

## IBS PIA

### 1. Contact Information

**A/GIS/IPS Director**  
 Bureau of Administration  
 Global Information Services  
 Office of Information Programs and Services

### 2. System Information

- (a) **Name of system:** Integrated Biometric System  
 (b) **Bureau:** CA Bureau of Consular Affairs  
 (c) **System Acronym:** IBS  
 (d) **iMatrix Asset ID Number:** 877  
 (e) **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):**  
 N/A

### 3. General Information

- (a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**

- Yes  
 No - Contact IRM/IA at [IASolutionCenter@state.gov](mailto:IASolutionCenter@state.gov) for assistance.

- (b) **What is the security Assessment and Authorization (A&A) status of the system?**

In accordance with the Federal Information Security Management Act (FISMA) of 2002, IBS received its last Authorization to Operate in February 2014. This document was updated as part of the reauthorization of the system.

- (c) **Describe the purpose of the system:**

IBS is a Commercial off the Shelf (COTS) product developed by Morpho Trust USA, formerly Identix Incorporated. The IBS 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 IBS 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 facilitate

the anti-fraud goals of the U.S. Department of State's existing travel document issuance processes. The IBS 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 through fraud. The enterprise IBS system contains databases of visa, passport, watch list gallery and Passport Lookout Tracking System (PLOTS) images.

**(d) Describe the PII that the system collects, uses, maintains, or disseminates:**

The PII collected and maintained in IBS includes photos, gender, region of residence or nationality and birth dates, as well as an assigned identification number to each record. IBS 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' Office of Consular Systems and Technology (CA/CST). The Department of Homeland Security's Terrorist Screening Center (TSC) also provides watch list data to IBS via CCD. All data within the system is collected from CCD during enrollment of records. The PII for the enrollments is retained until the record is deleted by CCD. When a search is conducted, IBS only transmits the Source IDs of the match records back to CCD.

The following PII elements are collected and maintained by IBS:

- Photos
- Gender
- Region of residence or nationality
- Birth dates
- Assigned identification number to each record

**(e) What are the specific legal authorities and/or agreements that allow the information to be collected?**

IBS was developed and modified to support U.S. immigration and nationality law as authorized by the legal authorities listed below:

- 8 U.S.C. 1101- 1504 (Immigration and Nationality Act of 1952, as amended)
- 22 U.S.C 2651(a) (Organization of Department of State)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218 (Passports)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 C.F.R. Subchapter E, Visas
- 22 C.F.R. Subchapter F, Nationality and Passports

**(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?**

**Yes, provide:**

- **SORN Name and Number:** Passport Records – State 26 and Visa Records – State 39
- **SORN publication date :** Passport Records March 24, 2015; Visa Records October 25, 2012

 **No, explain how the information is retrieved without a personal identifier.****(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?** Yes  No**If yes, please notify the Privacy Division at [Privacy@state.gov](mailto:Privacy@state.gov).****(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?** Yes  No**(If uncertain about this question, please contact the Department's Records Officer at [records@state.gov](mailto:records@state.gov) .)****If yes provide:**

## A-13-001-16 Passport Lookout Master

Description: This on line information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have been denied passports, or those who are not entitled to the issuance of full validity passport and those whose existing files must be reviewed prior to issuance.

Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)

DispAuthNo: N1-059-04-2, item 16

## A-13-001-17 Passport Lookout Index

Description: This on-line information system provides rapid access to names in the Passport Lookout Master.

Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 27)

DispAuthNo: N1-059-04-2, item 17

## A-13-001-18 Name Check System (NC)

Description: Name Check History Master. This series contains a yearly listing of requests by Passport Services and Visa Services personnel to query the Passport and Visa Lookout systems (see schedules for A-13-001-16 and 17). The listing provides statistical data for the Bureau of Consular Affairs.

Disposition: Destroy when active agency use ceases.

DispAuthNo: N1-059-04-2, item 18

**A-14-001-20 Visa Lookout Master**

Description: This on-line series assists visa officers located at posts throughout the world in determining those individuals to whom a visa should be issued or denied. The system functions similarly to the Passport Lookout System (see items 130016 and 130017) by identifying individuals who have been denied visas.

Disposition: Destroy when active agency use ceases.

DispAuthNo: NC1-059-83-4, item 36

**A-14-001-21 Visa Lookout Index**

Description: This on-line series provides rapid access to names in the Visa Lookout Master. Searches may be by name (soundex codes), date of birth, or visa office.

Disposition: Destroy when active agency use ceases.

