DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA–2004–19160]

Privacy Act of 1974; Systems of Records: Secure Flight Test Records; Privacy Impact Assessment; Secure Flight Test Phase

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice to supplement and amend existing system of records and privacy impact assessment.

SUMMARY: The Transportation Security Administration is amending the Privacy Act System of Records for the Secure Flight Test Records system (DHS/TSA 017) and the Privacy Impact Assessment for the Secure Flight Test Phase.

DATES: This action will be effective upon publication.

FOR FURTHER INFORMATION CONTACT: Lisa S. Dean, Privacy Officer, Office of Transportation Security Policy, TSA Headquarters, TSA–9, 601 S. 12th Street, Arlington, VA 22202–4220; telephone (571) 227–3947.

SUPPLEMENTARY INFORMATION:

Background

The Transportation Security Administration (TSA) established the Secure Flight Test Records system (DHS/TSA 017) on September 24, 2004 (69 FR 57345), to cover records obtained or created in the course of testing the Secure Flight program. TSA also published on the same day a notice setting forth the Privacy Impact Assessment (PIA) prepared for the testing phase of the Secure Flight program (69 FR 57352). The Secure Flight program will implement the mandate of section 4012(a)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108–458) requiring the Transportation Security Administration to assume from air carriers the function of conducting pre-flight comparisons of airline passenger information to Federal Government watch lists.

TSA has described the testing of Secure Flight in previously-published documents (69 FR 57345, 57352, Sept. 24, 2004). TSA is issuing these revised versions of the System of Records Notice and PIA to provide additional detail regarding the Secure Flight testing program.

In addition, TSA is amending the Secure Flight Test Records system to reflect the fact that TSA will not assert any Privacy Act exemptions for the system. In the system of records notice published on September 24, 2004, TSA stated that it was claiming exemptions for portions of the system of records from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G) and (H), and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). TSA has not initiated a rulemaking to implement these exemptions from the Privacy Act, however, because it became clear from the nature of the records in the system that the exemptions were not necessary. Rather than claiming Privacy Act exemptions to withhold this information, TSA has released passenger name records (PNR) to individuals who have requested them under the Privacy Act and will continue to respond to such records requests, to the extent permitted by law. Therefore, TSA is amending the system of records and the PIA to reflect this practice.

Finally, TSA is making a change to the system of records to reflect the change of the name of TSA's Office of National Risk Assessment to the Office of Transportation Vetting and Credentialing.

Summary of Amendments to the Secure Flight Test Records System and the PIA

TSA is amending the scope of the system of records notice and the PIA to clarify and describe with greater particularity the categories of records and categories of individuals covered by the Secure Flight Test Records system. The categories of records include PNRs enhanced with certain elements of commercial data that were provided to TSA for purposes of testing the Secure Flight program and include commercial data purchased and held by a TSA contractor, EagleForce Associates, Inc. (EagleForce), for purposes of the commercial data test. In addition, the categories of individuals covered by the system include individuals identified in commercial data purchased and held by EagleForce. Finally, TSA is clarifying that part of the Secure Flight test involves testing whether watch list matching could be more effective if the Government were to use certain limited additional data elements derived from commercial data to enhance PNRs.

1. The complete revised Secure Flight Test records system follows:

DHS/TSA 017

SYSTEM NAME:

Secure Flight Test Records.

SECURITY CLASSIFICATION:

Classified, sensitive.

SYSTEM LOCATION:

Records are maintained at: the Office of Transportation Vetting and Credentialing (OTVC), Transportation Security Administration (TSA), Department of Homeland Security, P.O. Box 597, Annapolis Junction, MD 20701–0597; the OTVC assessment facility in Colorado Springs, Colorado; and at EagleForce Associates, Inc., McLean, VA.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(a) Individuals traveling within the United States by passenger air transportation on certain domestic flights completed in June 2004;

(b) Individuals identified in commercial data purchased and held by a TSA contractor for purposes of comparing such data with the June 2004 Passenger Name Records and testing the Secure Flight program;

(c) Individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

CATEGORIES OF RECORDS IN THE SYSTEM:

