

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 uses 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

of this notice nor the inclusion or omission of information in the summary is intended to affect the legal status of the petition or its final disposition.

DATES: Comments on this petition must identify the petition docket number involved and must be received on or before January 29, 2008.

ADDRESSES: You may send comments identified by Docket Number FAA-2007-0383 using any of the following methods:

- *Government-wide rulemaking Web site:* Go to <http://www.regulations.gov> and follow the instructions for sending your comments electronically.
- *Mail:* Send comments to the Docket Management Facility; U.S. Department of Transportation, 1200 New Jersey Avenue, SE., West Building Ground Floor, Room W12-140, Washington, DC 20590.
- *Fax:* Fax comments to the Docket Management Facility at 202-493-2251.
- *Hand Delivery:* Bring comments to the Docket Management Facility in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue, SE., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

Privacy: We will post all comments we receive, without change, to <http://www.regulations.gov>, including any personal information you provide. Using the search function of our docket web site, anyone can find and read the comments received into any of our dockets, including the name of the individual sending the comment (or signing the comment for an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477-78).

Docket: To read background documents or comments received, go to <http://www.regulations.gov> at any time or to the Docket Management Facility in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue, SE., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: Tyneka Thomas (202) 267-7626 or Frances Shaver (202) 267-9681, Office of Rulemaking, Federal Aviation Administration, 800 Independence Avenue, SW., Washington, DC 20591.

SUPPLEMENTARY INFORMATION: This is a corrected summary of petition that was published on December 28, 2007.

This notice is published pursuant to 14 CFR 11.85.

Issued in Washington, DC, on January 3, 2008.

Pamela Hamilton-Powell,

Director, Office of Rulemaking.

Petition for Exemption

Docket No.: FAA-2007-0383.

Petitioner: Ameriflight, LLC.

Section of 14 CFR Affected: 14 CFR 61.51(f)(2).

Description of Relief Sought: To permit Ameriflight pilots to log second in command (SIC) flight time in aircraft types for which an SIC is not required by their type certification in specific circumstances and provided certain pilot certification, training, and checking requirements are met.

[FR Doc. E8-149 Filed 1-8-08; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Highway Administration

Environmental Impact Statement: Charleston County, SC

AGENCY: Federal Highway Administration (FHWA), USDOT.

ACTION: Notice of Intent.

SUMMARY: The FHWA is issuing this notice to advise the public that an environmental impact statement will be prepared for a proposed highway project in Charleston County, South Carolina.

FOR FURTHER INFORMATION CONTACT: Mr. Robert Lee, Division Administrator, Federal Highway Administration, 1835 Assembly Street, Suite 1270, Columbia, South Carolina 29201, Telephone: 803.765.5411, E-mail: bob.lee@fhwa.dot.gov.

SUPPLEMENTARY INFORMATION: The FHWA, in cooperation with the South Carolina Department of Transportation (SCDOT) and Charleston County will prepare an environmental impact statement (EIS) on a proposed Mark Clark Expressway (I-526) located in Charleston County, South Carolina. The U.S. Army Corps of Engineers will serve as a cooperating agency in developing the EIS. Completing I-526 (Mark Clark Expressway) would improve mobility in the areas by serving the anticipated future traffic growth. The Interstate 526 extension project is approximately 7.1 miles long beginning at U.S. 17 (Savannah Highway) and terminating at SC 171 (Folly Road).

The FHWA and SCDOT are seeking input as a part of the scoping process to assist in identifying issues relative to this project. Letters describing the proposed action and soliciting comments will be sent to appropriate

Federal, State, and local agencies, and to private organizations and citizens who have previously expressed or are known to have interest in this proposal. A formal public scoping meeting will be held between February and March 2008. A public meeting will be held between September and October 2008. In addition, a public hearing will be held after the approval of the Draft Environmental Impact Statement (DEIS). Public notice will be given indicating the time and place of the meetings and hearing. The DEIS will be available for public and agency review and comment prior to the public hearing.

To ensure that the full range of issues related to this proposed action are addressed and all significant issues identified, comments, and suggestions are invited from all interested parties. Comments or questions concerning this proposed action and the EIS should be directed to the FHWA at the address provided above.

(Catalog of Federal Domestic Assistance Program Number 20.205, Highway Planning and Construction. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities apply to this program).

Issued on January 3, 2008.

Robert Lee,

Division Administrator, Columbia, South Carolina.

[FR Doc. E8-246 Filed 1-8-08; 8:45 am]

BILLING CODE 4910-22-P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

[U.S. DOT Docket Number NHTSA-2008-0001]

Reports, Forms, and Recordkeeping Requirements

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation.

ACTION: Request for public comment on proposed collection of information.

SUMMARY: Before a Federal agency can collect certain information from the public, it must receive approval from the Office of Management and Budget (OMB). Under procedures established by the Paperwork Reduction Act of 1995, before seeking OMB approval, Federal agencies must solicit public comment on proposed collections of information, including extensions and reinstatement of previously approved collections.