.S. visa or for refugee status.

Consular Lookout and Support System (CLASS). Information outlined in paragraph 3 is shared with the CLASS. Applicant name check: confirmation that no aliases are present and verification of supplied information. These data elements are used to determine entries in the CLASS database that are, or could be, the subject of the query. It is used by passport agencies, posts, and border inspection agencies to perform name checks on visa and passport applicants in support of the issuance process. Queries to CLASS contain information such as the name, data of birth, and place of birth.

Information in paragraph 3d is also shared with: the Immigrant Visa Information System (IVIS) for transfer of cases; the Diversity Immigrant Visa Information System (DVIS) for management and transfer of cases; and the Immigrant Visa Allocation Management System (IVAMS) for visa allocation management.

EXTERNAL SHARING

ACRS - Credit Card transactions are routed through the Treasury Department website, www.Pay.gov to implement the fee collection process. The transaction includes the credit card holder's name, credit card number, credit card expiration date, and payment amount to track and process fee payment collections.

ACS – does not share any direct external connections to external agencies/organizations.

INK - does not share any direct external connections to external agencies/organizations.

IVO - The IVO data: applicant biometric data (fingerprints, photo), personal data, and issuance data are shared with other federal agencies via Consular Consolidated Database (CCD) data sharing arrangements for the following purposes:

- Checking the applicant's fingerprint information against Department of Homeland Security (DHS) databases
- Establishing a record within DHS' Integrated Biometric System (IBS)
- Use at U.S. ports of entry to verify the validity of the visa
- Checking to determine if the person has a criminal record that would have an effect on visa eligibility

NIV- Information outlined in paragraph 3d, is shared with U.S. government agencies (DHS IDENT (Department of Homeland Security Automated Biometric Identification System) and the PATRIOT Act Federal Bureau of Investigation (PATRIOT FBI) fingerprinting system/KFE (Kingfisher Expansion) counterterrorism system via CCD as per statutory requirement and in accordance with confidentiality requirements under INA section 222(f). Information is also shared with Canada's Citizenship and Immigration Canada (CIC) case management system via the CCD in accordance with the Beyond the Border agreement.

(b) What information will be shared?
Information addressed in paragraph 3d is shared Internally and Externally.

(c) What is the purpose for sharing the information?
This information is included in the Internal and External Sharing sections.

(d) The information to be shared is transmitted or disclosed by what methods?
ACRS - A Memorandum of Understanding (MOU) is implemented between the data owner and the Treasury Department (www.Pay.gov) to define how the data will be used and the safeguards that are in place to protect the data. The Bureau of Consular Affairs' (CA's) agreement with Treasury regarding the use of Pay.Gov is called an "Agency Participation Agreement" or APA. CA has one agreement for all CA users, overseas and domestic. The credit card transaction information is transmitted to Pay.Gov via a Secure Socket connection.

ACS - Outside the Department, there are no direct electronic interfaces between ACS and external systems. Instead, ACS information is passed using manual processes such as file downloads, and email or FTP (File Transfer Protocol) transfers from/to secure environments. This applies to all sources of data whether internal or external to the Department. This type of sharing is accomplished by these manual, secure methods as opposed to permitting direct access to ACS. Department policy requires that ACS users follow guidelines in the sharing of PII with external

parties when using email or fax. In some cases, when possible, ACS users use their Private Key Infrastructure (PKI) token to encrypt emails for internal and external transmission of data.

INK - Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. An Interface Control Document (ICD) is used to define and disclose transmission formats via the Department of State's secure intranet, OpenNet.

IVO - Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. An Interface Control Document (ICD) is used to define and disclose transmission formats via OpenNet.

NIV- Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Data is replicated from the databases at each post to the Consular Consolidated Database (CCD). When the CCD receives fingerprint requests or visa issuance data, the CCD forwards the information to the Department's data share applications.

(e) What safeguards are in place for each internal or external sharing arrangement?
ACRS - As part of the Transport Architecture, the system uses Virtual Private Networking, encrypted tunnel constructs, Virtual Local Area Networks (LANs), and Access Control Lists (ACLs) to enforce assigned authorizations for controlling the flow of information within the system boundaries, and between interconnected systems. All communication is encrypted using Transport Layer Security (TLS) v1.2. As noted above, the database is isolated from the application. Archived data is stored in a data warehouse for reporting purposes only and is not accessible by end-users.

ACRS Standalone Version (SAV) is installed on internet-facing workstations at consular posts in order to accommodate the 50+ Consular Agencies around the world that still use a manual process of collecting fees and to allow for better accountability of the fee collection process. Since these workstations are not connected to the Department of State intranet, there is no opportunity to inherit the security controls, and therefore they require a secure and automated solution for these unique and very remote location environments.

ACS – Secure transmission methods as permitted by Department of State. An Interface Control Document (ICD) is used to define and disclose transmission formats. MOU/MOA is agreed upon between agencies.