DispAuthNo: NC1-059-83-4, item 37

**A-14-001-24 Name Check System (NC)**

Description: Name Check History Master. This series contains a yearly listing of requests by Passport and Visa Office personnel to query the Passport and Visa Lookout systems (see items 140020 and 140021). The listing provides statistical data for the Bureau of Consular Affairs.

Disposition: Destroy when active agency use ceases.

DispAuthNo: NC1-059-83-4, item 23

**4. Characterization of the Information**

**(a) What entities below are the original sources of the information in the system? Please check all that apply.**

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

**(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?**

- Yes  No

**If yes, under what authorization?**

**(c) How is the information collected?**

IBS 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 Terrorist Screening Center (TSC) feed. See the PIA for CCD for more information on the original collection of PII.

**(d) Where is the information housed?**

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

**If you did not select “Department-owned equipment,” please specify.**

**(e) What process is used to determine if the information is accurate?**

Accuracy is the responsibility of the source that originally collected the data. The Post that submits a photo and its identifiers for comparison is a good example. IBS' built-in constraints require completion of all fields. If a record is missing information, the record is stored in a queue and reviewed prior to being added into the system. Additionally, IBS performs quality checks on each image prior to being added into the system.

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

The IBS Facial Recognition (FR) program for visas checks the photos against two galleries:

- The Visa Gallery is comprised of visa applicant photos, including Category One and Two Refusals.
- The watch list gallery is comprised of photos from the National Counterterrorism Center via the Terrorist Screening Center.

The IBS FR program for passports checks the photos against four galleries:

- The Passport Gallery is comprised of previous passport applicant photos.
- The PLOTS gallery is comprised of potential or known fraudulent passport applicants.
- The watch list gallery is comprised of photos from the National Counterterrorism Center via the Terrorist Screening Center.
- The Visa Gallery is comprised of visa applicant photos, including Category One and Two Refusals.

**(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?**

IBS data is current and constantly kept up-to-date via enrollment and un-enrollment requests routed to IBS via the Consular Consolidated Database (CCD). The IBS FR system retrieves requests from the CCD. After processing each request, the IBS FR system notifies the CCD that the request has been processed. The FR system performs automated, periodic (multiple times per hour) validations to ensure data integrity.

**(g) Does the system use information from commercial sources? Is the information publicly available?**

No. The system does not use commercial information, and the information is not publicly available.

**(h) Is notice provided to the individual prior to the collection of his or her information?**

IBS 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 IBS. 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. All passport application forms contain a Privacy Act disclosure stating that one of the purposes for soliciting the information on the form, including the PII entered into IBS, 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.

**(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?**

Yes  No

**If yes, how do individuals grant consent?**

**If no, why are individuals not allowed to provide consent?**

IBS does not directly collect personal information from applicants; therefore, opportunity and/or right to decline options do not directly apply to this system. IBS is used to perform a Face Recognition check on all visa and passport applicants. The information and photographic images entered into IBS 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.

**(j) How did privacy concerns influence the determination of what information would be collected by the system?**

The IBS system was designed so that users cannot retrieve images from the system. The PII facial scanned images are stored in a binary format that is not human readable or searchable. Therefore, the system simply cannot display facial images. IBS data is retrieved by other systems within the State Department network, processed by those systems, and displayed as facial images on other systems which are covered by separate PIAs. For example, passport photos are displayed by other systems but the data and PII are stored in binary format in IBS. The IBS system collects the minimum amount of PII required to successfully complete facial recognition processing. Since the actual images are neither stored nor searchable in IBS, there are no privacy issues related to IBS. IBS and the systems involved are subject to stringent access control and auditing due to security and privacy concerns. State Department personnel with privileged access to these systems are required to adhere to all Federal regulations regarding the protection and use of PII, and the use of the information is restricted according to job responsibilities and access control lists.

## 5. Use of information

**(a) What is/are the intended use(s) for the information?**

IBS 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. By performing this function, the Department greatly lessens the threat of issuing passports or visas to known criminal threats and fraudulent actors.

**(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?**

Yes.

**(c) Does the system analyze the information stored in it?**

Yes  No

**If yes:**

**(1) What types of methods are used to analyze the information?**

IBS 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. IBS 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. IBS uses analysis of photographic images to determine similarities and determine probability rankings.

**(2) Does the analysis result in new information?**

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.

**(3) Will the new information be placed in the individual's record?**

Yes  No

**(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?**

Yes  No

## 6. Sharing of Information

**(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.**

The only internal organization that has access to IBS data is the Bureau of Consular Affairs (CA).

