



## **Privacy Impact Assessment (PIA)**

**For: American Citizen Services (ACS)**

**Version 02.01.01**

**Last Updated: August 6, 2014**

## 1. Contact Information

### **Department of State Privacy Coordinator**

Department of State Privacy Coordinator  
Bureau of Administration  
Global Information Services  
Office of Information Programs and Services

## 2. System Information

- a. **Date PIA was completed:** August 6, 2014
- b. **Name of system:** American Citizen Services
- c. **System acronym:** ACS
- d. **IT Asset Baseline (ITAB) number:** # 818
- e. **System description (Briefly describe scope, purpose, and major functions):**

The American Citizen Services (ACS) system supports 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.

The types of events or issues that correspond to services supported by ACS are:

- Arrest
- Citizenship
- Death
- Financial Assistance
- Loss of Nationality
- Lost and Stolen Passport Tracking
- Property
- Registration
- Welfare/Whereabouts

Most ACS services take place entirely at overseas posts and do not require any immediate or direct Overseas Citizen Services (OCS) involvement. However, several services require OCS action or approval. These services include Loss of Nationality and

Financial Assistance. Other services such as Arrests, Welfare and Whereabouts or Death are of such immediate importance that OCS is kept informed on a real-time basis by means of emails, telegrams and the Activity Log. The Activity Log permits a post employee with the proper access and user profile to enter details into the record and attach documents regarding the Department personnel handling a case, the family member receiving assistance, and the name of an adjudication specialist if one is needed.

When a service is accessed on behalf of an individual identified by a unique subject ID, a case with a unique case ID is created and is associated to that individual. A service, with a unique service ID, is included and is automatically created in the case record. The case data also includes the Activity Log entries, Namecheck results, and proof of citizenship information. Each case may contain one or more services.

The overseas posts' ACS database provides an accessible inventory of all open services and all previous services (subject to Department of State purge procedures). All subjects, cases, and services (i.e., the entire post database) are replicated from each post through the ACS data replication server to the CCD every five minutes. OCS personnel can examine any case and all service details connected to it but can only take actions in certain types of services. The ACS Financial Assistance services require the replication of data from posts to OCS. If data replication at a post is not operational, then the post and OCS must perform the loan approval process, including assigning of a fiscal strip, disbursement and trust updates through the use of cable and/or email instead.

**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):**

N/A

**h. Date of previous PIA (if applicable):** November 23, 2009

**3. Characterization of the Information**

The ACS 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 information collected from the public contains data relevant to the service for which an individual is applying. ACS collects and maintains the following personally identifiable information (PII) elements:

- Name;
- Date and place of birth;
- Passport number;
- Social security number;
- Address;
- Nationality;
- Names of in-country contacts;
- Photograph (for passport issuance).

The primary source of the information is the individual applicant. In some cases, however, information may be collected from third parties, e.g. local authorities. In cases of the arrests or deaths of American citizens, local authorities may have provided the information.

**b. How is the information collected?**

The information is entered into the electronic ACS system by a Department of State employee working either domestically or at the relevant post abroad. The information is collected from other databases depending on the services required by the American citizen. Post employees with the access and privileges to update ACS can populate ACS with information regarding passport issues by pulling data from passport databases and the Secure Traveler Enrollment Program (STEP) database. The American citizen of record also can provide information to the post employee via face-to-face interviews after submitting proper identification.

**c. Why is the information collected and maintained?**

ACS collects and maintains relevant information about U.S. citizens for the purpose of allowing the Department of State to assist U.S. citizens while overseas. The most common uses of information in ACS is to provide financial assistance to Americans abroad, assist with citizenship services, and track any other legal information pertaining to citizens abroad (births, death, arrests).

**d. How will the information be checked for accuracy?**

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.

**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 ACS:

- 22 U.S.C. 2651a (Organization of Department of State)
- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- 22 U.S.C. 211a-218, 2651a, 2705 (2007); Executive Order 11295, August 5, 1966(Department of State Authority to Issue, Deny, Limit Passports);
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1401-1504(2014) (Nationality and Naturalization)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 8 U.S.C. 911, 1001, 1541-1546 (2013) (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)
- Title 22 of the Code of Federal Regulations, Parts 1 to 299, Foreign Relations (various parts).

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

ACS collects a substantial amount of information from the U.S. public; CA personnel collect the minimum amount of PII necessary to accomplish a specific service on behalf of a U.S. citizen. The potential privacy risk posed by ACS is mitigated and negated by comprehensive employee training, access controls and security controls.

