



Privacy Impact Assessment (PIA)

**For: Automated Cash Register System
(ACRS)**

Version 08.01.01

Last Updated: June 4, 2015

1. Contact Information

A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** June 4, 2015
- b. **Name of system:** Automated Cash Register System
- 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 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.

f. **Reason for performing PIA:**

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

g. **Explanation of modification (if applicable):**

ACRS reaccreditation

h. **Date of previous PIA (if applicable):** August 20, 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?

The following PII is collected and maintained by ACRS:

- Customers' first and last names are collected and stored for all transactions.
- Credit card information is collected for credit card transactions only.

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). ACRS collects and stores only the first and last name for cashiering customers.

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?

ACRS is currently used by the consular cashiers at posts world-wide to collect fees for consular services, print receipts, and process refunds.

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 following authorities provide for the administration of the program supported by ACRS:

- 8 U.S.C. 1101 note (Immigration and Nationality Act Definitions, nonimmigrant visas)
- 8 U.S.C. 1153 note (Allocation of Immigrant Visas, Fee for Diversity Immigrant Visa Lottery)
- 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)
- 10 U.S.C. 2602(c) (Waiver of passport fee for American National Red Cross in certain circumstances)
- 22 U.S.C. 211a- (Executive Order 11295, 31 FR 10603 (1966) Authority of the Secretary of State to designate and prescribe for and on behalf of the United States rules governing the granting, issuing, and verifying of passports.)
- 22 U.S.C. 214, 214 note (Fees for Execution and Issuance of Passports, Persons excused from Payment)

- 22 U.S.C. 214a (Fees Erroneously Charged and Paid; Refund)
- 22 U.S.C. 1475e (Use of English-teaching program fees)
- 22 U.S.C. 4201 (Fees for certification of invoices)
- 22 U.S.C. 4206 (Fees for Services to American Vessels or Seamen prohibited)
- 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, 22 FR 4632 (1957) Delegation of Authority to Secretary of State to Prescribe Rates or Tariffs of Fees for Official Services at U.S. 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)
- 22 CFR Subchapter C, Part 22, Schedule of Fees for Consular Services – Department of State and Foreign Service

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.

The Oracle database is isolated from the application. Archived data is stored in an archived data warehouse for reporting purposes only and is not accessible by end-users.

The ACRS application data is protected by multiple layers of security controls including OpenNet (the Department's internal unclassified network/intranet) security, ACRS application security, Department site physical security, and management security.

The ACRS SAV (Stand Alone Version) image is initially built using the standard CA/CST overseas image. The SAV designation denotes that this installation of ACRS is not connected to OpenNet, has a local database, and does not interact with a centralized Post ACRS database. The security configuration for the ACRS SAV database is identical to the ACRS Post database.

The Windows Update and other Operating System-level system settings are configured and controlled by the Technical Team based at Post which creates the image to be deployed at a Consular Agency that has no OpenNet access. The parent Embassy/Consulate for that Agency is responsible for the software and security updates for the Agency workstations. ACRS SAV is placed onto the image after the security configuration has been applied. The setup instructions inform the Consular Agent, who does not have OpenNet access, to create a webmail account for the purpose of emailing the database "backup files" to CA/CST. There currently is no other method of sending the ACRS SAV backup that is supported by CA/CST.

To mitigate the risk posed by possession of credit card information, this system collects the minimum amount of PII necessary to process payments. However, this information is stored only

in the system and the user can only see the last four digits of the card number. The “backup file,” noted above, is encrypted using the Advanced Encryption Standard 256 (AES 256) Algorithm, as specified in Federal Information Processing Standard Publication (FIPS) 197, Advanced Encryption Standard, and is zipped up with password protection. Also, the backup file is a separate, encrypted file because it cannot be opened or viewed without an Oracle installation. The Consular Agent emails to CA/CST the encrypted “backup file” of the Oracle data, which is zipped up with password protection.

ACRS SAV can function with or without Point-of-Sale (PoS) peripherals. Payments are processed via the pay.gov server as a separate process. The Accountable Consular Officer (ACO) does not operate a PoS register. The ACO uses the ACRS application to perform daily functions. An ACO workstation does not utilize the cash register, receipt printer or pole display. The ACRS team does not have administrative rights to make any changes to the servers. The credit card transactions are transmitted over a Secure Sockets Layer (SSL), via a TLS 1.0 connection, and using 128 bit Cipher Strength Encryption. Furthermore, only individuals with a need to know can access this information. With regard to the handling of PII, ACRS SAV and ACRS Post operate identically in that the only information considered PII that they collect is customer First and Last Name.

Safeguards for ACRS SAV, listed above, relate to the security configurations of Consular Agencies as a whole, which are outside the security boundary of ACRS.

