PRIVACY IMPACT ASSESSMENT

Management Information System (MIS)

1. Contact Information

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

2. System Information

(a) Name of system: Management Information System
(b) System acronym: MIS
(c) Bureau: Consular Affairs
(d) iMatrix Asset ID Number: 724
(e) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(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):

3. Purpose

(a) Describe the purpose of the system.

The Management Information System (MIS) is a web-based reporting tool that tracks predefined productivity statistics of U.S. passport agencies. The MIS provides passport system managers the ability to manage passport productivity operations by providing capabilities to query databases and generate a wide number of reports on passport information and statuses specific to any passport agency within the United States. This information includes weekly and monthly workloads on passport production, book inventory, agency hiring summaries, and statistics regarding agency staff. The MIS streamlines the data entry required to produce reports on the management of passports. It is designed to connect to other CA databases to acquire data necessary for reporting on passports, including the ability to assign controlled access to view, run, and schedule reports. The MIS helps to manage report cycles through the implementation of a report approval hierarchy by alerting users of due dates, enforcing established submission deadlines, and enabling communication of important messages between Passport Agencies and Field Operations. Implementation of MIS, a web application, provides easy access to obtain and analyze information from the Field Operations. This custom web-based report management and distribution system provides the ability for authorized
users to 1) collect data from multiple sources, 2) generate a wide variety of critical reports, and 3) conduct key analysis tasks.

(b) Personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

U.S. Persons PII:
- Name
- Date of Birth
- Place of Birth
- Social Security Number (SSN)

Department of State employee information:
- Name
- Title
- Business Phone Number
- Business Email Address
- Passport Agency

(c) How is the PII above collected?

The MIS receives PII as a data transfer from the CA systems Travel Document Issuance System (TDIS) and the Passport Lookout Tracking System (PLOTS). The applicant completes the required form for a passport or passport renewal either through a paper form or online via a CA source system, where information is uploaded, and transmitted via TDIS and PLOTS to MIS.

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

The PII is used to generate management reports on information specific to passport agencies and personnel within the United States depicting passport workload statistics and performance. This information includes weekly and monthly workloads, book inventory, agency hiring summaries, and statistics regarding agency staff and the processing of passports.

(e) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

☒ Yes ☐ No

If no, please explain:

4. Authorities and Records

(a) What are the specific legal authorities and/or agreements that allow the information to be collected?
- 22 U.S.C. 2651a (Organization of Department of State)
Executive Order 11295, August 5, 1966, 31 FR 10603
31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
22 C.F.R. Subchapter F (Nationality and Passports)
26 U.S.C. 6039E (Information Concerning Resident Status)
Executive Order 9397, November 22, 1943 (Numbering system for federal accounts relating to individual persons)
Executive Order 13478, November 18, 2008 (Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers)
22 U.S.C. § 2714a. (f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(b) If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security number.

26 U.S.C. 6039E (Information Concerning Resident Status)
22 U.S.C. § 2714a. (f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)?

☑ Yes, please indicate relevant System of Records Notice (SORN) below.

- SORN Name and Number:
  STATE-26 Passport Records 03/24/2015

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

(d) 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.

(e) List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system?

- Disposition Authority Number(s): Pending approval

5. Data Sources, Quality, and Integrity
(a) What categories of individuals below originally provide the PII in the system? Please check all that apply.

☒ Members of the public (U.S. persons which includes U.S. citizens or LPRs)
☒ U.S. government employees/contractor employees
☐ Other (people who are not U.S. citizens or LPRs)

(b) Do the individuals listed in 5(a) provide PII on individuals other than themselves? Please check all that apply.

☐ Members of the public
☐ U.S. government employees/contractor employees
☐ Other
☒ N/A

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

All PII in the MIS is transferred from TDIS and PLOTS. PII in these systems are checked for accuracy against submitted documentation, administrative procedures and other CA systems prior to information being transmitted to the MIS.

(d) What steps or procedures are taken to ensure the PII remains current?

PII processed by the MIS is retrieved from the source CA systems TDIS and PLOTS. Currency is the responsibility of the applicants completing the application for specific services via the CA systems. Applicants can modify or amend records by following procedures of the website where the record was established. Information can also be updated during the adjudication process for services requested, where updates to the source systems takes place prior to information being transmitted to the MIS.

