



GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 22, 2005

Congressional Committees

Subject: *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*

As you know, we have been reviewing the Department of Homeland Security's (DHS) Transportation Security Administration's (TSA) efforts to develop and implement the Secure Flight program. The purpose of Secure Flight is to compare information on domestic airline passengers against information on known or suspected terrorists to identify passengers who should undergo additional security scrutiny. As we reported in February and March 2005, to develop Secure Flight, TSA has been conducting tests to compare data from airline reservation systems, such as name and flight number, with data from the government's consolidated terrorist watch lists, which include names of known and suspected terrorists.¹ We also reported that TSA has been testing the use of selected data available from commercial data sources—private companies that maintain records on individual names, addresses, phone numbers, and other information—as a means of verifying the accuracy of passenger-provided data. In this letter, we report on key aspects of TSA's disclosure of its use of personal information during commercial data testing for Secure Flight as required by the Privacy Act, and TSA's actions to more fully disclose its use of personal information.² We will continue our assessment of Secure Flight privacy protections as part of our ongoing review of the Secure Flight program.

Results in Brief

During the course of our ongoing review of the Secure Flight program, we found that TSA did not fully disclose to the public its use of personal information in its fall 2004 privacy notices as required by the Privacy Act. In particular, the public was not made fully aware of, nor had the opportunity to comment on, TSA's use of personal information drawn from commercial sources to test aspects of the Secure Flight

¹For more on the Secure Flight program, see GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed*, GAO-05-356 (Washington, D.C.: Mar. 28, 2005) and GAO, *Aviation Security: Measures for Testing the Impact of Using Commercial Data for the Secure Flight Program*, GAO-05-324 (Washington, D.C.: Feb. 23, 2005).

²Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a). The Privacy Act provides safeguards against an invasion of privacy through the misuse of records by federal agencies and allows citizens to learn how their personal information is collected, maintained, used, and disseminated by the federal government.

program. In September 2004 and November 2004, TSA issued privacy notices in the *Federal Register*³ that included descriptions of how such information would be used.⁴ However, these notices did not fully inform the public before testing began about the procedures that TSA and its contractors would follow for collecting, using, and storing commercial data. In addition, the scope of the data used during commercial data testing was not fully disclosed in the notices. Specifically, a TSA contractor, acting on behalf of the agency, collected more than 100 million commercial data records containing personal information such as name, date of birth, and telephone number without informing the public. As a result of TSA's actions, the public did not receive the full protections of the Privacy Act.

On June 10, 2005, we briefed TSA on our concerns about privacy protection issues related to Secure Flight testing. TSA officials stated that they recognized the merits of GAO's concerns, and on June 22, 2005, the agency published revised privacy notices to more fully disclose the nature of tests being conducted.⁵ The revised notices clarified the purpose of commercial data testing for Secure Flight and expanded the categories of records and individuals covered by the system of records as it applied to commercial data tests. In moving forward, TSA officials stated that they will put procedures in place to ensure that prior to making any change in testing procedures, the TSA Privacy Officer and TSA counsel would be consulted to determine whether a change to TSA's privacy notices would be required to inform the public. TSA officials also stated that no adverse consequences resulted from the use of commercial data because the data were used only in a test environment and not to make passenger prescreening decisions prior to actual flights.⁶ TSA officials further stated that data collected from commercial sources will not be used during the initial operation of Secure Flight, which is expected to begin in late 2005 or early 2006. TSA is, however, considering the use of such data in the future, if the data can be shown to improve the ability of Secure Flight to identify known or suspected terrorists.

In its written comments to a draft of this letter, DHS reiterated that it recognized the merits of the issues raised by GAO, and that TSA acted immediately to address them. DHS also affirmed its commitment to adhere to the letter and intent of the Privacy Act and applicable policies on privacy protections. DHS further stated that the DHS Chief Privacy Officer is assessing the handling of passenger information and commercial data during Secure Flight testing and will, if appropriate, make recommendations to strengthen privacy protections. DHS also provided technical comments on the draft, which we incorporated as appropriate.

