[4910-62-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA-2004-19160]

Privacy Impact Assessment; Secure Flight Test Phase

AGENCY: Transportation Security Administration (TSA), Department of Homeland Security (DHS).

ACTION: Notice.

SUMMARY: This notice sets forth the Transportation Security Administration's (TSA) Privacy Impact Assessment (PIA) prepared for the testing phase of the Secure Flight program. After a lengthy review of the initial plans for a successor system to Computer Assisted Passenger Prescreening System (CAPPS), and consistent with a recommendation of the National Commission on Terrorist Attacks upon the United States (9/11 Commission), the Department of Homeland Security is moving forward with a next generation system of domestic passenger prescreening, called "Secure Flight", which will prescreen airline passengers using information maintained by the Federal Government about individuals known or suspected to be engaged in terrorist activity and certain other information related to passengers' itineraries-specifically, passenger name record (PNR) data. On a limited basis, TSA will also test the use of commercial data to identify instances in which passengers' identifying passenger information is inaccurate or incorrect.

filed: 12:58 pm 9/21/04
pub: 9/24/04

Elsewhere in this edition of the Federal Register, TSA is publishing notice of a new system of records under the Privacy Act, known as "Secure Flight Test Records," which TSA will use for records related to the testing of the program. Also in this edition of the Federal Register, TSA is publishing a notice announcing its request for approval by the Office of Management and Budget of TSA's collection of a limited set of historical PNR from domestic airlines for purposes of testing the Secure Flight program.

DATES: This notice is effective ~~[Insert date of publication in the Federal Register]~~ September 24, 2004.

FOR FURTHER INFORMATION CONTACT:

Lisa S. Dean, Privacy Officer, (TSA-9) Transportation Security Administration, Arlington, VA 22202; Nuala O'Connor Kelly, Chief Privacy Officer, U.S. Department of Homeland Security, Washington, DC, 20528.

SUPPLEMENTARY INFORMATION:

Availability of Notice

You can get an electronic copy using the Internet by--

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) web page (http://dms.dot.gov/search);

(2) Accessing the Government Printing Office's web page at http://www.access.gpo.gov/su_docs/aces/aces140.html; or

(3) Visiting TSA's Law and Policy web page at http://www.tsa.dot.gov/public/index.jsp.

In addition, copies are available by writing or calling the individual in the FOR FURTHER INFORMATION CONTACT section. Make sure to identify the docket number of this notice.

Secure Flight
Test Phase Privacy Impact Assessment

I. Introduction

Pursuant to the authority granted it by the Aviation and Transportation Security Act of 2001 (ATSA), TSA has developed a new program for screening domestic airline passengers in order to enhance the security and safety of domestic airline travel. Under this new program, Secure Flight, TSA will compare PNR information against expanded and consolidated watch lists held in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC)[1] to identify known or suspected terrorists who would use the airways to inflict catastrophic damage on the United States. TSA plans to test the efficacy of the Secure Flight program after issuing an order to domestic air carriers to compel the collection of historic passenger name record (PNR) information for testing purposes. TSA will also conduct a separate test to determine if commercial data is effective in identifying passenger information that is incorrect or inaccurate. TSA does not assume that the result of comparison of passenger information to commercial data is determinative of information accuracy or the intent of the person who provided the passenger information.

Earlier this year, the Department of Homeland Security ordered a thorough review of the next generation passenger prescreening program under development by TSA. That review, which reflected helpful input to DHS from Congress, the public, privacy and civil liberties groups, airline passengers and the airline industry, and our international partners, has now been completed. Based on the results, TSA has developed a new program,

[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.

Secure Flight, described above, which it intends to test prior to actual implementation. The new program will allow DHS to add a critical piece to its layered strategy for securing the nation's commercial air transportation system and is consistent with the 9/11 Commission recommendation: (1) that the Federal Government take over the responsibility for checking airline passengers' names against expanded "no-fly" and "automatic selectee" lists (this function is currently performed by individual airlines); and (2) that air carriers be required to supply data to test and implement this new system. Because existing watch lists that are being consolidated and expanded in the TSC will be used to test the prescreening of airline passengers by TSA using the TSDB, the E-Government Act of 2002 requires that a Privacy Impact Assessment (PIA) be conducted. That assessment follows. After the test 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 this passenger pre-screening system?

