Automated Biometric Identification System (ABIS)

Privacy Impact Assessment

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**: June 8, 2011

b. **Name of system**: Automated Biometric Identification System

c. **System acronym**: ABIS

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

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

ABIS is a Commercial Off the Shelf (COTS) product developed by L-1 Identity Solutions, Inc. The ABIS system is an enterprise-level, facial-recognition matching program. The system is built on open standards and COTS hardware and can be scaled as the ABIS implementation is defined.

Computerized Face Recognition (FR) has the potential to recognize several photos of the same person in databases that are exponentially larger than those which a human could review. Additionally, automated FR can detect mathematical similarities that could be easily disguised from a subjective human viewer. The use of face recognition technology is expected to increase at the Department of Homeland Security and better facilitate the anti-fraud goals of the U.S. Department of State's existing travel document issuance processes. The ABIS FR system provides the Department's 292 consular posts and 25 passport agencies around the world additional information to use to evaluate visa and passport applications thereby lessening the possibility that a terrorist or criminal would be allowed into the United States or receive a U.S. passport under fraudulent conditions. The enterprise ABIS system contains databases of visa, passport, Watchlist Gallery and Passport Lookout Tracking System (PLOTS) images, making it the largest facial recognition system deployed in the world.

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 28, 2008

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?

ABIS stores and processes personally identifiable information (PII). The PII collected and maintained in ABIS includes photos, gender, region of residence or nationality and birth dates, as well as an assigned identification number to each record.

ABIS receives its data from visa and passport applications via the Consular Consolidated Database (CCD), an information system which is owned by the Bureau of Consular Affairs (CA/CST). The Department of Homeland Security's Terrorist Screening Center (TSC) also provides watchlist data to ABIS via CCD.

b. How is the information collected?

There is no direct end user access to the ABIS FR system. ABIS receives its data from the Consular Consolidated Database (CCD) within CA/CST. Information in CCD is extracted from both visa and passport applications and from a direct TSC feed.

c. Why is the information collected and maintained?

The Bureau of Consular Affairs (CA) is responsible for issuing visas to foreign nationals and passports to U.S. citizens. Photographic images are collected as identifying information during the application and travel document issuance process. They are also used to perform background checks on a visa or passport applicant to verify applicant identities, to prevent the issuance of travel documents to those who pose national security threats, and to prevent the issuance of travel documents to applicants using fraudulent aliases.

The USA PATRIOT Act of 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002 require a technology standard for positive identification of visa applicants. This led to the establishment of biometric identifier standards for visas and other travel documents including the use of facial recognition (FR) technology employed by ABIS. CA's success with its visa program prompted passport services to pilot FR for the purpose of identifying additional fraud in the passport application process.

In addition, passport applicant information that is collected and maintained is used by PLOTS to identify those applicants for a U.S. passport who are suspected of having felony warrants or of committing passport fraud, who owe debts to dependents or to the federal government, or who may be denied a passport or be issued only a restricted passport for certain other reasons permissible by statute.

d. How will the information be checked for accuracy?

The ABIS Facial Recognition (FR) program for visas checks the photos against two databases: the Watchlist Gallery and the visa applicant Photo Gallery. The Watchlist Gallery, which is accessed through CCD, contains photos from the National Counterterrorism Center via the Terrorist Screening Center. The Photo Gallery is a database of previous visa applicant photos, including Category One and Two Refusals.

The ABIS Facial Recognition (FR) program for passports checks the photos against three databases: the Watchlist Gallery, the passport applicant Photo Gallery, and the Passport Lookout Tracking System (PLOTS). The Watchlist Gallery, which is accessed through CCD, contains photos from the National Counterterrorism Center via the Terrorist Screening Center. The Photo Gallery is a database of previous passport applicant photos. The PLOTS gallery is a database of potential or known fraud passport applicants.

ABIS automated FR can detect mathematical similarities that could be easily disguised from a human viewer. Pattern recognition of photographic elements is coupled with biographical text.

ABIS has built-in constraints that require all fields be complete. If a record is missing information, the record is stored in a queue and reviewed prior to being added into the system. Accuracy is the responsibility of the source that originally collected the data, i.e.. the post that is submitting a photo and its identifiers for comparison.