³System of Records Notice, 69 Fed. Reg. 57,345 (Sept. 24, 2004); Privacy Impact Assessment, 69 Fed. Reg. 57,352 (Sept. 24, 2004); Notice of Final Order for Secure Flight Testing, 69 Fed. Reg. 65,619 (Nov. 15, 2004).

⁴The Privacy Act requires that an agency publish a system of records notice in the *Federal Register* upon establishment or revision of the existence and character of any system of records. See § 552a(e)(4). The notices also addressed requirements of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, which requires agencies to conduct a privacy impact assessment before developing systems that collect, maintain, or disseminate information in an identifiable form, and the Paperwork Reduction Act of 1995, Pub. L. No. 104-13, 109 Stat. 163, which requires public notice of agency information collection proposals, which in this case was the proposed order to the airlines to provide passenger name records.

⁵70 Fed. Reg. 36,320 (June 22, 2005).

⁶Passenger prescreening is the identification of aviation passengers that may pose a security risk before they reach the passenger screening checkpoint at airports.

Background

Following the events of September 11, 2001, and in accordance with the Aviation and Transportation Security Act,⁷ TSA took action to enhance passenger prescreening operations. In March 2003, TSA began developing a new Computer-Assisted Passenger Prescreening System, known as CAPPS II, as a means of enhancing security through passenger prescreening. However, following our review of this program in February 2004, and a DHS internal review, DHS canceled CAPPS II's development in August 2004, due in part to concerns about privacy issues.⁸ That same year, TSA announced plans to develop a new passenger prescreening program known as Secure Flight. Under the Secure Flight program, TSA plans to take over from commercial airlines the responsibility for comparing information on domestic airline passengers against information on known or suspected terrorists. In addition, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004,⁹ establishing requirements that TSA assume this passenger prescreening responsibility.

As part of Secure Flight's development, TSA contractors conducted tests to identify data elements needed to make accurate comparisons between airline reservation system data and government watch list data. TSA contractors also conducted tests to determine if the use of commercial data could improve the results of watch list comparisons. To accomplish this, TSA collected information from airline reservation systems—including passenger name, flight reservation date, and flight number—for passengers who flew during June 2004. This type of information is contained in the passenger name record (PNR). Also, to test the use of commercial data, TSA contractors collected and used commercially available data maintained by private companies. Commercial data providers maintain databases that contain personal information, such as name, address, phone number, date of birth, and social security number, among other identifiers.

The Privacy Act regulates federal agencies' use of personal information and allows citizens to learn how their personal information is collected, maintained, used, and disseminated by the federal government.¹⁰ The act applies to personal information maintained by federal agencies or their contractors in a "system of records" from which records are retrieved by name or other personal identifier.¹¹ The Privacy Act requires agencies to disclose information to the public regarding the collection of personal information through a system of records notice (SORN) published in the

⁷Aviation and Transportation Security Act, Pub. L. No. 107-71, § 136, 115 Stat. 597, 636-37 (2001).

⁸For more information on the CAPPS II program, see GAO, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: Feb. 12, 2004).

⁹The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4012, 118 Stat. 3638, 3714-19, requires that TSA begin to assume performance of the passenger prescreening function within 180 days after the completion of testing.

¹⁰Many provisions of the Privacy Act are based on fair information practices—a set of internationally recognized privacy protection principles—including the requirement to keep collection of personal information limited, to specify the collection's precise purpose, to limit the use of collected data, to notify individuals subject to data collection, and to give those individuals the opportunity to access the information collected about them and request corrections.

¹¹Government contractors are bound by the Privacy Act provided they are operating a system of records on behalf of an agency to accomplish an agency function. § 552a(m).

