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: August 28, 2008

(b) Name of system: Automated Biometric Identification System

(c) System acronym: ABIS

(d) IT Asset Baseline (ITAB) number: 877

(e) System description: ABIS supports enterprise-level facial-recognition matching related to the issuance of visas. The Department of State is responsible for issuing visas to foreign nationals. Inherent in this responsibility is the obligation to verify applicant identities to prevent the issuance of visas to those who pose national security threats and to prevent the issuance of visas to applicants using fraudulent aliases.

(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: Not applicable

(h) Date of previous PIA: July 20, 2007

3. Characterization of the Information

The system:

- ☐ does NOT contain PII.
- ☒ does contain PII.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The sources of information maintained in ABIS are two other Department of State systems: Consular Consolidated Database (CCD) and Electronic Diversity Visa (e-DV). The elements of PII maintained in ABIS are facial images, gender, date of birth, and an assigned identification number of each individual.

b. How is the information collected?

Information is electronically copied into ABIS from both CCD and e-DV. The information in the CCD and e-DV systems originates from the visa application process. Information collected from the applicant is used to verify the applicant's identity.

c. Why is the information collected and maintained?

The information is collected and used to verify the applicant's identity for the purpose of granting a visa.

d. How will the information be checked for accuracy?

The accuracy of the information is dependent on the quality controls established in CCD and e-DV.

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

The following authorities pertain to the Department of State program supported by ABIS:

- Immigration and Nationality Act of 1952, as amended.
- USA PATRIOT Act of 2001
- Enhanced Border Security and Visa Entry Reform Act of 2002

4. Uses of the Information

a. Describe all uses of the information.

The information is used to verify an applicant's identity in order to prevent the issuance of visas to those who pose national security threats and applicants using fraudulent aliases.

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

Scientific biometric tools are used to analyze images. Results such as positive matches are produced for analysis, and assist the Department of State to authenticate the identity of visa applicants.

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

No such external sources are used in ABIS.

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

ABIS is a government system. It is supported by contract employees, some of whom are located at contractor-owned facilities. Direct-hire U.S. government employees have the sole responsibility for visa processing. Contractors involved in the development or maintenance of ABIS 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 Privacy Act clauses. Contractor-owned facilities are annually inspected by Diplomatic Security.

5. Retention

How long is information retained?

Records can be stored up to 100 years but can be destroyed or deleted sooner if the information is no longer needed. Electronic records are deleted or destroyed in accordance with published record schedules as approved by the National Archives and Records Administration.

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 information is available only to authorized users within the Department of State for the purpose of executing their official duties related to visa processing.

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

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

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?

No information in ABIS is shared with other government agencies; and no information originating at other government agencies is electronically imported into ABIS.

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

Not applicable.

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?

ABIS does not collect personal information directly from individuals; therefore, notice at point of collection does not apply to this system.

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

ABIS does not collect personal information directly from individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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?

ABIS does not collect personal information directly from individuals; therefore, consent to limited, special, or specific uses of information by the individual do not apply to this system.

9. Notification and Redress

What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

No notification or redress procedures exist for ABIS. The accuracy of information maintained in ABIS is dependent on the two source systems, CCD and e-DV, from which the information originates.

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 employees who require access in order to perform their official duties. All authorized users maintain a security clearance level at least commensurate with public trust positions. To access ABIS, the staff member must first be an authorized user of the Department's unclassified computer network. Access to the network requires a unique user name and password assigned by Diplomatic Security. Apart from network access, the ABIS application requires a separate user account with unique user name and password. Each prospective authorized user must sign a user access agreement. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes rules of behavior where the individual's responsibility to safeguard ABIS information is described.

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

The Department of State's information technology appropriate use policy and rules of behavior for use of the Department's SBU network are the general terms under which federal employees and contractors use ABIS. In order to access ABIS, the user must first have access to the SBU network. All users of this network must complete annual computer security and privacy refresher training.

11. Technologies

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

No technologies commonly consider to elevate risk are employed

12. Security

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

In accordance with FISMA provision for the triennial recertification of this system, the most recent date of authorization to operation was January 11, 2008.