DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data (Redacted)

The Department of Homeland Security, Office of Inspector General, has redacted this report for public release under the Freedom of Information Act, 5 U.S.C. § 552(b)(4).

Office of Inspections, Evaluations, & Special Reviews

OIG-05-12

March 2005

Office of Inspector General

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

Homeland Security

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared by the OIG as part of its DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses TSA's role in the use and dissemination of airline passenger data, assesses TSA's related disclosures, and evaluates the agency's operating environment with respect to privacy issues. It is based on interviews and exchanges with employees and officials of the Transportation Security Administration, other federal agencies, and contractors, as well as a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Acting Inspector General

Contents

Contents

Appendices

Figures

Contents

Abbreviations

AAI	Airline Automation, Inc.
ACLU	American Civil Liberties Union
ATSA	Aviation and Transportation Security Act
ADI	Airline Data Interface
AVOPS	Transportation Security Administration, Aviation Operations
CAPPS	Computer Assisted Passenger Pre-screening System
CAPPS II	Computer Assisted Passenger Pre-screening System, Second Generation
CD	Compact Disc
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CPO	Chief Privacy Officer
CRS	Computerized Reservation System
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	Department of Transportation
FAA	Federal Aviation Administration
Fed. Reg.	Federal Register
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
GAO	Government Accountability Office
GDS	Global Distribution System
IBM	International Business Machines Corporation
MOU	Memorandum of Understanding
OCC	Transportation Security Administration, Office of Chief Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget, Executive Office of the President
ONRA	Transportation Security Administration, Office of National Risk Assessment
PIA	Privacy Impact Assessment
PNR	Passenger Name Record
RAE	Risk Assessment Engine
TSA	Transportation Security Administration
SCPC	Selectee Checkpoint Program Completion Team
U.S.C.	United States Code
USSS	United States Secret Service

Contents

Introduction

TSA has authority to access and obtain airline passenger data under provisions of its enabling statute, the *Aviation and Transportation Security Act* (*ATSA*) of November 2001.[1] The Assistant Secretary[2] for TSA may establish policies and procedures requiring airlines to provide passenger data in order to protect transportation security.[3] The Assistant Secretary is further authorized to require "passenger air carriers to share passenger lists … for the purpose of identifying individuals who may pose a threat to aviation or national security."[4]

As the federal agency in charge of aviation security, TSA is also responsible for providing oversight of passenger pre-screening efforts.[5] Since 1998, airline passenger pre-screening has been performed using a data analysis application called the Computer Assisted Passenger Pre-screening System (CAPPS). After TSA assumed oversight of passenger pre-screening in February 2002, the agency began developing a second generation system, CAPPS II, to improve upon the existing system. TSA no longer plans to implement CAPPS II, and recently announced its intention to proceed with the testing and deployment of a new passenger pre-screening system, Secure Flight. Through its efforts to implement the Secure Flight system, TSA will continue to work with airline passenger data. The agency's handling of airline passenger data will, therefore, continue as TSA seeks to fulfill this mission.

In February 2004, the Department of Homeland Security (DHS) Privacy Office issued a *Report to the Public on Events Surrounding jetBlue Data Transfer* in

[1] Public Law No. 107-71.
[2] ATSA established TSA under the Department of Transportation. The head of TSA was the Under Secretary of Transportation for Security. Under the Homeland Security Act of 2002, Public Law 107-296, TSA transferred to DHS. The head of TSA is now referred to as the Assistant Secretary of Homeland Security for the Transportation Security Administration.
[3] 49 U.S.C. § 114(d)(1), § 114(e), and § 44901(a).
[4] The Assistant Secretary must consult with the Transportation Security Oversight Board before establishing this requirement. 49 U.S.C. § 114(h)(4).
[5] 49 U.S.C. § 44903(j)(2).

connection with one of the data exchanges covered in this review.[6] In its report, the DHS Privacy Office referred its findings to the DHS Office of Inspector General (OIG) for further review.[7] The U.S. Army OIG independently conducted an investigation into the same transfer and published a report on June 21, 2004. Neither of these reports addressed the other cases of airline passenger data sharing discussed in this review or TSA's disclosures associated with those exchanges.

Results in Brief

In reviewing TSA's role in the use and dissemination of airline passenger data, we focused on data sharing in three contexts.[8] First, we examined TSA's efforts to support the provision of airline passenger data to other agencies and their contractors. Second, we explored airline passenger data transfers associated with the Second Generation, Computer Assisted Passenger Pre-screening System (CAPPS II). Third, we reviewed TSA's role in obtaining airline passenger data to improve the current CAPPS. We did not review TSA's use or transfer of airline passenger data for investigative, law enforcement, or other purposes.

In addition to TSA's role in the use and dissemination of airline passenger data, we reviewed TSA's disclosures of information associated with its involvement in airline passenger data transfers. Finally, we reviewed measures TSA has taken to address data privacy and confidentiality issues.