Federal Register.¹² This notice must be issued upon establishment or revision of any system of records, and it must address specific types of information and “routine uses”—the specific uses planned by the agency—for the records contained in the system. More specifically, a SORN is to include a system’s name and location, the categories of individuals included, the categories of records maintained, the use of records, the policies and practices regarding storage and maintenance of records, and agency procedures whereby individuals can be notified that they are subject to having their data collected, among other requirements.¹³

Scope and Methodology

To assess key aspects of TSA’s disclosure of its use of personal information during commercial data testing for Secure Flight as required by the Privacy Act, we reviewed the provisions of the Privacy Act and the Secure Flight privacy notices, including the SORN and privacy impact assessment. As TSA developed and conducted its commercial data tests, TSA provided us with the statement of work, contract, contract modifications, test plans, and draft test results. We analyzed these documents and met with TSA officials and TSA contractors responsible for Secure Flight testing to discuss the scope and methodology of commercial data testing. In addition, we also met with DHS and TSA officials to discuss Secure Flight privacy notices and privacy issues we identified related to commercial data testing. We also compared TSA’s amended privacy notices, issued on June 22, 2005, with the fall 2004 privacy notices with regard to the issues addressed in this report. We did not evaluate whether TSA made any uses beyond testing of personal information it collected. We also did not review other aspects of privacy related to Secure Flight testing, including TSA’s internal controls for monitoring compliance with Privacy Act requirements. We will continue to assess privacy protections as part of our ongoing review of the Secure Flight program. We conducted our work in accordance with generally accepted government auditing standards from February 2005 through July 2005.

TSA’s Disclosure of Its Use of Personal Information from Commercial Sources Was Not Consistent with Privacy Act Requirements

Descriptions of how TSA planned to use personal information from commercial sources during Secure Flight testing, as published in the *Federal Register* in September 2004 and November 2004, differed in scope from how the data were actually used. As a result, the agency did not provide appropriate disclosure about its collection, use, and storage of personal information as required by the Privacy Act. For example, TSA collected and stored commercial data records even though TSA stated in its privacy notices that it would not do so.

¹²Apart from the Privacy Act, the E-Government Act requires agencies to describe similar privacy protections in a privacy impact assessment, which addresses what information is to be collected, the intended use of the information, with whom the information will be shared, what notices or opportunities for consent would be provided to individuals regarding what information is collected, how the information will be secured, and whether a system of records is being created.

¹³See § 552a(e)(4).

TSA's Scope and Objectives of Commercial Data Testing Differed from Fall 2004 Public Disclosure Notices

In September 2004, TSA published its SORN for Secure Flight testing in the *Federal Register*, as required by the Privacy Act, disclosing its plans to use personal information during Secure Flight testing.¹⁴ However, the way TSA's contractors used information to conduct commercial data tests differed from the usage disclosed in TSA's fall 2004 privacy notices. Specifically, TSA's contractors used PNR data supplemented with commercial data to determine if commercial data could be effective in eliminating incorrect matches against the government's consolidated terrorist watch lists. However, in its fall 2004 privacy notices, TSA did not identify its plans to supplement PNR data with commercial data.

In testing the usefulness of commercial data to enhance watch list comparisons, a TSA contractor verified passenger identities and then added commercial data to PNRs in order to make them as complete as possible for comparing against terrorist watch lists. To carry out these steps, a TSA contractor sent three commercial data providers approximately 240,000 names, which included 43,000 names from a subset of the June 2004 PNR data and variations of those names, to obtain commercial data for testing. According to TSA officials, this approach obscured the identities of those individuals represented in the PNR data in an attempt to protect their privacy. For example, the name John Doe, an actual passenger, could have been included in the names sent to commercial data providers along with such variations as Jon Doe, John Dough, and J. Doe. As requested by a TSA contractor, the commercial data providers sent back to the contractor records matching those names, which totaled over 100 million records. These records included information on individuals who did not fly in June 2004 and included data elements beyond those requested by TSA's contractor.¹⁵ According to TSA, its contractors used data elements requested for testing, such as names, dates of birth, address information, and phone numbers received from the commercial data providers, in an attempt to verify the identities of those represented in the PNR data. Following the identity verification process, the commercial data records that were determined to be the best match were then used to fill in data elements that were missing from the PNR data. In turn, these supplemented PNRs were provided to TSA for enhanced matching against data from the terrorist watch lists.

