• Protect material required to be kept secret in the interest of national defense and foreign policy;

• Prevent individuals that are the subject of investigation from frustrating the investigatory process, to ensure the proper functioning and integrity of law enforcement activities, to prevent disclosure of investigative techniques, to maintain the confidence of foreign governments in the integrity of the procedures under which privileged or confidential information may be provided, and to fulfill commitments made to sources to protect their identities and the confidentiality of information and to avoid endangering these sources and law enforcement personnel; or

• Preclude impairment of the Department's effective performance in carrying out its lawful protective responsibilities under 18 U.S.C. 3056 and 22 U.S.C. 4802.

Records meeting any of the above criteria are exempt from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) (2007). See 22 CFR 171.36(b)(1), (b)(2), and (b)(3) (2007).

Dated: December 31, 2007.

Maura Harty,

Assistant Secretary for the Bureau of Consular Affairs, Department of State.

[FR Doc. E8–202 Filed 1–8–08; 8:45 am]

BILLING CODE 4710–06–P

DEPARTMENT OF STATE

[Public Notice 6056]

Privacy Act of 1974; System of Records

Summary: This report is submitted in compliance with Appendix I to OMB Circular Number A–130 entitled ''Federal Agency Responsibilities for Maintaining Records about Individuals.'' The Department of State (''Department'') intends to alter an existing system of records, ''Passport Records'' (STATE–26), to reflect additional routine uses for the information maintained in the Passport Records System.

Purpose: The information collected and maintained in the system of records entitled ''Passport Records'' is in keeping with the Department's responsibility to adjudicate applications for U.S. passports. Proposed alterations appear in the routine uses section of the system description. The purpose in granting access to other entities varies, but principally encompasses the following functions:

• To support national defense, border security, and foreign policy activities;

• To ensure the proper functioning and integrity of law enforcement, counterterrorism, and fraud-prevention activities by supporting law enforcement personnel in the conduct of their duties;

• To support the investigatory process; and

• To assist with verification of passport validity to support employment eligibility and identity corroboration for public and private employment.

This Systems of Records Notice (SORN) documents an updated list of routine uses for records maintained in the passport records system to include disclosure to the following entities:

• Department of Homeland Security for law enforcement; counterterrorism; border patrol, screening, and security purposes; fraud prevention activities; and verification of passport validity to support employment eligibility and identity corroboration for public and private employment;

• Department of Justice, including the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the U.S. Marshals Service, and other components, for law enforcement, counterterrorism, border security, fraud prevention, and criminal and civil litigation activities;

• INTERPOL and other international organizations for law enforcement, counterterrorism, fraud prevention, criminal activities related to lost and stolen passports;

• National Counterterrorism Center to support strategic operational planning and counterterrorism intelligence activities;

• Office of Personnel Management (OPM), other federal agencies, or contracted outside entities to support the investigations that OPM, other federal agencies, and contractor personnel conduct for the federal government in connection with verification of employment eligibility and/or the issuance of a security clearance;

• Social Security Administration to support employment-eligibility verification for public and private employers, and for support in verification of social security numbers used in processing U.S. passport applications;

• Federal, state, local or other agencies for use in legal proceedings as government counsel deems appropriate, in accordance with any understanding reached by the agency with the U.S. Department of State.

• Foreign governments, to permit such governments to fulfill passport control and immigration duties and their own law enforcement, counterterrorism, and fraud prevention functions, and to support U.S. law enforcement, counterterrorism, and fraud prevention activities.

• Public and private employers seeking to confirm the authenticity of the U.S. passport when it is presented as evidence of identity and eligibility to work in the United States;

• Contractor personnel conducting data entry, scanning, corrections, and modifications, or conducting other authorized functions related to passport records.

Authority: The authority for maintaining this system is derived from the Secretary of State's authorities with respect to the following provisions: Granting and Issuing U.S. Passports, 22 U.S.C. 211a–218, 2651a, 2705 (2007), and Executive Order 11295, August 5, 1966, 31 FR 10603; the Acquisition and Loss of U.S. Citizenship or U.S. Nationality, 8 U.S.C. 1401–1503 (2007); Travel Control of Citizens, 8 U.S.C. 1185 (2007); and Crimes and Criminal Procedure connected to U.S. Passport Applications and Use, 18 U.S.C. 911, 1001, and 1541–1546 (2007).

Impact on Privacy: The information collected and maintained in the system of records is necessary to accomplish the Department's mission as stated above. The Department believes the system offers suitably rigorous protection of privacy under the Privacy Act to the individuals covered by the system of records. Each of the above users either has been granted access to the passport database, or has been given passport information taken from the database, in order to facilitate these entities as they address issues and problems of a legal, investigative, technical, or procedural nature that may arise pursuant to an application for or any use of a U.S. passport. In granting access or providing information from the passport database to a routine user, the Department takes appropriate steps to limit disclosure to only the specific data elements required by each routine user in the performance of its mission, not all items of information that the Department maintains about an individual. To this end, the Department has established varying levels of access that are tailored to release the minimum amount of data necessary to support the attendant routine use.