**Protection and Mitigation Strategies**

Potential Risks	Protection and Mitigation Strategies	Control
Unauthorized Access	The system is restricted to system/ database administrators, and users. Security controls include firewalls and Network Intrusion Detection Systems (NIDS) which limit the risk of unauthorized access.	Account Management, Least Privilege
Unauthorized Browsing	The system servers monitor events on the application, detect attacks, and provide identification of unauthorized use of the system. System servers audit user actions and user activity history. The activities of all users are monitored on a continual basis. Audit logs track user name, timestamp, and	Auditable Events, Content of Audit Records

Potential Risks	Protection and Mitigation Strategies	Control
	actions taken in the application.	
Transfer to Portable/ Removable Media	Department policy prohibits the use of portable / removable media by general users. System and database administrators with specific responsibility to make backup tapes or archive data are strictly monitored and audited. Media is marked and stored in secure areas.	Media Marking, Media Storage
Unauthorized dissemination over unsecure networks	The system does not permit connections to the internet. All connections within the State Department domain are over secure networks.	Information System Connections

These risk factors are mitigated through the use of Technical, Management, and Operational security controls as part of the Department's computer security program. See the table above "Protection and Mitigation Strategies" under the "Control" column. The ACS application data is protected by multiple layers of security controls including OpenNet security, ACS application security, Department site physical security and management security.

#### 4. Uses of the Information

**a. Describe all uses of the information.**

ACS collects information for the following uses:

- Financial assistance: To help service trusts, repatriation loans, and Emergency Medical and Dietary Assistance loans (EMDA).
- 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, births, deaths, traveler enrollment and the whereabouts of U.S. citizens traveling or residing abroad.

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

The system is able to produce different types of reports, depending on the service being provided, which can then be analyzed by authorized users. Such a report, which would document the details of a specific case as it relates to an individual U.S. citizen, is the only type of new information produced by ACS.

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

ACS namecheck requests are routed via the Front End Processor (FEP) system to the Social Security Administration (SSA) to query the subject's Social Security Number against the SSA database for fraud prevention. Namecheck requests are also routed through the Consular Lookout and Support System (CLASS) database, which contains lookout ("hit") information provided from the Drug Enforcement Administration (DEA), Department of Homeland Security (DHS), the Department of Health and Human Services (HHS), the Federal Bureau of Investigation (FBI), Interpol, and the Interagency Border Inspection System (IBIS). The information provided by these agencies is used to prevent/ deter many types of illegal activities such as trafficking in humans, drugs or arms, terrorism, or flight from prosecution. Posts may find it necessary to alert and advise both the U.S. government and foreign cooperative governments of such illegal activities in order to track or apprehend suspects.

**d. Are contractors involved in the uses of the PII?**

ACS is a government-owned system. It is supported by contract employees and foreign nationals at post.

**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.**

ACS does not rely on commercial information, nor does it perform any internal analyses of the PII such as pattern matching, scoring, or data mining. For these reasons, privacy risk from the uses of the information is negligible. The residual risk to privacy is mitigated by role-based user access controls.

Contractors involved in the design, development, and maintenance of ACS are required to have a Moderate Risk Public Trust access authorization. This includes 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 ACS hardware or software must have at least a Secret-level security clearance.

All employees 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 the Bureau of Diplomatic Security (DS).

## 5. Retention

**a. How long is information retained?**

The retention period for information in ACS varies based on the type of information in question. For a comprehensive listing, see the Department of State's Records Disposition Schedules for overseas and passport records. A few examples are listed below:

- Arrest case files: destroy three years after the case is closed/abandoned or when no longer needed, whichever is later.
- Death case files: the Report of Death of an American Citizen (form OF-180) is a permanent record, to be retired to Records Service Center (RSC) three years after the case is closed and transferred to National Archives and Records Administration (NARA) when thirty years old.

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

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging. A perpetual risk with data retention is that documents will be kept indefinitely. For virtually all ACS data, however, there is a limited lifecycle established by the applicable records disposition schedules. Death case files, however, are a notable exception because the data is eventually transferred to the National Archives and Records Administration (NARA). The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of ACS throughout the lifetime of the data.

## 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?**

ACS does not share information with any internal organizations.

ACS shares information 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), and Cable Messaging Systems). All data sharing is for the purposes of completing the processing of passports, CRBAs, loans, and other citizenship services. Data shared is comprised of records indicating the CA services US citizens abroad have utilized.

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

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

Data from the ACS database is replicated via an encrypted network connection from the posts to the other Department systems located in Washington, DC. This data replication process ensures that: 1) posts around the world can access the ACS data in a timely manner, 2) requirements for data storage, backup and retrieval are met.

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 ACS.

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

The number of authorized personnel who have access to ACS data at posts around the world represents a risk due to the sheer numbers of authorized users. Many ACS users have read-only access without privileges to update or transfer information. These risks are addressed and mitigated by the stringent network and application security controls which are implemented. See the table "Protection and Mitigation Strategies" in Section 3f. Furthermore, the aforementioned personally identifiable information is shared internally within the Bureau of Consular Affairs, among cleared employees with role-based access to the data and is done so via secure transmission methods. As such, the privacy risk from internal sharing is negligible.