TSA's statement of work for commercial data testing, which was posted on the *Federal Business Opportunities* Web site on January 26, 2005,¹⁶ indicated the agency's plans to use commercial data to supplement the PNR data and to provide

¹⁴This discussion focuses on our assessment of TSA's description of its test in its fall 2004 SORN, as required by the Privacy Act, and Notice of Final Order. Because TSA similarly described its test in its fall Privacy Impact Assessment, our discussion generally applies to TSA's fall privacy impact assessment as well.

¹⁵The TSA contractor that purchased commercial data requested data elements such as name, date of birth, gender, and telephone number, among others. The TSA contractor also received other data elements as well, such as social security numbers, but TSA officials said these data elements were not used during testing.

¹⁶*Federal Business Opportunities*, Jan. 26, 2005. <http://www2.eps.gov/servlet/Documents/R/1090245/552071> (accessed July 6, 2005).

the enhanced PNRs to the government for matching against data from the terrorist watch lists.¹⁷ TSA also described in more detail its methods for supplementing these records in test plans of March 17, 2005, and April 5, 2005, and its draft final test results report of May 10, 2005. However, these latter documents were not released to the public.

TSA Did Not Collect, Use, and Store Data in Accordance with Privacy Act Requirements

In testing the use of commercial data, TSA's contractors collected, used, and stored personal information from commercial sources in ways that were inconsistent with disclosures in TSA's fall 2004 privacy notices as discussed below. As a result, the public did not receive the full protections of the Privacy Act. Specifically, TSA did not fully inform the public of: (1) the subjects of data collection, (2) the types of personal data to be collected, (3) the full purpose of collecting the data, (4) policies and practices regarding storage and maintenance of the data, and (5) how those subject to having their personal data collected could access and amend their data.

First, under the Privacy Act, agencies must disclose the categories of individuals on whom records are collected and maintained and the agencies' procedures for notifying individuals, when requested, if information collected pertains to them. TSA's commercial data testing involved more individuals than disclosed in its original privacy notices. The fall 2004 privacy notices stated that only those who were passengers on domestic flights in June of 2004 would be subject to collection. However, additional individuals who may not have flown during June 2004 were subject to having data collected if their names were similar to the names of individuals represented in PNR data.

Second, the Privacy Act requires disclosure of the categories, or types, of information collected and maintained by an agency in a system of records. A TSA contractor collected types of data for commercial data testing other than those TSA publicly disclosed in its fall 2004 privacy notices. In describing information to be collected and used for the system, the privacy notices refer only to PNR data to be obtained from airlines. Although TSA's contractors collected or used personal information from commercial sources for Secure Flight testing, the privacy notices stated that only "authentication scores and codes" would be obtained from commercial data providers. While PNR data are directly related to a passenger's reservation and travel itinerary, commercial data may include a wide variety of other personal information, such as social security numbers, credit reports, and gender, among other information.

Third, the Privacy Act specifies that information collected for one purpose may not be used for another purpose without notice to, or consent of, individuals subject to having their data collected. TSA's contractors used commercial data for purposes

¹⁷ Although the statement of work was publicly available through the *Federal Business Opportunities* Web site, any revisions or amendments to the SORN would need to be published in the *Federal Register* to conform to Privacy Act requirements.

that TSA did not disclose in its fall 2004 privacy notices. The privacy notices stated that TSA would use commercial data to identify PNR data that was incorrect or inaccurate. However, in addition to the publicly disclosed purpose, a TSA contractor used commercial data to fill in data that were missing from the PNR data, such as full name. The contractor also used the commercial data to capture additional information not consistently found in PNRs, such as date of birth.