Prior to granting access to the passport system of records for a proposed routine use, partner agencies generally enter into a Memorandum of Understanding (MOU) with the Department that establishes the parameters that guide and limit the use. In addition, these MOUs establish the partner agency's responsibilities in

relation to the information provided, including proper training, establishing that each user has been cleared to access the sensitive information contained in the passport records system, and ensuring that password-protected access is appropriately safeguarded by users and the agency alike.

Moreover, every user who is granted access to the system is subject to remote monitoring to ensure that s/he is accessing the system for the limited, routine use that has been prescribed in advance for each user. The overall impact on privacy is thereby minimized since each user may only access an individual's information in relation to a concrete, pre-determined purpose that has been authorized by Congress and/or established by a formal, written agreement with the Department. The Department ultimately retains control of the Passport Records System and is able to appropriately limit the amount and type of information each user is able to access. Furthermore, the responsibility and accountability for all users rests with the Directorate of Passport Services. Therefore, access and control of the Passport Records system remains within the Department to allow for appropriate internal checks and balances over all users, whether in the Department of State or at partner entities. Deviations from the predetermined routine uses are not permitted, and employees may be subject to sanctions for mishandling Privacy Act-protected information.

Safeguards: Access to the Department of State building and the annexes containing this system of records is controlled by security guards, and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. These records are maintained in secured file cabinets, computer media, and/or in restricted areas, access to which is limited to authorized personnel. The computerized files are password-protected and under the direct supervision of a system manager who can monitor and audit trails of access. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. In addition, the system logs all search and query activities conducted by users, and submits notification alerts to certifying authorities and system administrators if any unusual activity occurs. Any unusual system access patterns by non-Department users are logged and may result in suspension or termination of an individual user's or an agency's access rights.

In addition, all Department employees have undergone a thorough background investigation prior to their employment. Department employees with access to the passport system are also required to undergo initial training in proper handling of this sensitive data, as well as in the correct method to maintain the security of the passport records system. All Department employees must also engage in refresher training at least annually on basic cyber security awareness, as well as training in any new security protections that may be added. As described above, partner entities also agree to provide initial and updated security training to all users who have any form of access to the passport system.

Additional safeguards regarding access to the Department and its annexes are stated in the system description.

Compatibility: The routine uses indicated are necessary for the recipients of information from the Passport Services Office to carry out their responsibilities for dealing with issues and problems of a legal, investigative, technical, or procedural nature that may arise pursuant to an application for or any use of a U.S. passport.

The Department collects data on individual passport applicants in order to establish an individual's unique identity and citizenship for passport issuance. This not only enables the Department to issue passports to qualified U.S. citizens and nationals, but it also facilitates the international travel of millions of passport holders by minimizing potential fraud in the application process, which in turn increases the value and functionality of the U.S. passport as a travel and identification document. Moreover, this database enables the Department to further support the Secure Border, Open Doors initiative by assisting border patrol officers to efficiently process returning U.S. passport holders whose identities are clearly established by their passport document, which in turn is validated by the passport records system.

The routine uses listed above are functionally equivalent to the original purpose of data collection. Passport Services gathers data in order to establish a sound basis to establish and document an individual's unique identity. The proposed routine users listed above likewise must establish an individual's identity in order to carry out their critical missions, which range from law enforcement, to border security, to verification of potential employment eligibility. For example, the U.S. passport is an I–9-listed Employment Eligibility Verification document that may be presented as proof of employment eligibility; thus, data disclosure to corroborate the passport's validity is compatible with the original purpose of collection.

Additionally, Passport Services has worked to make the U.S. passport an internationally recognized, premier travel document. Of those entities listed above, many carry out travel-related functions that are compatible with the Passport Services mission and, thus, the original purpose of the data collection. Without adequate information and documentation, these entities would be unable or less able to ascertain whether the individual seeking entry into the United States or using the passport for overseas travel, is in fact the individual s/he claims to be.

The passport records system provides a database of information that has already been well-scrutinized and evaluated by Department employees who are trained in fraud detection. Access to this thoroughly inspected database will aid the above-listed routine users as they seek to accomplish their functions. Additionally, providing other agencies the ability to confirm an individual's unique identity supports national defense, border security, and foreign policy activities, and ensures the integrity of law enforcement, counterterrorism, and fraud-prevention activities.

Dated: December 31, 2007.

Maura Harty,

Assistant Secretary for the Bureau of Consular Affairs, Department of State.

[FR Doc. E8–203 Filed 1–8–08; 8:45 am]

BILLING CODE 4710–06–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

[Summary Notice No. PE–2007–48]

Petition for Exemption; Summary of Petition Received; Correction

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of petition for exemption received; correction.

SUMMARY: This notice contains a corrected summary of a petition seeking relief from specified requirements of 14 CFR. The purpose of this notice is to improve the public's awareness of, and participation in, this aspect of FAA's regulatory activities. Neither publication