INK - Secure transmission methods as permitted by Department of State. An Interface Control Document (ICD) is used to define and disclose transmission formats. INK shares data (for storage) only with the CCD, and the CCD does not further share it.

IVO - The Department of State systems that interface with the IVO are strictly controlled by firewall and network intrusion detection systems (NIDS) rules that limit ingress and egress to the IVO. All changes are requested from the Firewall Advisor Board (FAB) using a Universal Trouble Ticket (UTT). Each UTT is vetted by technical personnel and management prior to the change being implemented.

NIV - Security Officers determine the access level an application user (including managers) may require depending on the user's particular job function and level of clearance. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted by NIV. 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. Data is sent through encrypted lines.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
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 via Risk Management Framework (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 policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

ACRS-Does not store applicant data. Applicants would need to acquire access to information via procedures in place for the system that provided the service, such as NIV or IVO. ACRS only stores payee information (name and credit card) and only ACRS Cashiers and ACOs have the ability to enter ACRS data; applicants do not enter data in this system and have no access to view or edit this information.

ACS- The American citizen (e.g., a person who received the passport) cannot access his/her data in the system. The ACS is an internal management system used by Posts to facilitate delivery of services to citizens overseas. Information in ACS may be protected in accordance with provisions of the Privacy Act of 1974, as amended (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to the Freedom of Information Act (FOIA) or the Privacy Act, as appropriate. Procedures for notification and redress are published in the Privacy Act SORN cited in this PIA, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about existence of records, how to request access, and how to request an amendment to a record.

INK- The information in INK may be protected in accordance with provisions of the Privacy Act of 1974, as amended (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to the Freedom of Information Act (FOIA) or the Privacy Act, as appropriate. Procedures for notification and redress are published in the Privacy Act SORN cited in this PIA, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about existence of records, how to request access, and how to request an amendment to a record.

IVO – Visa applicants may access their information on-line at any time prior to submission of the application to the U.S. Consulate or Embassy. Once information is submitted, the Department will release the following information to a visa applicant upon request, in writing per guidance available to the public in 9 FAM 603.2-8:

(1) Correspondence previously sent to or given to the applicant by the post;
(2) Civil documents presented by the applicant; and

(3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

IVO information may also be protected in accordance with provisions of the Privacy Act of 1974, as amended(5 U.S.C. 552a), and individuals may request access to and/or correction of their PII pursuant to the Freedom of Information Act (FOIA) or the Privacy Act, as appropriate.

NIV- The information in NIV is considered a visa record subject to confidentiality requirements under INA 222(f). The Department will release the following information to a visa applicant upon request in writing, per guidance available to the public in 9 FAM 603.2-8:

(1) Correspondence previously sent to or given to the applicant by the post;
(2) Civil documents presented by the applicant; and
(3) Visa applications and 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.)

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

If yes, explain the procedures.

The published SORNs and Title 22 of the Code of Federal Regulations Sections 171 include procedures on how to contact an office or individual for assistance with inquiring about the existence of records pertaining to the individual, 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.

Foreign national information specifically collected in ACRS in connection with payment for a visa service is considered a visa record subject to confidentiality requirements under INA 222(f) instead of information covered by the Privacy Act. Notification is provided and adequate mechanisms to correct visa information are afforded during the course of a visa interview consistent with the applicable legal requirements of INA 222(f) and guidance available to the public in 9 FAM 603.2-8.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
(1) During their interview process.
(2) Published SORNs.
(3) Being notified by email or letter that correction is needed.

Each method contains information on how to amend records and with whom/what office to communicate as well as contact 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 to 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 (Personal Identification Verification/Common Access Card) and PIN (Personal

Identification Number) which meets the dual authentication requirement for federal system access and is required for logon. Authorized users must first authenticate to the OpenNet using their Department of State PIV Card and then authenticate to the systems listed in paragraph 3d, from Department of State configured workstations using a unique user id and password.

A system use notification ("warning banner") is displayed before logon is permitted and informs the user of system use and restrictions with every login. Users are required to read and actively click a button indicating understanding and agreement before logon can be completed.
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 Department of State Security 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 annual security/privacy training is required for all authorized users, including security training and regular refresher training. Each user annually must complete the Cyber Security Awareness Training and pass the Privacy Act PA-459 course, entitled Protecting Personally Identifiable Information. The State Department requires system users to sign the standard "Rules of Behavior Agreement" regarding the use of any computer system and the data it contains, and agree to 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(National Institutes of Standards and Technology) 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?

Administrators and users – each are restricted to the portion of data which has been approved by managers/supervisors and ISSOs.

(b) How is access to data in the system determined?

Access is determined based on requests which are approved by the supervisor and ISSO. Access is role based and user is granted only the role(s) required to perform officially assigned duties.

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

Information is documented in the System Security Plan. The Plan includes information regarding system access to data.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Other than administrators, users will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. Concerning PII, the Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN).