Automated Cash Register System (ACRS)

1. Contact Information

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

2. System Information

(a) Date PIA was completed: August 20 2009

(b) Name of system: Automated Cash Register System (ACRS) v7.02.00

(c) System acronym: ACRS

(d) IT Asset Baseline (ITAB) number: 554

(e) System description (Briefly describe scope, purpose, and major functions):

The 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 Foreign Service Nationals) at posts world-wide 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.

(f) Reason for performing PIA:

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

(g) Explanation of modification (if applicable): ACRS reaccreditation

(h) Date of previous PIA (if applicable): January 15, 2009

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Customers' first and last names are collected for all transactions and stored with a corresponding user ID of the cashier capturing the information. Credit card information is collected for credit card transactions only. Cashier User IDs are used for records and reports as they relate to the auditing of actions taken during the use of ACRS transactions.

With respect to customer information specifically collected in connection with payment for a visa service, ACRS collects data on foreign nationals who are U.S. visa applicants. As such, the information provided by the customer is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). Because visa applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the Privacy Act.

b. How is the information collected?

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.

c. Why is the information collected and maintained?

The ACRS is currently used by the consular cashiers at posts world-wide to collect fees for consular services, print receipts, and process refunds. It also performs end of period reconciliation tasks and prints receipts and management reports used by the Accountable Consular Officer (ACO) to maintain accountability of the fee collection process. ACRS tracks fees in two currencies (local and U.S.) and prints required receipts as well as daily, monthly and yearly reports to assist post in compiling consular statistics.

d. How will the information be checked for accuracy?

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 (ACO).

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

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

- Immigration and Nationality Act (INA) of 1952 (and amendments);
- Anti-Drug Abuse Act of 1988 (P.L. 100-690);
- Immigration Act of 1990;
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA96);
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208) ;
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000);

- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56) ; and
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)

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

The ACRS security and privacy controls in place are adequate to safeguard customer privacy. ACRS utilizes numerous management, operational and technical security controls to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

ACRS is used to collect fees for the consular services provided (e.g., passport applications, immigrant visa applications, and certain reciprocity fees) print receipts, and process refunds. Information within ACRS is used to perform end of period reconciliation tasks, print receipts and management reports that are used by the Accountable Consular Officer (ACO) to maintain accountability of the fee collection process.

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

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 the information.

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

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

d. Is the system a contractor used and owned system?

ACRS is a U.S. Government owned system maintained by cleared U.S. Government employees. All employees undergo an annual security briefing and Privacy Act briefing.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Contractors involved in the design, development and maintenance of ACRS are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of ACRS hardware or software must have at least a Secret-level security clearance.

All employees (including Foreign Nationals working in Embassies and Consulates worldwide) and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by Diplomatic Security.

5. Retention

a. How long is information retained?

In the table below, the left column lists the type(s) of record and the right column lists the retention period for the type(s) of record.

Duplicate copies of consular receipts (yellow or DEPARTMENT OF STATE COPY) initialed by the servicing officer	Shred or burn after satisfactory completion of the Daily Accounting Sheet at the end of each month
A file for each month consisting of: • A copy of the Daily Accounting Sheet • The copies of Form OF-158, General Receipt • The ACRS EOD reports	One year from the end of the month
Records of cash verifications	One year from the date of the verification
Records of the periodic comparison of MRV fees	One year after the end of the previous fiscal year
A chronological file of the daily accounting sheets for each month verified by the financial management officer together with the corresponding Monthly Consular Services Report	Five years from the end of each month (Note: This retention period has increased from the previous requirement of three years.)
Written designations of Accountable Consular	Five years after termination of

Officers, subcashiers, and alternates	the designation
A file of any memoranda and supporting documents relating to fiscal irregularities and relief	Five years from the occurrence
Letter of designation as a sub-cashier Records of any changes to the amount of the cash advance	During the period of designation
A file for each month consisting of: • Original Form OF-158 receipts issued by the Class B cashier as record of receipt for the collections • Duplicate copies of ACRS end-of-day (EOD) reports 1, 2 and 3	Five years from the end of each month
Copies of memoranda confirming random quarterly cash verifications	Five years from the date of the memorandum
Copies of any memoranda relating to fiscal irregularities and relief	Five years from the occurrence

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

None. The data retained in the information system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in Chapter 13 Passport Records; and little privacy risk as a result of degradation of data quality in this information system over an extended period of time.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Information within ACRS is shared with CA/EX in reports that describe the fees collected for the CA services provided to the applicants. Information within ACRS is used to perform end-of-period reconciliation tasks and management reports to maintain accountability of the fee collection process.

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

Information from ACRS is manually entered into another system's database that is replicated to the CCD via the secured OpenNet connection for use by CA/EX. The databases are secured by passwords and are role based. The communication lines are secured by Encryption and Decryption devices as described in the FAM. Only cleared

personnel who have a "need to know" as part of their official duties have access to this information.

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

Internal sharing occurs only with authorized users, who are cleared government employees or contractors with work-related responsibilities specific to the access and use of the information. No other internal disclosures of the information within the Department of State are made.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Credit Card transactions are routed through Treasury Department website, www.Pay.gov. The transaction includes the credit card holder's Name, credit card number, credit card expiration date, payment amount. This information is transmitted to Pay.Gov via secured socket connection.

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

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. CA's agreement with Treasury regarding use of Pay.Gov is called an "Agency Participation Agreement" or APA. CA has one agreement for all CA users, overseas or domestic.

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

The risks associate with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and not using secure connections are also a serious threat to external sharing. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with external sharing and disclosure including, but not limited to formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements (SLA) annual security training, separation of duties, least privilege and personnel screening. All transactions are transmitted via secured socket to Pay.Gov. All employees (including Foreign Nationals working in Embassies and Consulates worldwide) and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by Diplomatic Security.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

STATE-05 Overseas Citizen Services Records

STATE-26 Passport Records

STATE-39 Visa Records

☐ does NOT contain information covered by the Privacy Act.

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

Individuals are made aware of the uses of the information prior to the collection. Notice is also published in the System of Records Notices STATE-5, 26 and 39.

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

Yes, an individual does have the opportunity or right to decline to provide information. However, if he or she declines, they will not be provided with the consular service they are requesting (e.g. passport).

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No, the individual cannot consent to a limited, special or specific use of the data.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

ACRS processes Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the

existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport 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.

With respect to foreign national information specifically collected in ACRS in connection with payment for a visa service, the information is considered a visa record subject to confidentiality requirements under INA 222(f) and not PII 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 40.4.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to the ACRS is limited to authorized CA staff having a need as part of their official duties for the system in the performance of their official duties. All users maintain a least a SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to ACRS requires a unique user account assigned to CA staff members who have a "need to know" in order to perform their job. Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed in order for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer prior to assigning the individual a logon. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged and audited.

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

All users are required to undergo computer security and privacy awareness training prior to being given access to the system and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Adequate controls to limit access and to regulate the behavior of authorized users are implemented in ACRS. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.) As a result of these actions, the residual risk is low.

11. Technologies

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

ACRS operates under standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or technologies.

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

No technologies commonly considered to elevate privacy risk are employed in ACRS.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates ACRS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, its 36 month authorization to operate began February 8, 2007. ACRS is going through its three years re-accreditation and re-certification.