PRIVACY IMPACT ASSESSMENT

Automated Cash Register System (ACRS)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA:

August 2021

(b) Name of system:

Automated Cash Register System

(c) System acronym:

ACRS

(d) Bureau:

Consular Affairs (CA/CST)

(e) iMatrix Asset ID Number:

554

(f) Child systems (if applicable) iMatrix Asset ID Number:

N/A

(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒ Yes ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒ Yes ☐ No

If yes, has the privacy questionnaire in Xacta been completed?
☒ Yes ☐ No

(c) Describe the purpose of the system:

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 ACRS personnel to maintain accountability of the fee collection process.

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

ACRS collects names, partial credit card numbers, and financial institution account numbers from U.S. citizens applying for U.S. passports and other consular services. For noncitizens, ACRS collect names, partial credit card information, and financial institution account numbers to collect fees for visa applications and certain reciprocity fees.

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

- 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
- 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. 2651a (Organization of Department of State)
- 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, etc.)?

☒ Yes, provide:

SORN Name and Number: Visa Records, STATE-39
SORN publication date: June 15, 2018

SORN Name and Number: Passport Records, STATE-26
SORN publication date: March 24, 2015

SORN Name and Number: Overseas Citizen Services Records and Other Overseas Records, STATE-05
SORN publication date: September 8, 2016

☐ 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 (Consolidate as much as possible):

Schedule number: A-13-001-05a
Disposition Authority Number: N1-059-04-02, item 5a
Length of time the information is retained in the system: Destroy when 2 years old. (ref. N1-059-96-5, item 5a)
Type of information retained in the system: Passport Accounting Records – Accounting records showing money received, deposited, or refunded by Passport Services. Consular cash receipts (DS-233)

Schedule number: A-13-001-05b
Disposition Authority Number: N1-059-04-02, item 5b
Length of time the information is retained in the system: Destroy when 5 years old. (ref. N1-059-96-5, item 5b)
Type of information retained in the system: Other accounting records.

Schedule number: B-03-003-09
Disposition Authority Number: NN-169-105 item 3
Length of time the information is retained in the system: Destroy when 3 years old or 2 years after audit by GAO, whichever occurs first.
Type of information retained in the system: Record of Fees and Consular Cash Receipt

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
☐ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐ Yes ☐ No ☒ N/A

- If yes, under what authorization?

(d) How is the PII collected?

The information is collected directly from the customer who is requesting a fee-based consular service. This information is manually entered in ACRS by consular personnel providing the service and/or is automatically collected when the credit card is swiped.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Information is validated for accuracy at the point of collection. If information is not correct, collection of the fee payments cannot be executed.

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

Information is checked for currency at the point of collection. If information is not current, collection of the fees cannot be executed.

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

No commercial sources of information are used. Information is not publicly available.

(i) How was the minimization of PII in the system considered?

The PII items listed in ~~Q~~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 PII?

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

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

Yes, the information collected is used to pay fees, print receipts and to process refunds for services provided by Consular Affairs.

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

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(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

(d) If the system will use test data, will it include real PII? ☐ Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal: The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau. With that understanding, information in ACRS will be shared internally with the following CA systems: Consular Consolidated Database (CCD), Enterprise Payment Service (EPS) and the Consular Shared Tables (CST).

External: No information is transmitted directly from ACRS to other agencies.

(b) What information will be shared?

Internal: Information addressed in paragraph 3d is shared via ACRS internally within Consular Affairs.

External: N/A

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

Internal: ACRS transmits information to CCD which serves as the Consular Affairs data warehouse, providing near real-time aggregate of consular transaction activity collected in post databases that interface with external agencies.

ACRS transmits information to EPS to process collection of fees and refunds.

ACRS transmits information to CST to identify, authenticate, and validate Department users of ACRS.

External: N/A

(d) The information to be shared is transmitted or disclosed by what methods?

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

External: N/A

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

Internal: ACRS safeguards entail secure protocol connections (Hypertext Transfer Protocol (HTTP)) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior required by security controls for each major application, including ACRS. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In addition, DoS employees must have a Verification/Personal Identification Number (PIV/PIN), as well as a separate unique user ID and password to access ACRS data. Data are transmitted within DoS database to database.

External: N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, individuals are made aware of the use of the information prior to collection to pay for the required consular service.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☒ Yes ☐ No

If yes, how do record subjects grant consent?
Individuals can decline to provide the information; however, the consular services requested will not be provided.

Information is given voluntarily by the consenting applicants, the individual, family members or designated agent to provide information to collect fees for the consular

services rendered. Individuals are informed of the required payment of fees prior to providing the payment information required.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

Applicants cannot access information in ACRS as it is not a public facing system. However, applicants can acquire records contained in ACRS by following the procedures in SORNs STATE-39, Visa Records, STATE-26, Passport Records, and STATE-05 Overseas Citizen Services Records and Other Overseas Records.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒ Yes ☐ No

If yes, explain the procedures.

The published SORNs STATE-39, STATE-26, and STATE-05 include procedures on how to contact an office or individual for assistance with inquiring about the existence of records pertaining to the individual.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

(1) During the payment process itself. If the banking or credit card information does not go through to remit payment the individual is notified at that time.

(2) Published SORNs STATE-39, STATE-26 and STATE-05 provides information on procedures to obtain information and points of contact to inquire about information.

Each method contains information on how to amend records and contact information.

8. Security Controls

(a) How is all of the information in the system secured?

ACRS is secured within the Department of State intranet where risk factors are mitigated through 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 to perform official duties.

Access to ACRS information is further protected with additional access controls set at the database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer.

ACRS is 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.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Department of State ACRS users, system administrators, and database administrators have access to data in the system based on their prescribed roles and duties approved by their supervisors.

DoS ACRS User: Department of State personnel accessing ACRS consist of DoS post users and ACRS headquarters management. These users can view data, but there are restrictions as to what data each user can access. Post users are mostly limited to viewing the data for their own post. ACRS headquarters management can see and have access to all of the ACRS information.

System Administrators: Include both government and contract personnel. System administrators are responsible for the daily maintenance, establishing access control lists (ACLs) accounts and backups. System administrators have access to all data.

Database Administrators: Database Administrators (DBA) are responsible for the daily maintenance, upgrades, patch/hot fix application, back-ups, and configuration to the database. DBAs have access to application files necessary to perform daily activities to manage the databases. They can see all of the information in ACRS, but are limited to the specific roles listed above, as granted.

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

Separation of duties and least privilege access are employed; users have access to only the data that the supervisor and local Information System Security Officers (ISSOs) approve to perform official duties. Access is role-based, and the user is granted only the role(s) required to perform officially assigned duties.

Least privileges are restrictive rights/privileges or access users need for the performance of specified tasks. The Department of State works to ensure 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.

(d) How is access to data in the system determined for each role identified above?

Access to ACRS is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. The local information security officer (ISSO) ensures the access level requested (including managers), correlates to the user's particular job function, supervisor's approval, and the level of clearance in the approval of account establishment.

(e) What monitoring, recording, auditing safeguards, and other controls 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 systems 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 applications for changes to the Department of State mandated security controls. Access control lists on OpenNet servers and devices along with Department of State Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures.

In accordance with Department of State 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.

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

The ACRS System Security Plan (SSP) contains the procedures, controls and responsibilities regarding access to data in the system.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially.

The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.