The information to be collected will be used for a test of the Secure Flight program to ensure its accuracy, efficacy and reliability. In order to conduct the test, TSA will require domestic air carriers to submit historic PNR about individuals who have completed domestic flight segments during the month of June, 2004. PNR varies according to airline, but includes the following information fields which TSA will need for testing purposes: full name, contact phone number, mailing address and travel itinerary limited to domestic flight segments that were completed prior to June 30, 2004. Upon

completion of testing and before implementation of the Secure Flight program, TSA will publish an amended Privacy Impact Assessment and Privacy Act Notice reflecting changes to the program based on knowledge gained from testing as well as constructive feedback from the public.

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

TSA is collecting information 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. The PNR to be collected will be compared 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. Individuals subject to the data collection requirements and processes of Secure Flight are persons who traveled within the United States during June 2004, the pre-selected 30-day period.

This same historic PNR data also will be used to conduct a limited test to determine if the use of commercial data is effective in identifying passengers' information that is incorrect or inaccurate. This test will involve commercial data aggregators who currently provide services to the banking, home mortgage and credit industries. Testing will be governed by strict privacy and data security protections. TSA will not store the commercially available data that would be accessed by commercial data aggregators. TSA will use this test of commercial data to determine whether such use: (1) could accurately identify passenger information that is incorrect or inaccurate; (2) would not result in inappropriate differences in treatment of any protected category of persons; (3)

could be governed by data security safeguards and privacy protections that are sufficiently robust to ensure that commercial entities or other unauthorized entities do not gain access to passenger personal information, or to ensure that the federal government does not gain access inappropriately to certain types of personally sensitive data held by commercial entities.

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.

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

The Privacy Act System of Records Notice being published at this time – as well as this Privacy Impact Assessment – provide notice that TSA intends to collect historic PNR to test the Secure Flight program. Because the test phase will rely on historical PNR from the month of June 2004 for flights that were completed by the end of that month, the notice given by this Privacy Impact Assessment and the publication of a Privacy Act System of Records Notice for these records does not afford the opportunity for a passenger to provide consent in advance of this collection. Nevertheless, airline passengers are aware that by engaging in air travel they have consented to certain screening protocols since passenger prescreening is already in place. Additionally, Secure Flight has now been the subject of numerous media reports that convey additional notice, including information that appears on the TSA website at http://www.tsa.gov/public/.

The information to be collected will be 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.

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

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 will be conducted have been assessed for security risks, have implemented security policies and plans consistent with statutory, regulatory and internal DHS guidance, and are certified and accredited.

TSA will maintain the data to be collected for this test in a secure facility on electronic media and in hard copy format. The information will be 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 will be 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. Additionally, a real time audit function will be part of this record system to track who accesses the information, and any infractions of information security rules will be dealt with severely. 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.

Yes. The Secure Flight Test Records system of records, DHS/TSA 017, is being published concurrently in today's Federal Register.

- What is the intended use of the information?

The information collected by TSA will be used solely for the purpose of testing the Secure Flight program 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 will retain these records for a sufficient period of time to conduct and review the Secure Flight test and in the event where a request for redress must be resolved. TSA does not yet have a record retention schedule approved by the National Archives and Records Administration (NARA) for records pertaining to this program and must retain these records until such schedule is approved. TSA is in the process of developing a

records retention schedule that will dictate the retention period for these records and allow TSA to dispose of them within an appropriate timeframe.

- 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 greatest extent possible and consistent with national security and homeland security requirements, 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 run against?

TSA will run 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.

- Privacy Effects and Mitigation Measures

The decision to initiate Secure Flight follows completion of a thorough review of the TSA's next generation passenger prescreening program, and is consistent with recommendations of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) that "improved use of 'no-fly' and 'automatic selectee' lists should not be delayed while the argument about a successor to CAPPS continues." Moreover, by focusing solely on potential terrorism and not other law enforcement purposes, Secure Flight addresses concerns raised by privacy groups and others about the potential for "mission creep" by TSA.

