



Privacy Impact Assessment (PIA)

For: Action Request System (ARS)

Version 02.05.00

Last Updated: May 22, 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:** May 22, 2015

b. **Name of system:** Action Request System

c. **System acronym:** ARS

d. **IT Asset Baseline (ITAB) Number:** # 555

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

The Bureau of Consular Affairs (CA) provides computer support to domestic offices and agencies and U.S. embassies and consulates overseas utilizing the Action Request System (ARS) application. ARS is the Service Management Toolset that captures the essential information and notes for work requests. These work requests are made for:

- Information system problems, whether hardware or application oriented;
- Asset modifications, such as installing or updating hardware or software; and
- Network operations, including password requests.

In addition, CA uses ARS to capture and track passport and visa issues, such as questions regarding passport or visa applications or problems with issuing particular passports or visas. Apart from this, CA uses the software module supplied by the manufacturer to track and manage requests for assistance.

The essential purpose and function of ARS is to provide computer support and assistance to Department of State, Bureau of Consular Affairs (Department of State /CA) users. Personally Identifiable Information (PII) is rarely captured as a part of that activity. However, a service technician may need some elements of PII in order to troubleshoot a record or identify a requester's problem. Service technicians also may choose to save screenshots containing PII to the knowledge base for future reference to resolve similar problems.

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):** August 21, 2009

3. Characterization of the Information

The system ARS:

- 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?**

ARS has the potential to capture the following types of PII information: names, birthdates, Social Security Numbers or other identifying numbers, and e-mail addresses of individuals. This information is captured via screen shots from Passports, Visas or American Citizen Services (ACS) systems.

ARS also collects the name of the passport agent submitting the trouble ticket, as well as his or her work address, phone number, and e-mail address. This information is obtained from the Active Directory (AD).

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

When a Department employee is having a problem with an information system being used to support a passport function, (s)he may submit to ARS by e-mail or phone a trouble ticket. In addition to the trouble ticket, a screen shot (either requested by the help desk technician or provided by the Department employee) may contain PII elements deemed necessary to resolve the problem. The PII is originally obtained by other CA systems, including PRISM, and is used in ARS for troubleshooting purposes.

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

Any PII that is collected as part of the troubleshooting process to resolve problems with passport, visa applications or other information systems is deemed relevant to the underlying problem and is used by the CA Helpdesk only to identify and resolve the problem with the information systems.

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

ARS captures the essential information and notes for work requests. On rare occasion, ARS is populated with passport, visa or similar data. That is, a ticket may be generated for a particular issue such as a stuck record in Travel Document Issuance System (TDIS). ARS only supports Department of State/CA clients, not the general public.

ARS utilizes "drop down" menus. Options for answers are limited to selections from the menu lists. There are a few "free text" areas where information from passport, visa or similar records may be pasted or "free form" text typed. These text areas are searchable but are not checked for accuracy.

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

The following documents apply to ARS:

- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- 22 U.S.C. 211a-218, 2651a, 2705; 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 (Nationality and Naturalization)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 8 U.S.C. 911, 1001, 1541-1546 (2013) (Citizenship, passport, and visa related crimes)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 C.F.R. parts 50 and 51, Citizenship and Naturalization and Passports

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

With the collection of passport and visa data, ARS has high data element sensitivity and high data subject distinguishability. The primary risk is misuse by Department employees and contractors. Misuse of PII could result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised. Misuse could also cause administrative burdens, financial loss, loss of public reputation and public confidence, or civil liability for the Department of State.

These factors are mitigated through a very specific context of use, in that ARS uses passport and visa information only as necessary to resolve problems with the information systems.

Considering the type and amount of PII collected by ARS, the security and privacy controls in place are adequate to safeguard passport and visa applicant privacy. The collection of PII is the minimum amount necessary to fulfill the statutory purposes of the system. Any remaining privacy risks inherent in the sources or methods of collection are mitigated by appropriate privacy and security controls detailed throughout this privacy impact assessment.

Specifically, ARS is protected by Technical, Management and Operational controls in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). The ARS application data is protected by multi-level system security. The multi-level system security includes OpenNet (OpenNet is the Department's unclassified computer network) security, ARS application security, Department of State site physical security and management security. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, firewalls, intrusion detection systems, antivirus software, and audit reports. In addition, these controls are subject to rigorous testing and a formal Assessment and Authorization (A&A) process. Authorization To Operate (ATO) is granted by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually and the system is assessed and authorized every three years or sooner if significant changes are made to the existing application.

4. Uses of the Information

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

Necessary information collected in the help desk ticket as well as PII captured via screenshot within ARS is used only for the resolution of problems with information management systems reported to the CA service center.

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

The purpose of ARS is not to analyze or report on PII. PII is used only for the resolution of problems recorded in trouble tickets or in the ARS Knowledge Base. No new data is produced as part of this process.

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

The ARS system does not use any commercial information, public information, or information from other Federal agencies' databases.