Fourth, pursuant to the Privacy Act, agencies must disclose their policies and practices regarding storage, retrievability, access controls, retention, and disposal of records containing personal information. TSA did not indicate how it would access, retrieve, retain, and dispose of the commercially obtained personal data or how it would apply controls regarding the maintenance of such data. In addition, TSA's privacy notices stated that TSA would not store commercially obtained personal data. However, TSA and TSA contractors did store this data based on two separate data collection activities that compiled more than 100 million commercial data records.

Fifth, under the Privacy Act, agencies must disclose their procedures for allowing individuals to access any records pertaining to them and provide a means for contesting the content of such records. While TSA offered airline passengers who flew during June 2004 an opportunity to access or request to amend their PNR data, they did not make a similar provision for individuals represented in the commercial data that was collected. TSA collected more than 100 million commercial data records during commercial data testing. As a result, an unknown number of individuals whose personal information was collected were not notified as to how they might access or amend their personal data.¹⁸

On June 10, 2005, we briefed TSA on these concerns about privacy protection issues related to Secure Flight testing. TSA officials stated they recognized the merits of GAO's concerns, and on June 22, 2005, the agency published revised privacy notices to more fully disclose the nature of tests being conducted. TSA officials further stated that the use of commercial data was limited to testing and did not involve determinations affecting any individuals. Specifically, officials stated that they did not use test data in making passenger prescreening decisions or to provide information on potential terrorist activity to law enforcement officials.¹⁹ While it appears that no determinations were made by TSA with regard to air travel by specific individuals on whom it had collected data, these people were unable to exercise their rights of access to their information. In addition, these individuals, as well as the general public, were not informed as to how personal information would be used and did not have the opportunity to comment on TSA's use of the data.

¹⁸The TSA contractor did not determine how many individuals were represented in the more than 100 million commercial data records it received.

¹⁹We did not assess whether there were any resulting effects on individuals.

TSA Issued Revised Privacy Notices and Plans to Further Address Secure Flight Privacy Issues

TSA issued revised privacy notices on June 22, 2005, to clarify and describe with greater particularity who was subject to having their data collected, and the type of data collected, during Secure Flight commercial data tests. In its revised notices, TSA clarified that the Secure Flight test system of records includes individuals identified in commercial data purchased and held by TSA contractors, and that the Secure Flight test system of records included PNRs that were enhanced with certain commercial data elements which were provided to TSA (commercial data that was purchased and held by TSA contractors). In addition, the notices identified that the purpose of the Secure Flight test includes testing the government's ability to verify the identity of passengers, and to improve the efficacy of watch list comparisons by making passenger information more complete and accurate using commercial data. The notices further stated that commercially obtained personal data were stored in at the Office of Transportation Vetting and Credentialing (OTVC) in Annapolis Junction, Maryland; the OTVC assessment facility in Colorado Springs, Colorado; and at a contractor's headquarters in McLean, Virginia. The data were stored on magnetic disc, tape, digital media, CD-ROMs, and may also have been retained on paper. TSA's revised notices also identified that all persons may request information about them contained in the system of records by writing to the TSA Privacy Officer.

Although TSA did not fully disclose its plans to use personal information in its fall 2004 privacy notices as required by the Privacy Act, TSA officials stated that steps were taken by the agency and the agency's contractors to secure the commercial data obtained to ensure that personal information was not inappropriately accessed during testing. For example, according to TSA officials, they sent commercial data providers names using a secure file transfer protocol and e-mail, and data were loaded into a database on test and analysis computers in a secure lab and locked in a safe when not in use. TSA officials also stated that the discs containing PNR data enhanced with commercial data are being stored in a secure government safe at OTVC in accordance with the data-handling policy developed and approved by TSA's Privacy Officer. TSA officials also stated that access to personal information was, and continues to be, limited to only those TSA employees and contractors who have a "need to know," and each employee and contractor associated with the Secure Flight training has completed mandatory privacy training prior to beginning work on the program. We have not assessed the adequacy of TSA's security controls for commercial data testing as part of this review.

