PRIVACY IMPACT ASSESSMENT

INTEGRATED BIOMETRIC SYSTEM

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: November 2021
(b) Name of system: Integrated Biometric System
(c) System acronym: IBS
(d) Bureau: CA/CST
(e) iMatrix Asset ID Number: 877
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

☐ New system
☐ Significant modification to an existing system
☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The Integrated Biometric System (IBS) supports the Bureau of Consular Affairs mission requirements for issuing visas to foreign nationals and passports to U.S. citizens. The IBS is an enterprise-level, facial-recognition matching service.

The IBS 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. Face recognition technology is used to facilitate anti-fraud goals of the U.S. Department of State's existing travel document issuance processes. IBS provides the Department of State the ability to add, delete, and search millions of photographic images for the same person prior to the issuance of travel documents.

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 (CA/CST). CCD serves as the CA data warehouse that holds current and archived data from the Bureau of Consular Affairs (CA) domestic and post databases. The Department of Homeland Security's Terrorist Screening Center (TSC) also provides watch list images to IBS via CCD. All data within the IBS system is collected from CCD.

IBS supports the implementation of the State Department's visa and passport programs. The information is used to support visa and passport application submission, processing, and approval/denial decisions by performing photo checks to determine validation or to flag any inconsistencies.

IBS can 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.

The IBS FR system provides the Department's consular posts and passport agencies around the world additional information to use to evaluate visa and passport applications, thereby lessening the possibility of a terrorist or criminal being allowed into the United States or receiving a U.S. passport through fraud. The enterprise IBS contains databases of visa, passport, watch list gallery and the Passport Lookout Tracking System (PLOTS) templates, which are mathematical representations of images .The IBS images are retrieved from the Consular Consolidated Database (CCD) to conduct facial recognition screening. The images are not stored in IBS.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

Photos, gender, region of residence or nationality, birth dates.

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

- 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, etc.)?

☐Yes, provide:

- SORN Name and Number:

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

☒No, explain how the information is retrieved without a personal identifier.

Images are encoded into biometric templates which are mathematical representations of the image. When a probe is presented for search, the probe template is searched against the millions of templates looking for similarities. The templates are randomly assigned identification (id) numbers which are used to track records in IBS candidate lists. The random ids in IBS are assigned in the CCD system and are not affiliated with PII for searches, but instead a biometric mathematical image.

(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 Office at 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.)

If yes provide (Consolidate as much as possible):

- Schedule number: Submitted to NARA:
  Lookout, Namecheck and Case Management Records

- Disposition Authority Number:
  DAA-0059-2020-0017-0008

- Length of time the information is retained in the system:
  Temporary. Destroy when active agency use ceases but not to exceed 100 years.

- Type of information retained in the system:

Records used to determine those individuals to whom a passport or visa should be issued or denied, who have been denied passports or visa, are not entitled to the issuance of full validity passport or visa, or whose existing files must be reviewed prior to issuance; lookout index providing rapid access to names in lookout master file; name check history master file containing yearly listing of requests by Passport and Visa Services; and data extracted from case files requiring review and processing and used to track the life-cycle of each case.

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) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

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

☐Yes ☐No ☒N/A No SSNs are collected.

- If yes, under what authorization?

(d) How is the PII collected?

IBS receives its data directly 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.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Accuracy is the responsibility of the source that originally collected the data, e.g., the post that submits a photo and its identifiers (numbers assigned to images within the CCD) for comparison. 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 adding it to the system.

The IBS Facial Recognition 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 FR program for visas checks against against two Galleries:

- The Visa Gallery is comprised of visa applicant biometric templates from photos including Category One and Two Refusals.

- The Watch List gallery is comprised of biometric templates of photos from the National Counterterrorism Center via the Terrorist Screening Center.

The IBS FR program for passports checks against four galleries:

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

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

IBS data are 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.

(h) 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

(i) How was the minimization of PII in the system considered?

The PII listed in 3d are the minimum necessary to perform the actions required by this system. Concerns about collecting and maintain PII include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were assessed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

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

The PII collected enables the IBS 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 PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes – The information collected supports the implementation of the State Department's visa and passport programs. The information is used to support visa and passport application submission, processing, and approval/denial decisions by performing photo checks to determine validation or flag any inconsistencies.

(c) Does the system analyze the PII stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the PII?
IBS provides image verification, which is the one-to-one comparison of a known image against a submitted image for assessment and scoring. 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 biometric templates created from 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 which can produce new information. 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

(d) If the system will use test data, will it include real PII?
☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal:
The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in IBS will be shared internally with the Consular Consolidated Database (CCD) system.