(e) Was the minimization of PII in the system considered?

☒ Yes  ☐ No

If no, please explain

(f) Does the system use information, including PII, from commercial sources?

☐ Yes  ☒ No

If yes, please list the commercial sources.

(g) Is the information, including PII, collected from publicly available sources?

☐ Yes  ☒ No
If yes, please list the publicly available sources.

(h) Does the system analyze the PII stored in it?

☐ Yes  ☒ No

If yes:

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

(2) Does the analysis result in new information?

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

(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?

(i) If the system will use test data, will it include real PII?

☐ Yes  ☐ No  ☒ N/A - this system does not use test data

If yes, please provide additional details

6. Redress and Notification

(a) Explain whether a notice is provided to the record subject at the point of collection of their information.

Notice is not provided in the MIS since it is not the original point of collection. The information is obtained from the TDIS and PLOTS. When the collection of information by the source system involves PII collected on U.S. persons, there is a Privacy Act Statement displayed on the form in which the applicant is seeking a consular service, such as a passport. The source system provides notice to U.S. persons when collecting PII for CA passport services.

(b) Are opportunities available for record subjects to decline to provide the PII?

☐ Yes  ☒ No

Please explain why not.

Record subject’s information in the MIS is obtained from TDIS and PLOTS and is not
collected directly from the record subject. Consent is acquired via the CA source systems where the applicant applies for services.

(c) Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?

☐ Yes ☒ No

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

Record subjects do not have access to the MIS, nor is data collected by the MIS directly from the record subject. The Department’s Privacy Act practices allows for record subjects to gain access to their information by contacting the Department’s Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-26.

(e) Are procedures in place to allow a record subject to correct or amend their information?

☐ Yes ☒ No

Explain why record subjects are not able to correct their information.

Record subjects do not have access to the MIS, nor is data collected by MIS directly from the record subject. If corrections are needed, individuals can make changes to correct information via the source system of origin where the information is captured. Individuals can also follow the record access procedures in SORN STATE-26, which include procedures on how to contact an office for assistance in addressing inaccurate information.

7. Sharing of PII

(a) To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.

<table>
<thead>
<tr>
<th>Internal (within the Department)</th>
<th>External (outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

(b) For each of the entities in 7a, list the PII from 3d that will be transmitted.

<table>
<thead>
<tr>
<th>Internal (within the Department)</th>
<th>External (outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

(c) For each of the entities in 7a, what is the purpose for transmitting the information?
(d) For each of the entities in 7a, list the methods by which the information will be transmitted.

<table>
<thead>
<tr>
<th>Internal (within the Department)</th>
<th>External (outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

(e) For each of the entities in 7a, what safeguards are in place for each method of internal or external transmission?

<table>
<thead>
<tr>
<th>Internal (within the Department)</th>
<th>External (outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

8. Security

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

The information in MIS is secured within the Department of State (Department) intranet which mitigates risk factors through defense-in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. The MIS is configured according to the Department’s Security Configuration Guides to optimize security while still providing functionality. 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. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need to perform official duties.

(b) 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.

(c) Below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.
Access to MIS is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. Department of State MIS users, system and report administrators and agency administrators, have access to MIS based on prescribed roles to conduct required business and assigned roles to support the management and execution of the passport program.

(d) After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.

For access to MIS, management approval is required; approval is based on position and need to know. Local Information System Security Officers (ISSOs) and system administrators are responsible for managing the local systems accounts as approved by the supervisor. This local responsibility includes establishing, activating, monitoring, modifying, reviewing, disabling, and removing accounts due to change in position or personnel. Accounts are reviewed and validated every 90 days by the supervisor and local ISSO for compliance with account management control requirements.

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

☒ Yes ☐ No

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

☒ Yes ☐ No

(g) Privacy Related Training Certification

- Do all OpenNet users of this system take PA-318 Protecting Personally Identifiable Information biennially?

☒ Yes ☐ No

- Do all OpenNet users of this system take PS800 Cybersecurity Awareness Training annually?

☒ Yes ☐ No

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

☒ Yes ☐ No

Please list the related trainings here: