# American Citizens Services (ACS)

## 1. Contact Information

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

## 2. System Information

**(a) Date of completion of this PIA:** October 2021
**(b) Name of system:** American Citizen Services
**(c) System acronym:** ACS
**(d) Bureau:** Consular Affairs (CA/CST)
**(e) iMatrix Asset ID Number:** 818
**(f) Child systems (if applicable) and 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:**

ACS supports the Bureau of Consular Affairs (CA) in providing assistance to U.S. citizens living or traveling abroad. ACS is a collection of automated services and support functions used to record services provided to citizens, including passport assistance, tracking consular reports of birth abroad (CRBA) issuance via the Consular Consolidated Database (CCD) system, arrests, deaths, welfare/whereabouts, legal assistance, loss of nationality, financial/medical assistance, and more. This is the system where CA

employees keep contemporaneous "notes" of their actions on cases for individual U.S. citizens traveling or residing abroad.

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

ACS collects the following information on U.S. citizens:

- Names, including aliases
- Date and place of birth
- Passport number
- Social Security Number (SSN)
- Addresses
- E-mail addresses
- Phone number
- Nationality
- Name of in-country contacts
- Information on relatives
- Driver's license
- Birth certificate information
- Medical information
- Financial information
- Legal information
- Travel information, and photographs (for passport issuance) from U.S. citizens

Non-U.S. Citizen PII:

Non-U.S. Citizen PII may also be included in open fields completed by the U.S. citizen who may be affiliated with the non-U.S. Citizen overseas, e.g., name, address, email and phone.

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

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C. 2656 (Management of foreign affairs)
- 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries pursuant to the Vienna Convention on Consular Relations and providing assistance to other agencies);
- 22 U.S.C. 211a et seq. (Passport application and issuance);
- 22 U.S.C. 2705 (Documentation of citizenship);
- 8 U.S.C. 1501–1504 (Adjudication of possible loss of nationality and cancellation of U.S. passports and CRBAs);
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries);
- 22 U.S.C. 1732 (Release of citizens imprisoned by foreign governments);

- 22 U.S.C. 2671(b)(2)(A)–(B) and (d) (Evacuation assistance and repatriation loans for destitute U.S. citizens abroad);
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance);
- 22 U.S.C. 4802 (overseas evacuations);
- 22 U.S.C. 2151n–1 (Assistance to arrested citizens) (Repealed, but applicable to past records); (l) 22 U.S.C. 5503-5511 (aviation disaster response);
- 22 U.S.C. 2715 (Procedures regarding major disasters and incidents abroad affecting United States citizens);
- 22 U.S.C. 2715a (Responsibility to inform victims and their families regarding crimes against U.S. citizens abroad);
- 22 U.S.C. 2715b (Notification of next of kin of death of U.S. citizens in foreign countries);
- 22 U.S.C. 2715c (Conservation and Disposition of Estates);
- 22 U.S.C. 4195, 4196 (Official notification of death of U.S. citizens in foreign countries; transmission of inventory of effects) (22 U.S.C. 4195 repealed, but applicable to past records);
- 22 U.S.C. 2729 (State Department records of overseas deaths of United States citizens from nonnatural causes);
- 22 U.S.C. 4197 (Assistance with disposition of estates of U.S. citizens upon death in a foreign country);
- 22 U.S.C. 4198 (Bond as Administrator or Guardian; Action on Bond);
- 22 U.S.C. 4193, 4194; 22 U.S.C. 4205–4207; 46 U.S.C. 10308, 10309, 10318 (Merchant seamen protection and relief);
- 22 U.S.C. 256 (Jurisdiction of consular officers in disputes between seamen);
- 46 U.S.C. 10704–10705 (Responsibility for deceased seamen and their effects);
- 22 U.S.C. 4215, 4221 (Administration of oaths, affidavits, and other notarial acts);
- 28 U.S.C. 1740, 1741 (Authentication of documents);
- 28 U.S.C. 1781–1785 (Judicial Assistance to U.S. and foreign courts and litigants);
- 42 U.S.C. 1973ff–1973ff–6 (Overseas absentee voting);
- 42 U.S.C. 402 (Social Security benefits payments);
- 50 U.S.C. App. 453, 454, Presidential Proclamation No. 4771, July 2,1980 as amended by Presidential Proclamation 7275, February 22, 2000 (Selective Service registration), and
- 22 U.S.C. 3306 (Services to United States citizens in Taiwan).

**(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?**

☒Yes, provide:

- SORN Name and Number:
  Passport Records, STATE-26
  Overseas Citizen Services Records and Other Overseas Records, STATE-05

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  March 24, 2015
  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 Office 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-15-001-02
**Disposition Authority Number:** N1-059-09-40, item 1
**Length of time the information is retained in the system:** TEMPORARY. Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is later. NOTE: ACS case records are replicated to the Consular Consolidated Database each day for long-term recordkeeping. (Supersedes NARA Job No. NI-059-96-30, Item 1 and NA
**Type of information retained in the system:** The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts. ACS records include case level data on the following types of citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases; issuance, lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Record level data includes biographic information, case information, and case activity log.

## 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?
  26 U.S.C. 6039E - Information Concerning Resident Status
  22 U.S.C. § 2714a.(f) (Revocation or denial of passport in case of certain unpaid taxes)

**(d) How is the PII 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 and is also collected from other CA databases, depending on the services required by the American citizen. Registration data from STEP (Smart Traveler Enrolment Program) is automatically ingested into the ACS database and made available to post users. Post employees can also populate ACS with information regarding passport issues and can input information provided by the citizen during the face-to-face interviews after submitting proper identification.