IBS does not share any information directly with external agencies. FR matching results are shared with external agencies via the Consular Consolidated Database (CCD), which has

extensive user authentication, role-based users and data encryption in place. 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.

The CCD is the single interface for all incoming requests processed by IBS, as well as all outgoing results. IBS interfaces with the CCD via secure transmission methods permitted by internal Department of State 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 IBS application is strictly limited to management and 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.

**(b) What information will be shared?**

The data processed in IBS includes photos, gender, region, and birth dates, as well as an assigned identification number for each record.

**(c) What is the purpose for sharing the information?**

CA is responsible for issuing visas to foreign nationals and passports to U.S. citizens and non-U.S. citizen nationals. 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. IBS results are used as a data source for this assessment at Posts abroad and domestic passport agencies.

**(d) The information to be shared is transmitted or disclosed by what methods?**

Information is shared through 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 IBS application is strictly limited to management and system administrators. Contractor system administrators are the only individuals that have direct access to the system. 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.

**(e) What safeguards are in place for each internal or external sharing arrangement?**

IBS does not share any information directly with external agencies. All FR matching results are available through 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.

**(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?**

While IBS does not share information with external agencies directly, IBS matching results are shared with external agencies via the CCD. 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 attempt to perform.

## **7. Redress and Notification**

**(a) What procedures allow individuals to gain access to their information?**

IBS 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 Terrorist Screening Center (TSC) feed. See the PIA for CCD for more information on the original collection of PII.

**(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?**

Yes  No

**If yes, explain the procedures.**

Refer to 7(a).

**If no, explain why not.**

**(c) By what means are individuals notified of the procedures to correct their information?**

All passport application forms contain a Privacy Act disclosure stating that one of the purposes for soliciting the information on the form, including the PII entered into IBS, is to establish the identity of the applicant. Additionally, notice of the use of and changes to personal information is

provided through the two SORNs mentioned above, State-39 and State-26 in the section entitled Record Access and Amendment Procedures.

## 8. Security Controls

**(a) How is the information in the system secured?**

The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and tested and implemented those controls to ensure that the controls continue to work properly.

**(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.**

Internal access to IBS 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 IBS 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.

**(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?**

The level of access granted to IBS 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 IBS 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.

**(d) Explain the privacy training provided to authorized users of the system.**

Once CA employee users have been provided Department of State Network access, they are required to attend CA specific security awareness training. All CA users are required to take two types of security training:

- Information Security (INFOSEC) Briefing - New CA users are required to attend a site-specific security briefing within 30 days of joining the Bureau.
- OpenNet Plus Online Training - Users who have taken this online training with another Bureau within the last year do not need to take the training again until after their one-year anniversary date. All other users are required to take the training within 5 days of receiving a CA logon.

Failure to take either training course can result in revoking a user's access to the Bureau's Information Systems.

PA459 – Protecting Personally Identifiable Information (PII) is a required course for those that handle PII. The purpose of this course is to provide employees with the skills and knowledge necessary to comply with laws and regulations by identifying and protecting Personally Identifiable Information (PII). This knowledge will allow employees to do their part to mitigate risks associated with privacy and security incidents and pitfalls. Further, employees learn how to handle sensitive information and safeguard workplace data, whether physical, electronic or personal and how to identify and report security breaches.

- (e) **Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users?**

Yes  No

**If yes, please explain.**

To appropriately safeguard the information stored in IBS, 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 assessment, and authorization. Authority to operate is authorized by the Department's Chief Information Officer (CIO). Security controls are reviewed annually and the system is assessed and authorized 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 IBS.

- (f) **How were the security measures above influenced by the type of information collected?**

Even though there is no direct end user access to the IBS facial recognition (FR) system, the Department of State and the Bureau of Consular Affairs recognize that PII must be appropriately secured. Accordingly, the rigorous security controls were put in place to minimize the risk that the information stored in IBS will be compromised.

## **9. Data Access**

- (a) **Who has access to data in the system?**

Access to the IBS 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.

- (b) **How is access to data in the system determined?**

Security officers determine the access level depending on job function and level of clearance.

**(c) Are procedures, controls or responsibilities regarding access to data in the system documented?**

Yes  No

**(d) Will all users have access to all data in the system or will user access be restricted? Please explain.**

Internal access to IBS 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 IBS 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 IBS restricts the data that may be viewed and the degree to which data may be modified.

**(e) What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?**

The level of access granted to IBS 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 IBS 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.