Finally, TSA officials stated that as the Secure Flight program moves from a testing environment to operations, which is expected to begin in late 2005 or early 2006, they will take additional steps to protect privacy. For example, TSA officials stated they will put procedures in place to ensure that prior to making any change in testing procedures, the TSA Privacy Officer and TSA counsel would be consulted to determine whether a change to TSA's SORN and privacy impact assessment would be required. TSA officials further stated that the agency will defer any decision on how

commercial data might be used by Secure Flight, if at all, until the completion of the test period, assessment of the test results, and publication of subsequent privacy notices announcing the intended use of such commercial data. TSA officials stated that the agency does not plan to use personal information collected from commercial sources during the initial operations of Secure Flight, but will consider the use of such data in the future if the data can be shown to improve the ability of Secure Flight to identify known or suspected terrorists.

Concluding Observations

Because the Secure Flight program involves, by design, personal information, it is important that TSA be vigilant with respect to individual privacy protections and fully disclose uses of personal information prior to accessing such data. In its fall 2004 notices, TSA informed the public of its plans to use personal information during Secure Flight testing, including the use of commercial data in a limited manner. However, these initial notices did not fully describe how personal information would be collected, used, and stored for commercial data testing. As a result, individuals were not fully informed of their personal information being collected and used, nor did they have the opportunity to comment on this or become informed on how they might exercise their rights of access to their information. Although TSA did not fully disclose its use of personal information prior to beginning Secure Flight testing, the agency recently issued revised privacy notices to more fully disclose the nature of these tests, and address the issues identified in this letter. Issuing the revised notices is an appropriate step to more fully inform the public of its use of personal information.

Agency Comments and Our Evaluation

We provided a draft copy of this letter to DHS for its review and comment. On July 21, 2005, we received written comments on the draft letter which are reproduced in full in Enclosure I. DHS generally agreed with our findings, and stated that TSA acted immediately to address the issues identified in this letter. DHS also affirmed its commitment to adhere to the letter and intent of the Privacy Act and applicable policies on privacy protections. DHS further stated that its Chief Privacy Officer initiated an assessment of TSA's handling of passenger information during Secure Flight commercial data testing. In addition, DHS stated that it had shared information regarding its privacy efforts with Congress, air carriers, and privacy groups, and stated that GAO reviewed all testing parameters prior to TSA's commencement of commercial data testing in mid-March 2005. Finally, DHS described data security controls that it put in place to protect commercial data from unauthorized access and to prevent system abuses. DHS also provided technical comments on the draft, which we incorporated as appropriate.

We believe that DHS' stated commitment to adhere to the letter and intent of the Privacy Act and applicable policies is an important step in addressing privacy protections, and we look forward to the results, including recommendations, if any,

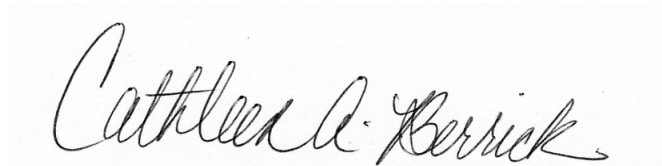
of the DHS Chief Privacy Officer's on-going privacy assessment related to commercial data testing. Regarding DHS' assertion that GAO reviewed all testing parameters prior to TSA's initiation of commercial data testing, we were not able to fully assess TSA's plans for commercial data testing prior to the initiation of testing because TSA did not provide to GAO its complete test plans or related details from the testing contractor until April 2005. Further, while we believe stakeholder coordination related to privacy protections is important, TSA is ultimately responsible for fully disclosing its use of personal data during testing to the public in accordance with Privacy Act requirements. Finally, we did not review the effectiveness of TSA's reported security controls related to commercial data.