## **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?**

Department of State employees may share information from ACS with a variety of external organizations under the routine uses that are listed in the Overseas Citizen Services System of Records Notice (SORN). External organizations may include: U.S. and foreign law enforcement, adoption agencies, law firms, airlines/ aviation organizations, international health organizations, disaster relief organizations, and many types of non-governmental organizations. ACS permits post employees to assist American citizens and organizations in many types of situations such as a death or medical emergency, aviation disasters, missing persons, adoptions, tax payments, arrests/detentions by foreign governments, and numerous others. The information will be shared in order to fulfill the mission of ACS by facilitating the delivery of Consular Affairs services to U.S. citizens overseas.

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

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 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.

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

See the table "Protection and Mitigation Strategies" in Section 3f. The risks and mitigation strategies are similar for internal and external sharing of ACS data. In addition, there are no direct connections from ACS to external networks and the Department's Network Intrusion Detection Systems (NIDS) are state-of-the-art. Vulnerabilities and risk are also mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure any risk is addressed through the user-authorization process.

## 8. Notice

The ACS system:

- Contains information covered by the Privacy Act.  
Provide number and name of each applicable system of records.  
Passport Records – STATE-26  
Overseas Citizen Services – STATE-05

Department wide Prefatory Statement of Routine Uses at Volume 73 Federal Register No. 136, Public Notice 6290.

- Does NOT contain information covered by the Privacy Act.

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

Yes, notice is provided prior to collection of information. All forms contain a Privacy Act Statement, which indicates what information is collected, why, for what purpose the information will be routinely used, who the information will be shared with, and the consequences of not providing the data requested.

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

Yes, though the individual is advised that failure to provide certain information may result in non-provision of the requested service and/or legal penalties.

**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?**

Yes, the individual may exercise some control over release of some information to private third parties, the press or the public through the signing of a specific Privacy Act Waiver.

- 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.**

ACS complies with all Privacy Act requirements for notice at the point of collection. Therefore, this category of privacy risk is appropriately mitigated.

## **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?**

ACS contains Privacy Act-protected records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the System of Records Notices identified in paragraph 7 above, and in rules published at 22 CFR Part 171 Subpart D. The procedures inform the individual how to inquire about the existence of records pertaining to the individual, how to request access to the records, and how to request amendment of such records.

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

Because ACS is subject to the Privacy Act, formal procedures for notification and redress currently exist. Therefore, this category of privacy risk is appropriately mitigated.

## **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?**

Access to the system is limited to authorized Department of State staff having a need for the system in the performance of their official duties. All authorized government users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network.

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 for the performance of official duties. The user access agreement includes a 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 (ISSO) prior to assigning the logon.

In order to login to ACS, a user must first login to the OpenNet network in order to be authenticated to access the database. Next, the user must login to ACS in order to activate his/her role-based permissions. ACS formats the user's name as part of the

ACS User ID in order to provide direct accountability within ACS . This ensures that all actions on ACS can be traced back directly to a specific user.

User access is "role-based," determined by the employee's supervisor. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. Access to ACS is occasionally audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls. See the table "Protection and Mitigation Strategies" in Section 3f. The audit logs indicate dates and times of login and access to the ACS application. Audit logs track all activities, including browsing, and actions completed or attempted by a user.

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

All domestic and overseas ACS 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 access, users must complete annual refresher training. These resources include online training modules and short training videos. CA also offers in-person training for both small and large groups of users.

Additionally, all Department employees must take an annual Cyber Security Awareness Training course, which includes elements of privacy training.

Furthermore, users must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice that describe the expected uses 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 ACS. There remains some residual risk, however, that an employee with authorized access to the ACS application and valid accounts on both the secure network and the ACS database might misuse his/ her privileges. A user might access ACS and "browse" records for which he/she has no work-related justification. The Department's auditing controls detect all such activity and generate reports to system and database administrators who review the audit logs on a regular, usually weekly basis. The computer security controls in-place are the Department's fiercest watchdog in this case. In contrast, the only protections against manual note-taking/ copying of the information can only be accomplished by the stringent personnel and security screening conducted by the Department. Infractions on the Rules-Of-Behavior regarding PII or computer access carry significant penalties, including criminal prosecution. Therefore,

the residual privacy risk is sufficiently mitigated by the computer system and personnel security controls in place throughout the Department's networks. See the table "Protection and Mitigation Strategies" in section 3f in this document for details regarding the strategies and protections which have been implemented.

## 11. Technologies

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

ACS operates under standard, commercially-available software products residing on government-operated computing platforms not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in ACS.

### 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 ACS. The current ACS safeguards are satisfactory to protect PII. Routine monitoring, testing, and evaluation of security controls are 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 ACS 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 a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) of 2002 provision for the triennial recertification of this system, the ACS Authorization-To-Operate will expire on July 31, 2014. This document was updated as part of the triennial reauthorization of the system.