(a) Passenger Name Records (PNRs) for certain passenger air transportation flights completed in June 2004 provided by aircraft operators in response to the Transportation Security Administration Order issued November 15, 2004 (69 FR 65625), (the June 2004 PNRs), the specific contents of which often vary by aircraft operator;

(b) Information obtained from the Terrorist Screening Center about individuals known or reasonably suspected to be or to have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;

(c) Authentication scores and codes obtained from commercial data providers;

(d) PNRs that were enhanced with certain fields of information obtained from commercial data—full name, address, date of birth, gender—and that were provided to TSA for purposes of testing the Secure Flight program;

(e) Commercial data purchased and held by a TSA contractor for purposes of comparing such data with June 2004 PNRs and testing the Secure Flight program;

(f) Results of comparisons of individuals identified in PNRs to watch lists obtained from the Terrorist Screening Center.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. 114, 44901, and 44903.

PURPOSE(S):

The system will be used to test the Secure Flight program. The purpose of

the program is to enhance the security of domestic air travel by identifying passengers who warrant further scrutiny prior to boarding an aircraft. The purposes of testing the Secure Flight program are: (1) To test the Government's ability to process and compare passenger information against terrorist watch list information held by the Terrorist Screening Center (TSC) in the Terrorist Screening Database (TSDB); (2) to test the Government's ability to operate a streamlined version of the rule set used under the existing computer-assisted passenger prescreening system (CAPPS) currently used by aircraft operators; and (3) to test the Government's ability to verify the identities of passengers using commercial data and to improve the efficacy of watch list comparisons by making passenger information more complete and accurate using commercial data. For more detail on the purposes and conduct of the Secure Flight testing, please see the revised PIA for the Secure Flight Test Phase, which is published below.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(1) To the Federal Bureau of Investigation where TSA becomes aware of information that may be related to an individual identified in the Terrorist Screening Database as known or reasonably suspected to be or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

(2) To contractors, grantees, experts, consultants, or other like persons when necessary to perform a function or service related to the Secure Flight program or the system of records for which they have been engaged. Such recipients are required to comply with the Privacy Act, 5 U.S.C. 552a, as amended.

(3) To the Department of Justice (DOJ) or other Federal agency in the review, settlement, defense, and prosecution of claims, complaints, and lawsuits involving matters over which TSA exercises jurisdiction or when conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) TSA; or (b) any employee of TSA in his/her official capacity; or (c) any employee of TSA in his/her individual capacity, where DOJ or TSA has agreed to represent the employee; or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and TSA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which TSA collected the records.

(4) To the National Archives and Records Administration (NARA) or other Federal agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

(5) To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual.

(6) To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are stored electronically in a secure facility at the Office of Transportation Vetting and Credentialing (OTVC), Transportation Security Administration (TSA), Department of Homeland Security, P.O. Box 597, Annapolis Junction, MD 20701–0597; the OTVC assessment facility in Colorado Springs, Colorado; and at EagleForce, Inc., McLean, VA. The records are stored on magnetic disc, tape, digital media, and CD–ROM, and may also be retained in hard copy format in secure file folders.

RETRIEVABILITY:

Data are retrievable by the individual's name or other identifier, as well as non-identifying information.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable OTVC, TSA, and DHS automated systems security and access policies. Access to computer systems containing the records in this system of records is limited and can be accessed only by those individuals who require it to perform their official duties. Safeguards also include a real time auditing function of individuals who access computer systems containing the records in this system of records. Classified information, if any, will be appropriately stored in a secured facility, in secured databases and containers, and in accordance with other applicable requirements, including those pertaining to classified information.

RETENTION AND DISPOSAL:

TSA has determined that the records contained in the Secure Flight Test records system are covered by NARA General Records Schedule (GRS) 20, which applies to electronic records. It covers electronic files or records created solely to test system performance, as well as hard-copy printouts and related documentation for the electronic files/records. Under GRS 20, an agency may delete or destroy such records when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. In accordance with GRS 20, TSA has destroyed certain copies of the original PNRs provided by the air carriers. In addition, in accordance with applicable law, TSA plans to direct and document the destruction of the remaining PNRs and commercial data in its possession or in the possession of EagleForce as testing activities and analyses are completed.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Administrator, Secure Flight/Registered Traveler, Transportation Security Administration, P.O. Box 597, Annapolis Junction, MD 20701–0597.

