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: March 1, 2012

(b) Name of system: Management Information System

(c) System acronym: MIS

(d) IT Asset Baseline (ITAB) number: 724

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

MIS is a web-based reporting tool that tracks predefined productivity statistics of U.S. passport agencies. It provides Passport System management the ability to query the Travel Document Issuance System (TDIS) databases for information specific to any passport agency within the United States. The information includes weekly and monthly workloads, book inventory, agency hiring summaries, and statistics regarding agency staff.

(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):

(h) Date of previous PIA (if applicable): April 9, 2009

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?

MIS collects and maintains the following personally identifiable information (PII) elements when passport agencies and Department of State employees use the MIS system to produce a variety of management reports: name of individuals, social security number, address/phone or similar information, and email address of individuals who are applying for passports.

The source of information is from the Travel Document Issuance System (TDIS) and Human Resource (HR) records at each passport agency. Sources of the information are passport agencies, other Department of State computer systems, and a variety of databases that acquire the data necessary for reporting. Report functionality includes the ability to assign controlled access to view, run, and schedule reports. MIS manages report cycles through the implementation of a report approval hierarchy which alerts users of due dates, enforces established submission deadlines, and broadens communication of important messages between agencies and field operations. It includes a variety of features and components for users with differing levels of system privileges.

- Passport Workload
- Labor & Staffing statistics
- Passport Employee Productivity
- Agency Deposit Information
- Product Inventory and Internal Controls
- PLOTS Case Tracking
- PIERS Privacy and User Activity

b. How is the information collected?

Information is gathered from the Travel Document Issuance System (TDIS) system from the passport agencies and centers regarding their respective employees by name, personal identity and authentication.

c. Why is the information collected and maintained?

The information on the employees is collected for the Department management to help them in their decision-making effort when conducting cost/benefit analyses, security reviews, enforcing established submission deadlines and enabling communication of important messages, passport workload, labor and staffing statistics, passport employee productivity, agency deposit information, and product inventory and internal controls for each passport agency and center on an individual basis.

d. How will the information be checked for accuracy?

Data for MIS is from the TDIS system. MIS is totally dependent upon the validity, safeguards and accuracy of the TDIS system. Manually entered data is reviewed for accuracy both by passport agency and center administrators, and passport personnel at SA-29.

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

The following authorities provide for the administration of the program supported by MIS:

- 8 U.S.C. 1401-1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality use of U.S. Passports)
- 18 U.S.C. 911, 1001, 1541-1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, 2651a, 2705 (2007) (Executive Order 11295, August 5, 1996)

- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)

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

MIS (using TDIS as a source) collects the minimum amount of personally identifiable information necessary to function as a reporting tool that tracks predefined productivity statistics of U.S. passport agencies. With the collection of passport data, MIS has a high data element sensitivity and high data subject distinguishability. The primary risk is misuse by Department employees and contractors. Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised, and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

These risk factors are mitigated through the use of Technical, Management, and Operational security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. 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. If these controls are not implemented, non-government employees could engage in criminal activities such as fraud or espionage against the United States Government. Failure to authorize the correct government worker could also endanger all overseas locations with terrorist or criminal activities.

4. Uses of the Information

a. Describe all uses of the information.

The MIS information is used by the Department management to help them in their decision-making effort when conducting cost/benefit analyses, security reviews, enforcing established submission deadlines and enabling communication of important messages, passport workload, labor and staffing statistics, passport employee productivity, agency deposit information, and product inventory and internal controls for each passport agency on an individual basis. The information collected for MIS is used for performance evaluation of employees, budget forecast for agencies and additionally for Labor Union Negotiations.

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

MIS produces reports about an individual passport agency employee's weekly schedule, worked hours, and leave activity, reports about individual Passport Specialist productivity. It also produces a report that details the staffing profile of an agency, including the names, position title, and grades of individuals on staff.

There is no new data produced by the MIS information.

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

MIS does not use any commercial information, public information or information from other Federal agency databases.

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

MIS is a Department of State system that is developed and maintained by APPTIS. The system is hosted at the Beltsville Information Management Center (BIMC) in Beltsville, Maryland with a disaster recovery site located in Charleston, South Carolina. Contractors are involved with the design, development, and maintenance of the system. Privacy Act information clauses have been inserted into all statement of work and become part of the signed contract. Each contractor employee is required to attend mandatory briefings that cover the handling of classified and other such information prior to working on the task.