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

ABIS was developed and modified to support U.S. immigration and nationality law as defined in the major legislation listed below:

- Immigration and Nationality Act (INA) 1952, 8 U.S.C. 1101, as amended;
- INA, 8 U.S.C. 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C 2651(a) (Organization of Department of State);
- INA, 8 U.S.C. 1202(f) (Confidential Nature of Visa Records);
- Immigration Act of 1990 (P.L. 101-649);
- Illegal Immigration Reform and Immigration Responsibility Act (IIRIRA) of 1996;
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208);
- Legal Immigration Family Equity “LIFE” Act (Part of HR 5548, 2000);
- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56);
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525); and
- Child Status Protection Act (HR 1209) 2002.

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

The Facial Recognition system currently contains over 139 million person records and is expected to grow to 210 million person records in the next year. Each year thereafter, approximately 25 million person records will be added. In addition to the face templates

(a mathematical depiction of the face image), minimal demographic data, identified in paragraph 3(a) above, is contained in the FR system. The demographics are used to filter information so searchable galleries are smaller (less than 20 million) thus improving the accuracy of the FR matches. Only demographic data that is needed is sent to the FR system with most of the applicant data remaining in the CCD as part of the visa or passport application case. The primary risk is misuse by Department employees and contractors. Misuse of PII could result in delays in processing applications. Misuse may also result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress for applicants whose PII is compromised. In addition to administrative burdens, data compromises may escalate to financial loss; loss of public reputation and public confidence; and civil liability for the Department of State.

The Department of State seeks to address these risks by minimizing the collection and transmission of PII to the smallest amount required to perform the function of Facial Recognition. Collecting this type of sensitive information results in a greater risk but this risk is mitigated in the following ways. To appropriately safeguard the information, numerous management, operational, and technical security controls are in place 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). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports.

In addition, these controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Department's Chief Information Officer (CIO). Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application. Only authorized system and database administrators with a need to know are granted access to ABIS.

4. Uses of the Information

a. Describe all uses of the information.

ABIS provides the Department of State with the ability to search millions of photographic images for duplicates or matches prior to the issuance of travel documents. All data records have a unique enrollment ID and source ID assigned to it. Records can be retrieved by using both the enrollment ID and source ID numbers.

Operational security controls for ABIS assure that there are no downloads to portable computers or portable storage devices; and no instances of computer-readable extracts of databases intended to be accessed remotely or to be physically transported outside the Department's secured physical perimeter on removable media or on portable/mobile devices.

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

ABIS provides image verification which is the one-to-one comparison of a known image against a submitted image for assessment and scoring. Verification requires prior knowledge of the individual being verified. ABIS also provides identification which is the one-to-many comparison of a captured image against a database of images. The search returns a list of potential matches, typically ranked in score for matching probability. ABIS uses analysis of photographic images to determine similarities and determine probability rankings.

Reports on the applicant and possible matching images from the database are produced for analysis. Statistical reports summarize metrics based on the number of record enrollments, searches, deletions and volumes.

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

The system does not use commercial information or publicly available information. The ABIS Facial Recognition (FR) program for **visas** checks the photos against two databases: the Watchlist Gallery and the Visa applicant Photo Gallery. The Watchlist Gallery, which is accessed through CCD, contains photos from the National Counterterrorism Center via the Terrorist Screening Center. The Photo Gallery is a database of previous visa applicant photos, including Category One and Two Refusals. Access to the information is through the CCD.

The ABIS Facial Recognition (FR) program for **passports** checks the photos against three databases: the Watchlist Gallery, the Passport applicant Photo Gallery, and the Passport Lookout Tracking System (PLOTS). The Watchlist Gallery is described above. The Photo Gallery is a database of previous passport applicant photos. The PLOTS gallery is a database of potential or known fraud passport applicants. Access to all passport and PLOTS information is through the CCD.

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

ABIS is a government-leased system. Government personnel and contractors are involved with the design, administration, and maintenance of the system. Privacy Act information clauses have been inserted into all Statements of Work and have become part of the signed contract for contractor personnel. All users are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements.

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.