**(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?**

In-person information provided to DoS personnel is verified by proper identification and other documents, depending on service requested. Also, accuracy of the information is checked during the routine processing of the service request at the time of adjudication by checking existing records and other CA systems addressed in paragraph 6(a). Information received by ACS via other CA systems listed are checked for accuracy during the submission and adjudication of the request by the applicant for the specific service requested. CA systems are updated continuously based on new information acquired and shared with other CA systems such as ACS to maintain accuracy.

**(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 source system point of collection when the applicant applies for a specific service, which is updated in ACS. Information in the source systems where the original service is requested is also checked against other CA systems for currency or any anomalies. In-person collection of information at Posts are verified by supporting documentation provided by the applicant such as passports and social security numbers, in addition to checks conducted against other CA systems to verify information. It is the responsibility of the applicant to inform the Post or the State Department of any changes to the information provided in person at the Post or following the guidance of the source system for the requested service.

**(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 Question 3(d) are the minimum necessary to perform the actions required by this system. Concerns about collecting and maintaining PII 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 maintain records of consular services assistance provided to U.S. citizens, and to assist CA personnel in adjudicating and approving requests for required services. Examples of services include:

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

**(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 PII in the ACS system is used to aid the Bureau of Consular Affairs personnel in making decisions and providing U.S. citizen requested services. The information is used

to validate information provided by the requester and to determine services necessary to fulfill the requested services.

**(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 ACS will be shared internally with the following CA systems: Travel Document Issuance System (TDIS), Consular Consolidated Database (CCD), Front End Processor (FEP), Smart Traveler Enrollment Program (STEP), Consular Affairs Applications and Data (CAD), Consular Report of Birth Abroad (CRBA), Accountable Items (AI), Passport Information Electronic Records System (PIERS), and Consular Foreign & Domestic Post Infrastructure (CFDPI).

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

**(b) What information will be shared?**

**Internal:** ACS information addressed in paragraph 3(d) is shared with and among the Consular Affairs systems listed in paragraph 6(a). The data sharing is for the purposes of providing various requested services to U. S. citizens, such as completing the processing of passports, CRBAs, loans, communication with citizens overseas, and providing of other citizenship services. Data shared is comprised of records indicating the CA services for U.S. citizens abroad.

**External**: N/A

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

**Internal:** The PII in Question 3d is shared with the CA systems in Question 6a to provide requested U.S. citizen services living or traveling abroad, such as passport assistance, consular reports of birth abroad (CRBA) validation, arrests, deaths, welfare/whereabouts, legal assistance, loss of nationality, financial/medical assistance, and other services, depending on the need.

**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:** ACS safeguards entail secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS)) 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 ACS. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In addition, DoS employees must have a Personal Identity Verification/Personal Identification Number (PIV/PIN), as well as a separate unique user identifier and password to access ACS 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 via the source system in which the service is being requested. Post employees also provide notice on the use of information during face-to-face interviews at Posts to populate ACS with information regarding passport issue services or other services required.

**(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 via the CA source system where services are being requested or, if requesting in-person, at the time of applying for a service at the Post. However, if required information is not provided, applicants are made aware that the consular services requested may not be provided.

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

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

Individuals cannot access their own data in the ACS system. ACS is an internal management system used by Posts to facilitate delivery of services to citizens overseas. The published SORNs STATE-39, Passport Records; and STATE-05, Overseas Citizen Services Records and Other Overseas Records, include procedures on how to contact an office or individual for assistance with accessing or inquiring about the existence of records pertaining to the individual.

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

☒Yes ☐No

If yes, explain the procedures.

Applicants can follow guidelines of the source system where the services are requested to modify or amend records by accessing the website where the record was established. Information can also be updated during the adjudication process for services requested which, in turn, updates ACS. The published SORNs STATE-39, Passport Records; and STATE-05, Overseas Citizen Services Records and Other Overseas Records, 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?**

Published SORNs STATE-39 and STATE-05 provide procedures and points of contact to inquire about information if corrections are required.

Applicants can also contact the post where the service was requested to inquire about procedures to correct information for a specific servicethey have requested.

Each consular process contains information on how to amend records and contact information.

## 8. Security Controls

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

ACS 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.

ACS is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable federal National Institute of Standards and Technology (NIST) 800-53 guidance and privacy overlays of management, operational, and technical controls are in place and tested as part of the continuous monitoring program. Internal access is limited to only authorized Department of State users, including cleared contractors who have a justified need to perform official duties.

### (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 ACS users, system administrators, database administrators and the security administrator, have access to data in the system based on their prescribed roles and duties approved by the supervisor.

**ACS users:** Department of State ACS users consist of DoS post users and ACS headquarters management. These users respond to U.S. citizens requiring assistance while traveling or residing abroad, and maintain records of assistance provided

**System administrators:** System administrators are responsible for daily maintenanceand establishing access control lists (ACLs) and backups. The local information system security officer (ISSO), based on supervisor approval, authorizes the establishment, activation, modification and disabling of ACS system administrator accounts.

**Database administrators:** Database Administrators (DBA) are responsible for the daily maintenance, upgrades, patch/hot fix application, back-ups, and configuration to the database.

**Security administrator:** Responsible for the maintenance and management of ACS security functions including proper activation, maintenance, and use of security features on the system.

**(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.**

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 ACS information is further protected with additional access controls set at the database level.

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 accesses users have to perform specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties. Users are uniquely identified and authenticated to access only the specified PII approved within ACS.

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

The roles identified in paragraph 8(b) as having access to ACS are based on the position and specific functions of the job. Role-based procedures are implemented which provide security measures that regulate access, viewing, and use of information for that specific role 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 an 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 and 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 ACS 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.**

There is no specific role-based training. 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.