TSA appreciates the privacy risk inherent in any airline prescreening program in which passenger name record information is provided to the Federal Government for use in conducting the prescreening. However, TSA also recognizes that the risk is necessary for ensuring the security of our air transportation system. TSA believes it has taken action to mitigate any privacy risk by designing its next generation passenger prescreening program to accommodate concerns expressed by privacy advocates, foreign counterparts and others.

First, under the Secure Flight testing phase, TSA will not require air carriers to collect any additional information from their passengers than is already collected by such carriers and maintained in passenger name records. Testing of the Secure Flight program will compare only existing PNR record information against names in the TSDB in order

to determine how effectively existing PNR information can be compared against such names, how many instances of false positive matches occur, and what, if any additional limited data, would be most effective in reducing the number of such false positive hits. TSA envisions that carriers may be required to collect full passenger name and possibly one other element of information under a fully implemented operational Secure Flight program. However, TSA will not make such determination until the initial test phase results can be assessed and an additional Privacy Impact Assessment is published.

Second, the Secure Flight program will permit TSA to take on sole responsibility for conducting passenger name comparisons against a consolidated TSDB watch list, rather than continuing to require multiple individual air carriers to conduct such comparisons. TSA will be able to apply improved prescreening procedures, including more consistent analytical procedures, for identifying actual name matches and for resolving false positive name matches prior to a passengers' arrival at an airport, than can currently be applied by the individual air carriers that currently administer the watch list comparisons. TSA expects that the number of individuals currently subjected to automatic secondary screening will be reduced under an implemented Secure Flight program.

Third, Secure Flight will mitigate impact on personal privacy because of its limited purpose and anticipated limited retention period. Secure Flight will focus screening efforts only on identifying individuals known or reasonably suspected to be terrorists or engaged in terrorist activity, rather than on other law enforcement purposes. In addition, Secure Flight will only be applied to passengers on U.S. domestic flights. Passengers on international flights will continue to be prescreened using APIS (Advanced

Passenger Information System data – information from the machine readable portion of an individual's passport) provided to U.S. Customs and Border Protection for this purpose. Passengers on international flights will not be subject to duplicative information provision requirements or overlapping screening procedures. TSA also anticipates that passenger information will be held for a relatively limited amount of time after completion of a passenger's itinerary. TSA's prescreening efforts will be as narrow as reasonable to accommodate privacy concerns, including access to redress mechanisms, but as robust as necessary to accomplish its security mission.

TSA believes that the Secure Flight program will represent a vast improvement in security by permitting TSA to identify individuals known or reasonably suspected to be engaged in terrorism or terrorism related activity. However, because Secure Flight may be rendered less effective if passenger-provided information is not accurate or correct, TSA does seek to identify the most appropriate means to identify when passenger information is incorrect or inaccurate. For this reason, TSA will use PNR information obtained for testing of the Secure Flight program to conduct a separate test of the use of commercial data to identify such inaccurate or incorrect passenger information. TSA recognizes that this may raise privacy and civil liberties concerns. TSA's testing of commercial data use will therefore involve the following:

(a) TSA will only test the use of commercial data

(b) TSA does not assume that the result of comparison of passenger information to commercial data is determinative of information accuracy or the intent of the person who provided the passenger information.

(c) Such testing of commercial data will be governed by 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; strict firewalls between the government and commercial data providers; real-time auditing procedures to determine when data within the Secure Flights system has been accessed and by whom; strict rules prohibiting the accessing or use of commercially held personal data by TSA;

(d) Assessment of test results prior to any operational use of commercial data in TSA programs and determination that its use is effective in identifying incorrect or inaccurate information 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 will have the opportunity to correct any privacy-related design mistakes before the program becomes fully operational, ensuring a better program. TSA is purposely testing the Secure Flight system, in fact, 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 layering on top of the program design 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 intends to make sure that privacy is an integral part of this overall effort. TSA's efforts will not only be thoroughly examined internally, including review by the TSA Privacy Officer, but also will be reviewed by the DHS Chief Privacy Officer before a final program is designed. In this process, TSA will carefully review constructive feedback it receives from the public on this important program.

Issued in Arlington, VA, on SEP 2 1 2004.

Lisa S. Dean,

Privacy Officer.