Upon enrollment, ABIS converts the image provided to an algorithmic representation (template) of the features of the face used for matching. The template cannot be used to reconstruct the original face image. A number of algorithms are used so there are fourtemplates per source ID. Only the templates are stored in ABIS while the images remain in the CCD. ABIS only provides source IDs of possible matching candidates for

the search results – no images are transmitted back to the CCD. Similarly, the demographic data of date of birth, gender and region of residence or birth are associated with the template and source IDs. Before an additional search request type is added, it must be approved by the CA/CST management team as appropriate with any constraints defined.

Additionally, safeguards such as restricting access to the system, providing guidance to users as to acceptable use of the system, and restricting use of system functions to those defined by business requirements are used.

Guidance with regard to acceptable use of government systems and privacy information in particular is provided in the following ways. Security officers determine the access level needed for a particular job function and level of clearance. Contractors who support ABIS are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors who require access and install or maintain ABIS hardware and software deployed in support of the Department must have a level "Secret" security clearance. Once the highest-level background investigation required has been completed, cleared technical personnel (government and contractors) are allowed to access the server rooms housing the ABIS.

Finally, system functions are restricted in the following ways. Records cannot be added manually to ABIS. Requests to enroll (add), delete or search for a record in ABIS must be done using a CCD service. Once ABIS retrieves these requests from a CCD server, it validates the request before proceeding any further. Additionally, the system is configured in accordance with the principle of least functionality to ensure that only essential capabilities are enabled.

5. Retention

a. How long is information retained?

The retention time of the records varies depending upon the specific kind of record. Biometric data and demographics are currently active so all information is being used in the current system. As the amount of data in the system grows, all information is retained and used as part of the legacy applicant photo gallery. Completed search information is kept in a log file and archived to disk annually until needed. The search result information contains no demographic information nor photos. Search result information is only source ID numbers of matching images to the probe (applicant) source ID. Any information which needs to be deleted will come via request from the CCD.

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

All physical records containing ABIS PII are maintained in restricted areas, to which access is limited to authorized personnel. Access to ABIS files is password-protected and under the direct supervision of the System Manager. The use of ABIS does not result in the creation of hard copy records.

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 only internal organization that has access to ABIS data is the Bureau of Consular Affairs (CA). The data processed in ABIS includes photos, gender, region, and birth dates, as well as an assigned identification number to each record.

CA is responsible for issuing visas to foreign nationals and passports to U.S. citizens. Inherent in these responsibilities is the obligation to verify applicant identities, to prevent the issuance of travel documents to those who pose national security threats, and to prevent the issuance of travel documents to applicants using fraudulent aliases. ABIS results are used as a data source for this assessment at Posts abroad and domestic passport agencies.

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

Information is shared though an interconnection with the Consular Consolidated Database (CCD) by secure transmission methods permitted by internal Department policy for the handling and transmission of Sensitive But Unclassified (SBU) information. Security officers determine the access level depending on job function and level of clearance.

Access to the ABIS application is strictly limited to management and system administrators. Audit trails track and monitor usage and access. Regularly administered security and privacy training informs authorized personnel of proper handling procedures. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted.

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

The risks associated with sharing PII internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of PII by personnel can result from social engineering, phishing, abuse of elevated privileges or a

general lack of training. To combat the misuse of information, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure, including, but not limited to, annual security training, separation of duties, least privilege, personnel screening, and auditing.

Vulnerabilities and risks are mitigated through the information system certification process. Recommendations from the National Institute of Standards and Technology (NIST) are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

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?

ABIS does not share any information directly with external agencies. ABIS face recognition matching results are shared with external agencies via the CCD. U.S. Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Services (USCIS) of the Department of Homeland Security and the National Counterterrorism Center (NCTC) have access to the FR System for the purpose of enforcement of the Immigration and Nationality Act (INA) and for counterterrorism purposes.

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

ABIS does not share any information directly with external agencies. All FR matching results are provided via the CCD which has extensive user authentication, role-based users and data encryption in place. Information is shared through an interface with the CCD by secure transmission methods permitted by Department policy for the handling and transmission of Sensitive But Unclassified (SBU) information. Security officers determine the access level depending on job function and level of clearance.

Access to the ABIS application is strictly limited to management and administrators. Audit trails track and monitor usage and access. Regularly administered security and privacy training instructs authorized personnel on proper handling procedures. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted.

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

Only ABIS matching results via the CCD are shared with external agencies. The primary risk is misuse by external agencies' employees and contractors. Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress for applicants whose PII is compromised. In addition to administrative burdens, data compromises may escalate to financial loss; loss of public reputation and public confidence; and civil liability for the Department of State and other agencies.