We examined information related to TSA's role in fourteen transfers of airline passenger data.[9] In two cases, these transfers did not result in any data review or analysis on the part of the recipients. Collectively, the remaining transfers involved more than 12 million records associated with passengers traveling on at least six air carriers – America West Airlines, American Airlines, Continental Airlines, Delta Air Lines, Frontier Airlines, and JetBlue Airways.

[6] JetBlue Airways' corporate logo represents the airline's name with a lowercase "j." Accordingly, the DHS Privacy Office spelled "jetBlue" with a lowercase "j" in its report. Because the airline's incorporated name, "JetBlue Airways Corporation," appears with a capital "J," we have adopted this spelling in the body of our report.
[7] DHS Privacy Office, *Report to the Public on Events Surrounding jetBlue Data Transfer*, February 20, 2004, p. 9.
[8] As used in this report, "data sharing" refers to the transfer of data from one entity to another. Under this definition, data sharing includes the transfer of data in one direction, and does not necessarily imply two-way data transfers between the parties to the sharing.
[9] Under the definition above, a transfer of several sets of records from one entity to another is counted as a single transfer.

The fourteen transfers took place between February 2002 and June 2003. In two instances of airline passenger data exchange, TSA sought to support the national security functions of other agencies by facilitating transfers. In eleven cases, TSA was engaged in efforts to develop CAPPS II. In one case, TSA obtained records in order to study improvements to its existing CAPPS program. The information that we gathered and analyzed with respect to all of these exchanges indicated that, in each case, these data transfers were executed in the performance and support of TSA's responsibilities to improve transportation security.

According to the parties who received data in all but three of these transfers, the transferred data has been destroyed or is retained in a secured setting. The firm associated with the three remaining transfers did not provide information for our review and, as a result, we have no information on the final disposition of related passenger data. In all but one case, information communicated in the transfers was used for research purposes and did not result in any agency determinations regarding individuals reflected in the data.

In its role in these transfers, however, TSA did not ensure that privacy protections were in place for all of the passenger data transfers. While TSA applied privacy protections in some contexts, shortcomings were also apparent in the agency's related contracting, oversight, and follow-up efforts.

Although TSA and the Federal Aviation Administration (FAA), acting on TSA's behalf, included language safeguarding the security and confidentiality of passenger information in some contracts and agreements, they did not do so in all cases. In one case, the parties to a data transfer did not sign any contract or agreement restricting the use or disclosure of shared data. Even when the parties to a data transfer were bound by agreement, TSA failed to monitor and enforce adherence to the terms of the agreement completely. In addition, TSA did not consistently track the usage, security, or disposition of passenger data and was, therefore, not in a position to determine whether such usage, security, or disposition was appropriate.

Nevertheless, most of the transfers that we reviewed were executed between parties bound by agreements forbidding additional sharing or disclosure of the passenger information. Of the more than 12 million records transferred, a passenger's data was inappropriately disclosed to the public in only one instance. In this instance, a government contractor's inappropriate disclosure of information was inadvertent.

CAPPS II and TSA staff viewed passenger data in only three cases. In one of those instances, TSA did not demonstrate the effective use of sound privacy practice.

In 2003 and 2004, TSA officials made inaccurate statements regarding these transfers that undermined public trust in the agency. These misstatements were apparently not meant to mischaracterize known facts. Instead, they were premised on an incomplete understanding of the underlying facts at the time the statements were made.

Errors in TSA's statements about these airline passenger data transfers arose from internal document collection efforts that were incomplete and, in one case, from inaccurate information from an airline. Early shortcomings in the production of related documents have been improved by recent efforts within the agency to provide for full disclosure.

TSA's policy environment with respect to privacy has changed substantially since its inception. From its inception, TSA recognized personal privacy and confidentiality as important concerns. Especially in the immediate aftermath of the September 11, 2001, attacks, finding a balance between these concerns and transportation and aviation security was a difficult challenge. Over the past twenty months, a number of important changes have expanded the prominence of privacy concerns in the agency's operations. Major new privacy legislation is now in effect, and both DHS and TSA have dedicated staff to enforce this legislation.[10] In addition, program changes and the evolving public relations position of the agency have helped foster a new organizational culture with respect to matters of privacy. While TSA continues to balance privacy and security, its declared commitments to both goals have been corroborated by its recent actions.

We are recommending that the Assistant Secretary for Transportation Security, in coordination with the Chief Privacy Officer, as appropriate:

1. Develop clear protocols for obtaining airline passenger data and facilitating its exchange among other parties.

2. Ensure privacy and personal data protections are written into acquisition documents where performance may involve the collection, maintenance, use, or dissemination of individually identifiable data.

[10] Title II of the E-Government Act of 2002, Public Law No. 107-347, went into effect on April 17, 2003.

3. Require final reporting for acquisitions with intensive data analysis or processing components that addresses data receipt, processing, distribution, utilization, and disposition, as well as attention to data security and privacy.

4. Require entities performing work for TSA to report to the agency on how they are addressing data security, privacy protections, and confidentiality.