NOTIFICATION PROCEDURE:

See ''Record Access Procedure''.

RECORD ACCESS PROCEDURE:

DHS has determined that all persons may request access to information about them contained in the system by sending a written request to the TSA Privacy Officer, Transportation Security Administration (TSA–9), 601 South 12th Street, Arlington, VA 22202.

To the extent permitted by law, such access will be granted. Individuals requesting access must comply with the Department of Homeland Security Privacy Act regulations on verification of identity (6 CFR 5.21(d)). Individuals must submit their full name, current address, and date and place of birth. Individuals must sign the request and the signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

2. The complete revised PIA follows:

Secure Flight Test Phase Privacy Impact Assessment

I. Introduction

Pursuant to the authority granted by the Aviation and Transportation Security Act of 2001 (ATSA) and

section 4012(a)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108–458, 118 Stat. 3638, Dec. 17, 2004), TSA is developing a new program for screening domestic airline passengers in order to enhance the security and safety of domestic airline travel. Under this program, Secure Flight, the Transportation Security Administration (TSA) will assume from air carriers the function of conducting pre-flight comparisons of airline passenger information to the expanded and consolidated watch lists held in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC).[1] On November 15, 2004, TSA issued an order directing U.S. aircraft operators to provide to TSA, by November 23, 2004, a limited set of historical passenger name records (PNRs) for testing of the Secure Flight program.

Because the test involves existing watch lists that are being consolidated and expanded in the TSC, the E-Government Act of 2002 requires that a Privacy Impact Assessment (PIA) be conducted. The previously published PIA is being clarified and expanded to reflect more closely actual experience as the testing program has been conducted, refined and modified since September 2004. After the testing has been concluded and the results analyzed, TSA will update the PIA as necessary prior to actual implementation of the Secure Flight program.

System Overview

- What information is to be collected and used for testing Secure Flight?

In order to conduct testing, TSA obtained historic PNRs for individuals who completed domestic flight segments during the month of June 2004. PNR varies according to airline, but generally includes the following information fields: Full name, contact phone number, mailing address and travel itinerary. Also for purposes of the test, a TSA contractor, EagleForce Associates, Inc. (EagleForce), obtained commercial data from three commercial data aggregators. EagleForce contracted with each commercial data aggregator to identify records in its data bases associated with names in a sample set of PNRs and provide such records to EagleForce, but to provide only certain data elements associated with the names. Specifically, EagleForce requested the following data elements: First name; last name; middle name; home address; home phone number; date of birth; name suffix; second surname; spouse first name; gender; second address; third address; plus-four portion of Zip code; address type (residence, business, or mailing address); latitude of address; and longitude of address. In some cases the commercial data aggregators provided information that EagleForce did not request, such as social security numbers, due to the way the commercial data aggregators packaged their product. Although EagleForce loaded the commercial data provided by the commercial data aggregators onto a database, EagleForce has not queried or used any of the data elements that the commercial data aggregators provided over and above the specific data elements that EagleForce had specifically requested.

- Why is the information being collected and who will be affected by the collection of the data?

TSA collected the information described above to test the Secure Flight program, the purpose of which is to enhance the security of domestic air travel by identifying only those passengers who warrant further scrutiny. TSA's test of the Secure Flight program has three objectives. The first objective is to test the Government's ability to process and compare passenger information against terrorist watch list information held by the TSC in the TSDB. The second objective is to test the Government's ability to operate a streamlined version of the rule set used under the existing computer-assisted passenger prescreening system (CAPPS) currently used by aircraft operators. The third objective is to test the Government's ability to verify the identities of passengers using commercial data and to improve the efficacy of watch list comparisons by making passenger information more complete and accurate using commercial data to enhance PNRs with elements such as full name, address, date of birth, and gender. TSA, through its contractor IBM, has compared the PNR with data maintained in the TSDB regarding individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism. TSA is continuing watch list match testing through it contractor, Mitre, using the original PNRs provided by the air carriers. TSA also continues to conduct internal system testing of the watch list matching processes through Mitre and IBM.

