1. Contact Information

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

2. System Information

(a) Date PIA was completed: 08/21/09

(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) help desks for information systems use the BMC Inc. Action Request System (ARS) application. The fielded system provides support for Domestic Operations (DO) and Overseas Support (OSS) (at foreign posts). ARS is a helpdesk job ticket application 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, DO also use ARS to capture and track passport issues, such as questions regarding passport applications or problems with issuing particular passports.

OSS uses ARS to assist the Change Control Board in registering and recording changes to CA Overseas systems baselines.

Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

(g) Date of previous PIA (if applicable):

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?

ARS utilizes a free text file that may collect personal information relating to passport application inquiries such as passport numbers, social security numbers, and contact information. The sources of information are passport agents resolving passport problems. ARS also collects the name of the passport agent submitting the trouble ticket, as well as their work address, phone number, and email address. This information is obtained from the active directory.

b. How is the information collected?

The information is collected from the passport application by the passport agent. The passport agent submits a trouble ticket to ARS by email or phone.

c. Why is the information collected and maintained?

The information is collected as part of the troubleshooting process to resolve problems with passport applications.

d. How will the information be checked for accuracy?

The CA Helpdesk depends entirely upon the Passport Office for the accuracy of any passport information that is provided as part of the trouble ticket process.

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

- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports);
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure);
- 22 U.S.C. 211a–218, 2651a, 2705 (2007); Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports); and
- 8 U.S.C. 1185 (2007) (Travel Control of Citizens).

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

ARS is protected by Technical, Management and Operational controls. The ARS application data is protected by multi-level system's security. The multi-level system's security includes OpenNet security, ARS application security, DoS site physical security and management security. ARS collects the minimum amount of personally identifiable information (PII) required to satisfy the statutory purposes of the system as well as the mission of the CA Bureau. Access, authorizations and permissions are granted at a level commensurate with the user's "need to know" as part of their official job duties and database management.

4. Uses of the Information

a. Describe all uses of the information.

All data captured within ARS, including any privacy data, is used only for the resolution of problems recorded in trouble tickets.

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

No data is analyzed. All data captured within ARS, including any privacy data is used only for the resolution of problems recorded in trouble tickets. 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.

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

5. Retention

a. How long is information retained?

Records are destroyed/deleted when one year old or when no longer needed for review and analysis, whichever is later.

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

The information is only retained for the amount of time that is required to perform the System's purpose. No risks are associated with unauthorized use or exposure.

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?

Not applicable. ARS information is not shared with other 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.

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 organization.

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

Not applicable. ARS does not share with any external organization.

8. Notice

The system:

☐ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

☒ does NOT contain information covered by the Privacy Act.

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

Not applicable. Information is not collected from an individual. Information pertaining to a passport is collected by a passport agent from a passport application. Information pertaining to the passport agent is collected from the Active Directory.

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

Not applicable. See above.

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?

Not applicable. See above.

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.

Not applicable.

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 applications. Notification and redress procedures are offered at the point of passport collection.

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 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?

The ARS system verifies users through identification and authentication procedures. 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 in order for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). A username and password is created and user's access is restricted depending upon their role and "need to know." Audit logs are maintained to record system and user activity including invalid logon attempts and access to data. Information System Security Officers (ISSOs) monitor audits logs monthly for unusual activity.

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

All users are required to undergo computer security and privacy awareness training prior to being given access to OpenNet and must complete refresher training yearly in order to retain access. ARS training materials defining the proper use and handling of privacy-related data are provided during employee orientation.

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.

No residual risk is expected.

11. Technologies

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

There are no technologies associated with this system that would involve risk.

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

Not applicable.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Action Request System (ARS) was granted a 36 month full authority to operate in February 2007, which is set to expire February 28, 2010. This PIA is being done as part of its reaccreditation process.