* * * * *

We are sending copies of this letter to the Secretary of the Department of Homeland Security, the Director of the Transportation Security Administration, and the Assistant Administrator for Secure Flight/Registered Traveler. Copies of this letter will be made available to others upon request. In addition, the letter will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this letter, please contact us at (202) 512-3404 (berrickc@gao.gov) or (202) 512-6240 (koontzl@gao.gov). Other key contributors to this report were Amy Bernstein, John de Ferrari, Christine Fossett, Brent Helt, R. Denton Herring, Adam Hoffman, David Hooper, Thomas Lombardi, C. James Madar, David Plocher, and Jamie Pressman.

Sincerely yours,



Cathleen A. Berrick, Director,
Homeland Security and Justice Issues



Linda D. Koontz, Director
Information Management Issues

List of Congressional Committees

The Honorable Thad Cochran
Chairman

The Honorable Robert C. Byrd
Ranking Minority Member
Committee on Appropriations
United States Senate

The Honorable Judd Gregg
Chairman

The Honorable Robert C. Byrd
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable Ted Stevens
Chairman

The Honorable Daniel K. Inouye
Co-Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Conrad Burns
Chairman

The Honorable John D. Rockefeller IV
Ranking Minority Member
Subcommittee on Aviation
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Arlen Specter
Chairman

The Honorable Patrick Leahy
Ranking Minority Member
Committee on the Judiciary
United States Senate

The Honorable Susan M. Collins
Chairman

The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jerry Lewis
Chairman
The Honorable David R. Obey
Ranking Minority Member
Committee on Appropriations
House of Representatives

The Honorable Harold Rogers
Chairman
The Honorable Martin Olav Sabo
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

The Honorable Christopher Cox
Chairman
The Honorable Bennie G. Thompson
Ranking Minority Member
Committee on Homeland Security
House of Representatives

The Honorable Don Young
Chairman
The Honorable James L. Oberstar
Ranking Democratic Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

Enclosure I: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



Homeland Security

July 20, 2005

Cathleen Berrick
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Berrick:

Thank you for the opportunity to comment on GAO's letter report regarding privacy issues related to testing of the Secure Flight Program entitled, "*Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*" GAO-05-864R.

As the Department of Homeland Security (DHS) has demonstrated over the past several weeks, we take very seriously the concerns that GAO brought forward on June 10, 2005 regarding commercial data testing during the period between mid-March and mid-June of 2005, regarding privacy protection issues related to Secure Flight testing. TSA recognized the merits of GAO's technical concerns and acted immediately to address them.

As you know, commercial data testing began in mid-March of 2005, after GAO reviewed all testing parameters. Upon GAO's notification of its concerns, TSA published a notice on June 22, 2005, to supplement and amend the existing Privacy Act system of records notice (SORN) and Privacy Impact Assessment (PIA) for Secure Flight testing. The revised notices clarified the purpose of commercial data testing for Secure Flight and expanded the categories of records and individuals covered by the SORN. TSA also put procedures in place to ensure that prior to making any change in testing procedures, the TSA Privacy Officer and TSA counsel will be consulted to determine whether a change to the SORN or PIA are necessary.

Full Disclosure of Commercial Data Testing Plan

As you point out in your draft letter, the purpose of the Secure Flight commercial data test is to evaluate the Government's ability to verify the identities of passengers using

www.dhs.gov

commercial data and to improve the efficacy of watch list comparisons by making passenger information more complete and accurate using commercial data.

On September 24, 2004, TSA published in the *Federal Register* a number of documents necessary to allow the agency to begin testing the Secure Flight program. These included: (1) a proposed order to U.S. aircraft operators directing them to provide a limited set of historical passenger name records (PNRs) to TSA for use in testing the program (69 FR 57342); (2) a Privacy Act System of Records Notice (SORN) for records involved in testing the program (69 FR 57345); and (3) a Privacy Impact Assessment (PIA) for program testing (69 FR 57352). These documents explained that in addition to testing TSA's ability to conduct automated watch list comparisons for purposes of the Secure Flight program, TSA intended to conduct a separate test to determine whether the use of commercial data would be effective in identifying passenger information that is incorrect or inaccurate. At the time TSA issued the notices, the details of the plan for commercial data testing had not been finalized. Therefore, the September 2004 notices fully disclosed TSA's plan for commercial data testing, to the extent the plan had been developed at that time.