To prepare for the commercial data test, two statistically significant samples of the PNR data were extracted. One sample consisted of approximately 17,000 PNRs representing a cross section of air carriers and indicative of a typical PNR. A second sample was also developed that consisted of approximately 24,000 PNRs that contained dates of birth.

The sample data sets, which represent PNRs from eight U.S. air carriers, were stored on CD–ROMs. These data sets are used to perform watch list match testing in connection with the first objective of the program described above.

In addition, TSA hand delivered duplicates of the CD–ROMs containing the two sample PNR data sets to EagleForce. TSA also provided to EagleForce unparsed copies of other electronically stored June 2004 PNR data from the air carriers whose PNRs were included in the representative samples.

In preparing for the commercial test, for each of the approximately 42,000 names in the two sample sets of PNRs, EagleForce created up to twenty variations of a person's first and last names. Accordingly, EagleForce generated approximately 240,000 name variations derived from the approximately 42,000 names in the sample data sets. The original PIA and system of records notice did not discuss this process, because TSA had not developed its test plan with this level of detail at the time the documents were published.

EagleForce submitted the original names and name variations to three commercial data aggregators: Insight America, Acxiom, and Qsent. Upon receipt of the information provided by the commercial data aggregators, EagleForce loaded the records into a database. In order to accomplish the third test objective identified above, Secure Flight undertook two steps. First, EagleForce compared information in the sample PNRs with certain data elements contained in the information in the commercial data records to attempt to identify instances when the data in the PNRs was incorrect or inaccurate. In the course of this activity, EagleForce used only those data elements that it had asked the commercial data aggregators to provide. EagleForce did not use any of the data elements that the commercial data aggregators had provided beyond the specific data elements that EagleForce had specifically requested.

Second, to further test accuracy through verification testing, EagleForce used certain records obtained from the three commercial data aggregators to enhance the sample PNR data in cases

[1] The Terrorist Screening Center (TSC), established in December 2003, maintains a consolidated, comprehensive watch list of known or suspected terrorists. This database can be used by Government agencies in screening processes to identify individuals known to pose or are suspected of posing a risk to the security of the United States.

where PNRs were missing data. If a PNR in the sample data did not have complete information on a subject's full name, date of birth, address, gender, or one of the other categories of data that EagleForce specifically requested from the commercial data aggregators, EagleForce attempted to incorporate that data from the commercial data records, thereby ''enhancing'' the PNRs with these specific elements. However, EagleForce did not use the following data elements to enhance PNRs: spouse first name; latitude of address; and longitude of address. EagleForce then produced CD–ROMs containing the PNRs enhanced with the additional data elements and provided those CD–ROMs to TSA for use in watch list match testing. TSA currently retains the CD–ROMs containing the enhanced PNRs and stores these CD–ROMS when they are not in use in a controlled access safe. TSA provided for a limited period of time the CD–ROMs containing the enhanced PNRs to employees of TSA's contractor charged with conducting watch list testing (IBM), to determine whether using commercial data to enhance passenger information could lower the number of instances in which a person appears to be a match to the TSDB, but is not (a false positive) or appears not to be a match, but in fact is (a false negative).

The categories of individuals covered by the data collection are: individuals who traveled within the United States during June 2004 by passenger air transportation and whose PNRs were provided by aircraft operators in response to the Transportation Security Administration Order issued November 15, 2004 (69 FR 65625); individuals identified in commercial data purchased and held by a TSA contractor for purposes of testing the Secure Flight program; and individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

TSA has not and will not use the results of its testing for any purpose other than analysis of the efficacy of the program unless there is an indication during the testing of terrorist or possible terrorist activity. In such a case, appropriate action will be taken, which may include providing information in the system of records to relevant law enforcement agencies. To date no such action has been warranted.