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.

Contractors involved in the design, development and maintenance of MIS are required to have a Moderate Risk Public Trust access authorization. This includes a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of MIS hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

The internal users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized users in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that is SBU.

5. Retention

a. How long is information retained?

The established retention period for electronic records in MIS is presently 100 years in accordance with published record schedules as approved by the National Archives and Records Administration (NARA). The following record schedule specifies that these records are to be destroyed when they are 100 years old Chapter 13 Passport Records A-13-001-01c(2)(a) DispAuthNo: NCI-59-79-12 item 1b – Transfer to Washington National Records Center (WNRC) monthly.

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 user of MIS throughout the lifetime of the data. Accuracy of the data is dependent on the individuals providing self-identifying information. The information is only retained for the amount of time that is required to perform the system's purpose.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manger. When records have reached their retention end-date, as stated in the Department of State's Disposition of Schedule, as defined in Chapter 13 Passport Records (per A-13-002-05 which has 180 day retention period), they are immediately retired or destroyed in accordance with published Department of State record schedules as approved by the national Archives and Records Administration (NARA).

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?

MIS information is not shared with any other systems bureaus, offices or organizations outside of the Bureau of Consular Affairs.

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

MIS information is not shared with any other systems, bureaus, offices or organizations outside of the Bureau of Consular Affairs.

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 privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. To combat the misuse of information by personnel, 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 and personnel screening.

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?

MIS information is not shared with any entities outside of the Department of State. Only authorized Department of State General Functional Users and authorized passport agency personnel have access to the data in the system.

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

External access to any non-Department entities is strictly prohibited.

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

None. MIS data is not externally shared or disclosed.

8. Notice

The system:

☒ **contains information covered by the Privacy Act.**

Provide number and name of each applicable system of records.

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?

No. Information is gathered from the Travel Document Issuance System (TDIS) system and Human Resource records. State-26, the system of records notice (SORN) mentioned above, does provide notice of this type of collection of PII.

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

No. Information is gathered from the Travel Document Issuance System (TDIS) system and Human Resource records.

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?

No. Information is gathered from the Travel Document Issuance System (TDIS) system and Human Resource records.

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.

General Functional Users that utilize and have access to MIS are restricted to cleared, authorized Department of State direct hires or contractor personnel. MIS enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purposes and uses and its applicable legal requirements. For additional information on how notice is provided to individuals review the TDIS PIA.

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?

The MIS user data cannot be modified by any user. The user information is for management use only. Information that is obtained from TDIS may be accessed and amended in accordance with the rules published at 22 CFR 171.31. More information about notification and redress regarding information contained in TDIS may be obtained in the Privacy Impact Assessment for that system.

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to the MIS application is restricted to cleared, authorized Department of State direct-hire or contractor personnel via OpenNet. To access the system, users must be an authorized user of the Department of State's unclassified network. Each authorized user must sign a user access agreement before being given a user account. The user 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 MIS application enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties. System administrators can access the MIS application only at the central server location to perform application maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality. External access to any non-Department entity is strictly prohibited.

Personnel accessing MIS information must be authorized by MIS management. Authorized personnel require a user ID/password to access MIS information. User access to MIS information is based on roles.

Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed monthly to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system unusual or unauthorized activities or conditions, logon identification, logon events, and process tracking.)

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

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access users much complete annual refresher training.

Internal users must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice that describe the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

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.

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 terminated. Also, as mentioned earlier, the system audit trails that are automatically generated are regularly reviewed and analyzed. As a result of these actions, the residual risk is low.

11. Technologies

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

MIS is a custom web-based report management and distribution system that 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. However, to do so properly, each of the authorized client workstations must have an ActiveX plug-in installed for the sole purpose of passing Windows login credentials to MIS and **other** Passport applications for single sign-on authentication. These controls are all tested, proven technologies, and they pose no additional privacy risks.

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

Since MIS does not use any technology known to elevate privacy risk, the current MIS safeguards in place are satisfactory. Routine 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 MIS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security management Act (FISMA) of 2002 provision for the triennial recertification of this system, its 36 month authorization to operate expires May 31, 2012. It is anticipated that the current C&A process will be completed in May 2012 resulting in a projected authorization to operate (ATO) date of May 31, 2015.