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

The ARS system is owned, operated, and managed by the Bureau of Consular Affairs (CA). However, contractors may use the PII in ARS for uses described in Section 4a above. All contractors and government employees must complete the same security awareness training courses before access is granted. Contractors and government employees are also bound by the same security rules and standard operating procedures.

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.**

CA Helpdesk employees are restricted by their supervisor to limited group roles that are sufficient to perform their specific duties. ARS tracks and logs the activities of system users. It logs the employee and timestamps when the system was accessed. Training materials provided during employee orientation define the proper use and handling of privacy-related data.

All users are screened prior to their employment with the Department of State or their respective agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before given access to the OpenNet and any Consular Affairs/Office of Consular Systems and Technology (CA/CST) system, including ARS, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

It is mandatory for all Department of State employees and contractors to pass an annual computer security briefing and Privacy Act briefing from the Department of State. Contractors must also pass such briefings by the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

5. Retention

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

ARS records are presently retained indefinitely to provide an adequate trail for future problem solving and system auditing. ARS does not have an official records retention schedule to date. However, it is the intent to create one and to maintain one (1) years' worth of data on the production system and more than one (1) year on a reporting / archive database.

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 the risk of unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of information aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of ARS throughout the lifetime of the data.

In addition, the amount of PII that may be retained is limited since it is only included in "free text" comments occasionally.

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?**

ARS information is shared with other Department of State personnel for reporting of configuration management, service tickets, and general service management reporting. It is not the intent of ARS to share PII. Reports are manually exported from ARS. There are no direct connections with external systems.

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

Not applicable. ARS information is not shared with other systems.

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

Not applicable. ARS information is not shared with other systems.

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?**

Not applicable. ARS information is not shared with any external organizations.

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

Not applicable. ARS information is not shared with any external organizations.

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

Not applicable. ARS information is not shared with any external organizations.

8. Notice

The system ARS:

- contains information covered by the Privacy Act.
(visit www.state.gov/m/a/ips/c25533.htm for list of all published systems):
- STATE-56 Network User Account Records 14OCT10
 - STATE-26 Passport Records 24MAR15
 - STATE-39 Visa Records 25OCT12
- does NOT contain information covered by the Privacy Act.

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

Any PII that is recorded in ARS comes directly from a Department of State employee reporting a problem with an information management system. Department of State employees obtain the PII exclusively from passport, visa or similar records. The PRISM PIA contains information about notice provided to persons filling out passport and visa application forms.

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

ARS only processes records containing PII data that is collected by other CA systems. ARS does not collect PII data directly from applicants.

- 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?**

ARS only processes records containing PII data that is collected by other CA systems. ARS does not collect PII data directly from applicants. PII data processed by ARS is used only for processing applications and associated tasks.

- 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.**

Notice is given to individuals when they apply for passports through PRISM. ARS is not viewed by the public and contains information not obtained directly from the individual; therefore, notice is not possible. See the PIA for PRISM for more information on notice.

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?**

There are no procedures for an individual to gain access and amend information in ARS. The information in ARS is used to solve problems with passport and visa applications. Notification and redress procedures are offered at the point of passport and visa information collection on passport and visa application forms.

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

The notification and redress mechanisms offered to individuals upon the initial collection of their PII are reasonable and adequate in relation to the system's purpose and uses.

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 ARS is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform their official duties. To access the system, users must be an authorized user of the OpenNet. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform 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 a logon. The level of access for the authorized user restricts the data that may be viewed 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. ARS users are required to logon using their Active Directory user name and password. ARS then authenticates the user against Active Directory. Users do not have a separate ARS logon account.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. This is referred to as a multilayered approach. Monitoring occurs from the moment an authorized user attempts to authenticate to the network. From that point on any changes (authorized or not) that occur to data are recorded. If an issue were to arise, administrators of the system would review (audit) the logs that were collected from the time a user logged on till the time they signed off. The ARS system maintains audit trails for all entries. This will include an identification of the system user who makes a change to any record, the date/time of the change, and the fields to which changes were made

Ultimately it's very difficult to totally prevent an incident from occurring but by implementing a multilayered approach, risk can be greatly reduced.

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

Users internal to the Department of State 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.

Prior to being granted access, internal users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outlines the expected use of these systems and how the users are subject to monitoring.

- 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.**

As ARS can contain various elements of passport and visa PII, its information is sensitive and access to it must be protected. Several steps are taken to reduce residual risk related to system and information access. 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 from access is low.

11. Technologies

- a. **What technologies are used in the system that involves privacy risk?**

ARS is a customized Commercial off-the Shelf (COTS) product designed and developed by Consular Affairs' Helpdesk software services vendor. It is customized to track and provide management reports on the status of service tickets created at the Helpdesk. These are all tested, proven technologies, and they pose no additional privacy risks.

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

No added risk to privacy results from the usage of technology in ARS.

12. Security

- a. **What is the security assessment and authorization (A&A) status of the system?**

The Department of State operates ARS 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, the triennial assessment and authorization of this system was completed in June 2014. This document was updated as part of the triennial reauthorization of the system.