• What notice or opportunities for consent are provided to individuals regarding the information that is collected and shared?

The original Privacy Act System of Records Notice and PIA, as well as the revised versions of each document, provide notice of the scope, purposes, and effect of the test phase of the Secure Flight program. Because the test phase uses historical PNR from the month of June 2004 for flights that were completed by the end of that month, as well as data residing in commercial databases that already had been collected prior to the test, the notice given did not afford the opportunity for these individuals to provide consent in advance of this collection. Nevertheless, Secure Flight has been the subject of Congressional testimony, public statements by TSA officials, and numerous media reports that convey additional notice, including information that appears on the TSA Web site at *http://www.tsa.gov/public/.*

The information collected has been shared with TSA employees and contractors who have a ''need to know'' in order to conduct the required test comparisons. All TSA contractors involved in the testing of Secure Flight are contractually and legally obligated to comply with the Privacy Act in their handling, use and dissemination of personal information in the same manner as TSA employees.

If a comparison using the test data indicates that an individual is suspected of terrorism, TSA will refer the information to appropriate law enforcement personnel for further action. Referrals will only occur, however, in this limited circumstance because the basic purpose of this information collection is to test the Secure Flight program. To date, no such referrals have been warranted.

• What security protocols are in place to protect the information?

TSA has employed data security controls, developed with the TSA Privacy Officer, to protect the data used for Secure Flight testing activities. Information in TSA's record systems is safeguarded in accordance with the Federal Information Security Management Act of 2002 (Pub. L. 107–347), which established Government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. The systems on which the tests are or have been conducted were assessed for security risks, have implemented security policies and plans consistent with statutory, regulatory and internal DHS guidance.

Prior to accepting custody of the PNR data, TSA established chain-of-custody procedures for the receipt, handling, safeguarding, and tracking of access to the PNR data and TSA maintained the data at its secure facility in Annapolis Junction, Maryland. Access to the data was limited to individuals with a need for access in order to conduct testing activities.

Records of transmission of PNR data to EagleForce were maintained by TSA's security officers. EagleForce had measures in place to control access and handling of PNR data. In addition, EagleForce employees completed training for handling sensitive information and entered into non-disclosure agreements covering all data provided by the Government for use during the test. Copies of these agreements are maintained by TSA's security office.

TSA and its contractors maintain the PNRs and the limited commercial data collected for the test in a secure facility on electronic media and in hard copy format. The information is protected in accordance with rules and policies established by both TSA and DHS for automated systems and for hard copy storage, including password protection and secure file cabinets. Moreover, access is strictly controlled; only TSA employees and contractors with proper security credentials and passwords will have permission to use this information to conduct the required tests, on a need-to-know basis. Additionally, a real time audit function is part of this record system to track who accesses the information resident on electronic systems during testing. Any infractions of information security rules will be dealt with severely. None has occurred to date. All TSA and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of personal data. The procedures and policies that are in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.

• Does this program create a new system of records under the Privacy Act?

On September 24, 2004, TSA established a new Privacy Act system of records, known as the Secure Flight Test Records system of records, DHS/TSA 017, for purposes of Secure Flight testing activities (69 FR 57345). TSA has amended and supplemented that system of records to clarify the original system of records notice with additional detail on the Secure Flight testing activities.

• What is the intended use of the information?

The information collected by TSA and TSA contractors has been and will be used solely for the purpose of testing the Secure Flight program, as described in this PIA, and will be maintained in a Privacy Act system of records in

accordance with the published system of records notice for DHS/TSA 017.

• Will the information be retained and, if so, for what period of time?

TSA has determined that the records contained in the Secure Flight Test Records system are covered by NARA General Records Schedule (GRS) 20, which applies to electronic records. It covers electronic files or records created solely to test system performance, as well as hard-copy printouts and related documentation for the electronic files/records. Under GRS 20, an agency may delete or destroy such records when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. In accordance with GRS 20, TSA has destroyed certain copies of the original PNRs provided by the air carriers. In addition, TSA, in accordance with applicable law, plans to direct the destruction of the remaining PNRs and commercial data in its possession or in the possession of EagleForce as testing activities and analyses are completed.

