1. Contact Information

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

2. System Information

(a) Date PIA was completed: December 18, 2008.

(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 the Bureau of Consular Affairs (CA) in providing assistance to American citizens living or traveling abroad. ACS is used to record services provided to citizens, including passport issuance, report of birth issuance, 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 abroad.

(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):

(h) Date of previous PIA (if applicable): July 2007

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?

Information collected from the public contains data relevant to the service for which an individual is applying. Commonly captured personal information includes:

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

The primary source of the information is the individual applicant. In some cases, information may be collected from third parties. Examples include arrest and death cases (local authorities).

b. How is the information collected?

The information is collected from the individual applicant. In some cases, information may be collected from third parties such as local authorities. The information is entered into the electronic ACS system by a Department of State employee working either domestically or at the relevant post abroad.

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 to assist U.S. citizens while overseas. The most common uses of information in ACS are 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 system was developed to support U.S. immigration and nationality law as defined in the following major legislation:

- Immigration and Nationality Act (INA) of 1952, and amendments;
- 22 U.S. Code of Federal Regulations (CFR) (various sections), Title 22, Foreign Relations and Intercourse; and

- 22 U.S. Code of Federal Regulations (CFR) (various sections), Title 22, Foreign Relations.

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

ACS collects only the information needed to accomplish a specific service on behalf of a U.S. citizen. As such, the potential privacy risk posed by ACS is negligible. Any risks are mitigated by the controls on access described in the response to question 10.

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 (EMDA).
- Citizenship services: To assist with passport and loss of nationality issues.
- Other services: To track information regarding arrests, births, deaths, and the whereabouts of U.S. citizens 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.

No information is obtained from other Federal agency databases.

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

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

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.

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, refer to chapter 15 of the Department of State Records Disposition Schedule. A few examples are listed below:

- Arrest case files: destroy three years after the case is closed;
- Death case files: the Report of Death of an American Citizen (Form OF-180) is a permanent record that is 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 30 years old.

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

The perpetual risk with data retention is that documents will be kept indefinitely. However, for virtually all ACS data, there is a limited lifecycle established by the records retention schedule. One noted exception is with death case files, which are later transferred to NARA. The privacy risks are mitigated through the controlled access and rules of behavior governing 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?

The Office of Overseas Citizens Services (OCS) does not share information with any internal organizations.

ACS only shares information with CA passport systems (TDIS, PIERS, CCD, TCM, IBRS, and Cable Messaging Systems). All data sharing is for the purposes of completing the processing of passports. Data shared is comprised of records indicating the CA services U.S. 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 transmitted to and from ACS is protected by the bulk encryptors inherent within OpenNet encrypting the data from posts to the CCD database. The Bureau of Consular Affairs, Office Consular Systems and Technology, has developed several

Internet based business applications. The purpose of these applications is to automate and streamline certain business processes among CA, DHS, FBI, other government agencies, non-governmental organizations (NGOs), and the public. These applications use a secure protocol (SSL) and non-secure protocol to access CA's Web Sites for the purpose of conducting consular business. The secure protocol (SSL) connection provides strong encryption (128-bit); with some applications, user/client authentication is also required.

ACS uses OpenNet TCP/IP to assist with its data transport across the network. The TCP/IP protocol suite consists of multiple layers of protocols that help insure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data, if necessary.

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 aforementioned personally identifiable information is shared solely 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 use exceptions that are listed in the Department's SORN and in OCS' SORN. This information will be shared in order to fulfill the mission of ACS by facilitating the delivery of Consular Affairs services to American citizens overseas.

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

Information is shared with external actors in accordance with the routine uses of the Overseas Citizen Services SORN (STATE-05). This type of sharing is usually done via phone, email or fax, but not through direct access to ACS.

OCS states that ACS users follow the Department guidelines in the sharing of PII with external parties when using email or fax. In some cases, when possible, ACS users use their 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.

All sensitive but unclassified information shared between ACS and external organizations is governed by the Overseas Citizens Services SORN (STATE-05).

Vulnerabilities and risk are also mitigated through the system's certification process. The 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 system:

☒ contains information covered by the Privacy Act. The information in this system is covered by STATE-05, Overseas Citizen Services Records.

☐ does NOT contain information covered by the Privacy Act.

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

All forms contain a Privacy Act Statement indicating the information 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 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 of release of some information to private third parties, the press or the public through the signing of a specific Privacy Act Waiver. When an individual U.S. citizen applies for a specific service, their record is maintained in ACS until the records retention schedule requires its destruction.

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-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 7 above and in rules published at 22 CFR 171.31. The procedures inform the individual 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.

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

Since ACS is Privacy Act-covered, formal procedures for notification and redress 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 their 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 (ISSO) prior to assigning the logon.

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.

.

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

The Office of Consular Systems and Technology provides extensive training resources for both domestic and overseas ACS users. These resources include online training modules and short training videos. CA also offers in-house 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.

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 regulate the behavior of authorized users are implemented in ACS. Therefore, this category of privacy risk is negligible.

11. Technologies

a. What technologies are used in the system that 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.

12. Security

What is the security certification and accreditation (C&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. 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 (FISMA) provision for the triennial recertification of this system, its most recent date of authorization to operate was May 25, 2007.