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.

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. Are contractors involved in the uses of the PII?

Yes.

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.

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. 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. ACRS implements role based controls to control access to the point of sales system that provides cash accountability by managing and monitoring consular fee receipts.

5. Retention

a. How long is information retained?

The following records schedules specifically pertain to the types of records stored in ACRS:

A-13-001-05a Passport Accounting Records - Accounting records showing money received, deposited, or refunded by Passport Services. Also includes copies of cash receipts.

Description: a. Consular cash receipts (DS-233).

Disposition: Destroy when 2 years old. (ref. N1-059-96-5, item 5a)

DispAuthNo: N1-059-04-2, item 5a

A-13-001-05b Passport Accounting Records - Accounting records showing money received, deposited, or refunded by Passport Services. Also includes copies of cash receipts.

Description: b. All other accounting records.

Disposition: Destroy when 5 years old. (ref. N1-059-96-5, item 5b)

DispAuthNo: N1-059-04-2, item 5b

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

There are no risks associated with the duration that the data is retained. The data retained in the information system about a particular individual will not extend over the allotted time in the Department of State’s Records Disposition Schedule; and there is little privacy risk as a result of degradation of data quality in this information system over an extended period of time. See 5a above for the specific records schedules and retention periods.

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 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.

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

Information from ACRS is manually entered into the U.S. Government Financial Management System (GFMS). The databases are secured by passwords and are role-based. The communication lines are secured by encryption and decryption devices as described in the Foreign Affairs Manual (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.

As noted above, the ACRS Team does not have administrative rights to make any changes to the servers or to view information stored on the servers. The information considered PII that is collected by ACRS is the customer's first and last name. Although the credit card is utilized for Consular pay services, the full credit card number is not stored; only the last four digits of the card number are stored.

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 the Treasury Department website, www.Pay.gov. The transaction includes the credit card holder's name, credit card number, credit card expiration date, and payment amount.

- 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. 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 or domestic. The credit card transaction information is transmitted to Pay.Gov via a Secure Socket connection.

As part of the Transport Architecture, the system uses Virtual Private Networking, encrypted tunnel constructs, Virtual 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 Secure Socket Layer (SSL) v3.0.

As noted above, the database is isolated from the application. Archived data is stored in an archived data warehouse for reporting purposes only and is not accessible by end-users.

ACRS SAV is installed on workstations that are Internet-facing because Consular Agencies do not have OpenNet. ACRS SAV is not part of a local network or workgroup. However, the workstation does contain the same security configuration as all CA/CST Overseas images.

Consular Agencies do not have OpenNet and do not have any sort of local network infrastructure. Consequently, in order to function, the ACRS database needs to be present on the cashiering workstation. Therefore, the main difference between ACRS Post installation and ACRS SAV installation is that the ACRS SAV database resides on the same workstation at a Consular Agency. The ACRS SAV database is identical to the ACRS Post database in security configuration and protection features.

After encrypted data is exchanged, it is transmitted via a TLS 1.0 network connection for processing.

For ACRS Standalone Version (ACRS SAV):

There are two files that are sent via email. One is the log file and the other is an Oracle dump file (the backup file). The information contained in these files consists of transaction ID information and database file references only. They DO NOT contain any PII.

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

The risks associated 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 and/or general lack of training. Transmitting privacy data in an unencrypted form (plain text) and not using secure connections are also serious threats to external sharing. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associated 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 policies, and personnel

screening. All transactions are transmitted via secured socket to Pay.Gov and only external entities with a need to know are able to access the information.

8. Notice

The ACRS system:

contains information covered by the Privacy Act.
Provide number and name of each applicable system 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, he/she will not be provided with the consular service requested (e.g. a 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 requesting access to and/or correction of records are published in

the System of Records Notices identified in paragraph 8 above, and in Title 22 of the Code of Federal Regulations Sections 171.

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) 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 40.4.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Certain exemptions to Privacy Act provisions for access to and correction of records may exist for passport and visa records on law enforcement grounds, 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.

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 at least a SECRET security clearance level in order to gain access to the Department's unclassified computer network (OpenNet). To access the system, the individual must first be an authorized user of OpenNet. 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 receiving 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 reiterates 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 ACRS users must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access users must complete annual refresher training.

All users must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice that describe the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

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 platform that is 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.

ACRS does not utilize any technology known to elevate privacy risk. The current ACRS safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls is conducted to ensure that the safeguards continue to fully function.

12. Security

a. What is the security Assessment and Authorization (A&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 on an ongoing basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) of 2002, in December 2014, the Chief Information Officer granted the Automated Cash Register System (ACRS) an Authorization to Operate for 12 months.