• How will the passenger be able to seek redress?

During the test phase individuals may request access to information about themselves contained in the PNR subject to Secure Flight test phase by sending a written request to TSA. To the extent permitted by law, access will be granted. If an individual wishes to contest or amend the records received in this manner, he or she may do so by sending that request to TSA. The request should conform to DHS requirements for contesting or amending Privacy Act records, and should be sent TSA Privacy Officer, Transportation Security Administration (TSA–9), 601 South 12th Street, Arlington, VA 22202. Before implementing a final program, however, TSA will create a robust redress mechanism to resolve disputes concerning the Secure Flight program.

• What databases will the names be compared to?

TSA has compared the names against the TSDB, which is a consolidated, comprehensive watch list of known or suspected terrorists. This database can be used by Government agencies in screening processes to identify individuals known to pose or are suspected of posing a risk to the security of the United States. This consolidated database contains information contributed by the Departments of Homeland Security, Justice, and State and by the intelligence community. Because information related to terrorists is consolidated in the TSDB, TSA believes that the TSDB provides the most effective and secure system against which to run airline passenger names for purposes of identifying whether or not they are known or reasonably suspected to be engaged in terrorism or terrorist activity. TSA's contractor has compared names with information provided by commercial data aggregators to identify commercial data records from which to enhance PNRs for purposes of the Secure Flight test.

• Privacy Effects and Mitigation Measures.

The decision to initiate Secure Flight followed completion of a thorough review of the TSA's next generation passenger prescreening program and the mandate of section 4012(a)(1) of the IRTPA.

Testing has been and continues to be governed by strict privacy and data security protections. TSA will defer any decision on how commercial data might be used in its prescreening programs, as Secure Flight, until the completion of the test period, assessment of the test results and publication of a subsequent System of Records Notice under the Privacy Act announcing the intended use of such commercial data.

TSA has taken action to mitigate privacy risk by designing its test activities to address concerns expressed by privacy advocates, foreign counterparts and others. Under the Secure Flight testing phase, TSA did not require air carriers to collect any additional information from their passengers than was already collected by such carriers and maintained in passenger name records. TSA has adopted and carried out stringent data security and privacy protections, including contractual prohibitions on commercial entities' maintenance or use of airline-provided PNR information for any purposes other than testing under TSA parameters; real time auditing procedures to determine when data within the Secure Flight system has been accessed and by whom; and strict rules prohibiting the accessing or use of commercial data by TSA employees.

TSA will assess test results prior to any operational use of commercial data in TSA programs to determine whether its use is effective in verifying passenger identity or enhancing watch list comparisons, justifies the associated costs, does not result in disparate treatment of any class of individuals, and that data security protections and privacy protections are robust and effective.

TSA also recognizes that there is a privacy risk inherent in the design of any new system which could result from design mistakes. By testing the proposed Secure Flight program, TSA has had the opportunity to modify the program design in ways to enhance protection of individuals' privacy interests before the program becomes fully operational, ensuring a better program. TSA is purposely testing the Secure Flight system and will be carefully scrutinizing the performance of the system during the test phase—and conducting further analysis upon completion—to determine the effectiveness of Secure Flight both for passenger prescreening as well as for protecting the privacy of the data on which the program is based. By following strict rules for oversight and training of personnel handling the data as well as strong system auditing to detect potential abuse and a carefully planned and executed redress process, TSA will continue to ensure that privacy is an integral part of the program once it becomes operational, as it has been during testing. TSA's efforts have been and continue to be thoroughly examined internally, including review by the TSA Privacy Officer and the DHS Chief Privacy Officer. In this process, TSA will carefully review constructive feedback it receives from the public on this important program.

Issued in Arlington, Virginia, on June 17, 2005.

Lisa S. Dean,

TSA Privacy Officer.

[FR Doc. 05–12405 Filed 6–17–05; 5:02 pm]

BILLING CODE 4910–62–P