Commercial data testing began in mid-March of 2005, after GAO reviewed all testing parameters. When in mid-June 2005 GAO raised concerns about discrepancies between the description of the commercial data testing in the September 2004 notices and certain aspects of the way the test ultimately was conducted, TSA acted immediately to address those concerns as soon as they were brought to our attention. TSA provided briefings beginning in December 2004 regarding privacy efforts to Congress, Air Carriers and privacy groups regarding the testing and has been cooperating with GAO audits since Spring of 2004. In addition, commercial data records collected by the TSA contractor were used for testing purposes only and were not used in whole or in part in making any determination about an identifiable individual.

No decision has yet been made on whether commercial data will ultimately be used in Secure Flight. If TSA decides to use commercial data for Secure Flight, it will not do so until the agency publishes a new SORN and PIA announcing how commercial data will be used and how individuals' privacy will be protected. The initial rollout of Secure Flight will include only watch list checking, as directed by the House Appropriations Committee earlier this year.

TSA Maintains Stringent Data Protection Practices

TSA has employed data security controls to protect the data used for Secure Flight testing activities. 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.

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. TSA and its contractors' systems and facilities on which the tests are or have been conducted were assessed by the TSA Chief Information Officer (CIO) and other TSA officials for security risks, and TSA has implemented security policies and plans consistent with statutory, regulatory and internal DHS guidance.

Measures that are in place include the following:

- Access to private information is limited to only those TSA employees and contractors who have a "need to know" to perform their duties associated with Secure Flight operations;
- A detailed log of all instances in which data are transferred or accessed;
- Data are maintained at a secure facility, and 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;
- Each employee and contractor associated with the Secure Flight program has completed mandatory privacy training prior to beginning work on the program;
- TSA, in consultation with the TSA Privacy Officer, has established chain-of-custody procedures for the receipt, handling, safeguarding, and tracking of access to the PNR data;

Finally, at the conclusion of testing and GAO's review, all passenger and commercial data used for testing will be destroyed.

TSA is Committed to Protecting Personal Privacy

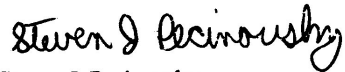
In March, 2004, TSA established Privacy Principles that every employee is required to follow in the design and development of programs as well as in collecting and using personal information about members of the public for use in those programs. The TSA Privacy Officer regularly communicates with program offices during the development and implementation of agency programs. In addition, program offices are required to consult with the TSA Privacy Officer on privacy matters affecting agency programs.

The Deputy Secretary has requested the DHS Chief Privacy Officer to assess the handling of passenger information and commercial data during the testing phase and to provide any recommendations about how to strengthen our focus on privacy protection as we continue testing and contemplate deployment of Secure Flight. The Deputy Secretary has made the same request of the Department's new Data Privacy and Integrity Advisory Committee. In addition, the Aviation Security Advisory Committee (ASAC) established the Secure Flight Privacy/IT Working Group in September 2004, which has been reviewing the development of the Secure Flight program and is expected to present its recommendations to the ASAC in the near future regarding Secure Flight.

The Department is resolute in our commitment to adhere to the letter and intent of the Privacy Act and applicable policies on privacy protection. Moreover, we have continuously consulted with various privacy advocates to seek best practices and share details about this important program, and TSA will continue to work with the DHS Privacy Officer on the privacy issues relating to Secure Flight.

Thank you again and we look forward to our continued work together to enhance the nation's transportation security. We appreciate the opportunity to contribute comments to the draft report. For further information for readers of this report, please contact TSA public affairs at (571) 227-2829.

Sincerely,



Steven J. Pecinovsky
Director, Departmental GAO/IG Liaison Office
Department of Homeland Security