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place 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). These controls include memorandum of understanding (MOU) arrangements with external agencies. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. An audit trail provides a record of all functions authorized users perform--or may attempt to perform.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

- Visa Records, State-39
- Passport Records, State-26

☐ 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 directly collect personal information from applicants. The identifying information and photos have been submitted by the visa or passport applicant prior to electronic transfer to ABIS. The visa application form contains a confidentiality statement indicating that visa records are confidential under INA 222(f) and can only be used for specific purposes including administering and enforcing U.S. immigration laws, and the passport application form contains a Privacy Act disclosure stating that one of the purposes for soliciting the information on the form, including the PII entered into ABIS, is to establish the identity of the applicant. Additionally, notice of the use of personal information is provided through the two SORNs mentioned above, State-39 and State-26.

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

ABIS does not directly collect personal information from applicants; therefore, opportunity and/or right to decline options do not directly apply to this system. ABIS is used to perform a Face Recognition check on all visa and passport applicants. The information and photographic images entered into ABIS are given consensually by the applicant as part of the visa or passport application. An applicant may refuse to provide the requested information, but doing so may result in the denial of the application.

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 directly collect personal information from applicants; therefore, consent to limited, special, or specific uses of information by the individual does not directly apply to this system. Applicants may decline to provide information, but they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses). The permitted uses of the information are disclosed on the visa and passport application forms.

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.

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

Notice is given to individuals as described in Section 8(a) above. ABIS relies on State-39 and State-26 and on the notice given to the visa and passport applicants who fill out the forms to mitigate the privacy risks posed by collection and use of PII.

The mechanisms for notice offered to individuals are reasonable and adequate in relation to the system's purpose and uses. The information provided by a visa applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). The information provided on the forms and in the SORN regarding visa records fully explains how the information may be used by the Department and how it is protected.

Access to ABIS is restricted to cleared, authorized Department of State employees and contractor personnel. ABIS enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

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?

Notification or redress procedures for ABIS do not lie directly with the Bureau of Consular Affairs (CA), since ABIS does not collect personal information directly from applicants. A passport containing errors can be returned for re-issuance with the correct information. When a visa application is filed, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request and this guidance is available to the public in 9 FAM 40.4:

- Correspondence previously sent to or given to the applicant by the post;
- Civil documents presented by the applicant; and

- Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted; i.e., with any remarks or notations by U.S. Government employees deleted.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 inform applicants about how to inquire about the existence of records concerning them, how to request access to their records, and how to request amendment to their records. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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

To the extent information in ABIS may be covered by the Privacy Act, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore this category of privacy risk is appropriately mitigated in ABIS.

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 ABIS is limited to authorized system and database administrators, including cleared contractors, who have a justified need for the information in order to perform official duties. Each authorized administrator must sign an access agreement before being given an administrator account.

The ABIS System Manager must sign the agreement certifying that access is needed to perform official duties. The 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 granted to ABIS restricts the data that may be viewed and the degree to which data may be modified. Administrative activity is monitored, logged, and audited. Access control lists permit categories of information and reports that are 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. The user's supervisor is the administrator for creating and modifying ABIS accounts, and grants the appropriate level of system access based on the determination

of the unit manager. Mandatory annual security/privacy training is required for all authorized users including security training and regular refresher training.

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

All users, including ABIS system and database administrators, internal to the Department, must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the CA systems. In order to retain the access, users must complete annual refresher training. In addition, all internal based users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

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 such residual risk is anticipated. Moreover, 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 deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. An audit trail provides a record of all functions authorized users perform--or may attempt to perform.

11. Technologies

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

ABIS does not employ any technology known to elevate privacy risk. All known vulnerabilities identified by the industry related to ABIS technologies have been mitigated. During the regular monitoring process, new vulnerabilities are identified and fixed.

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

Since ABIS does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be satisfactory in this application. Rigorous ongoing monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

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

The Department of State operates ABIS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. The Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function.

In accordance with the Federal Information Security Management Act (FISMA) of 2002 provision for the triennial recertification of this system, ABIS has completed the C&A process and ABIS was granted an Authority to Operate (ATO) in May 2011. This ATO will expire on May 31, 2014.