External:
IBS does not share any information directly with external agencies. FR matching results are shared with external agencies via the Consular Consolidated Database (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 data via the CCD for the purpose of enforcement of the Immigration and Nationality Act (INA) and for counterterrorism purposes. CCD is outside the IBS boundary.

(b) What information will be shared?

Internal:
Information shared with the CCD system includes photos, gender information, region of residence or nationality, and birth dates, as well as an assigned identification number for each record as described in paragraph 3d.

External:
N/A

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

Internal:
The Information is shared to conduct and provide FR assessment information to the Department's consular posts and passport agencies, and external agencies for use in evaluating visa and passport applications, thereby lessening the possibility of a terrorist or criminals being allowed into the United States or receiving a U.S. passport through fraud.

External:
N/A

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

Internal:
The information is shared by secured internal database to database connections with the Consular Affairs Consular Consolidated Database (CCD) system. Information is shared database to database by Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information. Electronic files are PIV/PIN or password protected and access is controlled by system managers. Audit trails track and monitor usage and access of systems that reside on the Department's secure intranet network, OpenNet. Information shared externally is exchanged through the CCD and utilizes connection security and service agreements.

External:
N/A

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

Internal:
Safeguards in place for internal sharing arrangements include secure transmission methods such as data encryption using Hypertext Transfer Protocol Secure (HTTPS) and secure communications using Transport Layer Security and multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers. These safeguards are permitted by internal Department of State policies for handling and transmission of sensitive but unclassified (SBU) information.

External:
N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

IBS does not collect information directly from applicants. IBS information is obtained from the CCD system. When the collection of information by the source system which populates CCD involves potential PII collected on U.S. citizens, there is a Privacy Act statement displayed on the form in which the applicant is seeking a consular service, such as a passport.

Non-citizen data is subject to the requirements of the Immigration and Nationality Act (INA)222(f) which are stated on the collection site of the source system collecting the PII.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

IBS does not collect information from the public, but instead pulls information from the CA CCD system to conduct FR assessments. Consent is acquired via the source systems in which the information is originally obtained when applicants request consular services. The identifying information and photos have been submitted by the visa or passport applicant process prior to the electronic transfer to IBS.

(c) What procedures allow record subjects to gain access to their information?

IBS receives its data from the Consular Consolidated Database (CCD) system within CA/CST. Information in CCD is extracted from both visa and passport application processes. The individual would need to follow processes outlined by the source system and SORNs STATE-26 and STATE 39 to request access to their information.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals must follow processes of the source system CCD to request correction of information. Notice to change personal information is provided at the site where applicants apply for the specific services. Individuals can also follow the record access procedures in SORNs STATE-26 and STATE-39 regarding points of contact to inquire about their information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

The IBS does not collect PII from individuals. IBS pulls PII information from the CCD database, which resides outside the IBS system boundary. Notifications to correct records are provided via the adjudication process of the source system collecting the information from the individual requesting the specific service and housed in CCD. Individuals can also follow procedures in SORNS STATE-26 and STATE-39 regarding points of contacts listed for individuals wanting to correct their information.

8. Security Controls

(a) How is all of the information in the system secured?

The system is secured within the Department of State intranet where risk factors are mitigated using defense in depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information to perform official duties.

Access to applications is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user’s supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

Systems are configured according to the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Access to IBS is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. System administrators, database administrators and Department of State employees have access to the system to aid in processing passport and visa applications and to perform system and database maintenance.

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

Access to IBS is role-based and restricted according to approved job responsibilities and requires managerial concurrence. Supervisors and local Information System Security Officers (ISSO) determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function, manager's approval, and level of clearance.

(d) How is access to data in the system determined for each role identified above?

In accordance with Department of State policy, IBS employs the concept of least privilege for each user by allowing only authorized access to information in the system necessary to accomplish assigned job and tasks. IBS employs the concept of least privilege to users by allowing only authorized access to information systems and information systems resources necessary to accomplish assigned tasks as approved by the manager. All roles have been analyzed to determine the specific data set and corresponding functions that will be required in accordance with the person's job and level of security approved by the supervisor. Accordingly, when a user or service account is added to a particular database role, access is limited to only the data and functions allotted.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

The IBS audit service on its servers captures many logs, access attempts, an all actions exceeding the DoS requirements. Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information in IBS. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system.

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

☒Yes ☐No

The IBS Security Plan includes information and procedures regarding access to data in IBS.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information bienniallyThe State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.