5. Re-evaluate TSA's response to FOIA requesters who solicited information in September 2003 regarding their airline passenger data. Such a reevaluation should, at minimum, involve the removal or amendment of the letter posted on TSA's FOIA reading room web site to reflect the fact that TSA is in possession of JetBlue passenger data.

6. Adopt procedures for responding to external and intra-departmental requests for information that help guarantee a comprehensive, timely, and reliable response.

7. Appoint a TSA external privacy advisory board, as specified in TSA's five-point plan, to review all agency privacy impact assessments, and, to provide consultation regarding the scope and methods of TSA supported data analysis and research involving individually identifiable data.

8. Develop procedures that will provide a clear process to: (1) approve the agency's role in data sharing that involves individually identifiable information; and, (2) identify a particular employee responsible for monitoring the data security, usage, and final disposition of each transfer of individually identifiable information in which TSA becomes involved.

Background

The Computer Assisted Passenger Pre-screening System (CAPPS)

Prior to the terrorist attacks of September 11, 2001, U.S. airlines analyzed airline passenger data to support aviation security for more than three years. Data submitted to airlines in the course of commercial transactions was routinely analyzed to identify "selectees" – individuals to receive additional security

screening. This data analysis was performed using a computer application called CAPPS. The system was established in 1998, based on development efforts begun in 1994 at Northwest Airlines in conjunction with funding from the FAA.

Aviation and security experts considered CAPPS an improvement in methods of screening potential threats to aviation from a large and expanding passenger base. The CAPPS program was structured to address various security, privacy, and civil rights concerns. First, to reduce predictability and mitigate efforts to reverse engineer the system, CAPPS included an element of randomness in passenger selections. Second, to address concerns about data retention, officials guaranteed that no CAPPS information on passengers was retained after the safe completion of their flight. Third, to ensure that the system was not discriminatory, CAPPS was reviewed by the U.S. Department of Justice and determined not to discriminate illegally against travelers, or involve any invasion of passengers' personal privacy.[11]

There were inherent CAPPS limitations, however. The system's decentralization figured prominently among these limitations. Significantly, CAPPS was regulated by the FAA and operated by the airlines. The FAA supplied scoring rules for flagging selectees, and the airlines used these rules to evaluate their passenger data, generate scores for each passenger, and determine whether a passenger would be selected for further security scrutiny. The decentralized nature of the system complicated the process of updating rules to reflect new information, such as intelligence about terrorist strategies and techniques.

The CAPPS system was also restricted in its informational reach. The CAPPS analysis was limited to airline passenger data provided by passengers to airlines and reservations systems. It did not: (1) access information on passengers from publicly available commercial data sources; (2) analyze passenger data for international flights operated by foreign carriers; or, (3) tap into information on government watch lists.

These CAPPS limitations and other aviation security weaknesses were most evident with the multiple hijackings and terrorist attacks of September 11, 2001. On that morning, the nineteen hijackers were screened prior to boarding four aircraft according to security measures in effect at the time. Seven of the hijackers were among passengers chosen for additional security scrutiny based on scores generated by CAPPS; two hijackers were selected for extra scrutiny

[11] U.S. Department of Justice press release, "Justice Department Review of FAA Passenger Screening Proposal Concludes It Won't Discriminate Against Airline Travelers," October 1, 1997.

by an airline representative who found them to be suspicious; and one hijacker was selected at random for additional security measures. As noted in the *9/11 Commission Report*, the only consequence of the hijackers' selection was that their checked bags were submitted to additional scrutiny.[12]

Second Generation Computer Assisted Passenger Pre-screening System (CAPPS II)

Authority to manage and regulate the CAPPS system was conferred upon TSA when it assumed civil aviation security functions and responsibilities performed by FAA on February 17, 2002.[13] Department of Transportation (DOT) officials understood that TSA's November 2001 enabling statute, ATSA, mandated improvement of CAPPS; therefore, as early as December 2001, senior DOT officials started evaluating ideas for system improvements.

On March 1, 2002, transportation officials chartered the formation of a team to develop a second-generation pre-screening system, CAPPS II. Administrative support for the project was provided under a contract with TRW, and information and personnel resources were drawn from throughout the government. The CAPPS II program budget and contracting staff came from the FAA's Technical Center in Atlantic City, New Jersey. Two special advisors to the Secretary of Transportation were brought in to provide technical expertise on system development. Just as early CAPPS II development efforts called on resources within DOT, so, too, was knowledge and expertise outside of the department sought. Staff from the Department of Defense's (DOD's) Defense Advanced Research Projects Agency (DARPA) evaluated proposals and shared technical insights during the March through June 2002 time frame.[14] Also, CAPPS II program staff received consultative and evaluative assistance from officials working with the interagency Foreign Terrorist Tracking Task Force and U.S.

[12] TSA now provides additional screening of a selectee's person, in addition to their checked bags. See National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, July 22, 2004, Chapter 1, "We Have Some Planes," for more detail on the screening of the September 11, 2001 hijackers.

[13] Notice of Assumption of Civil Aviation Security Functions, 67 Fed. Reg. 7939 (Feb. 20, 2002).

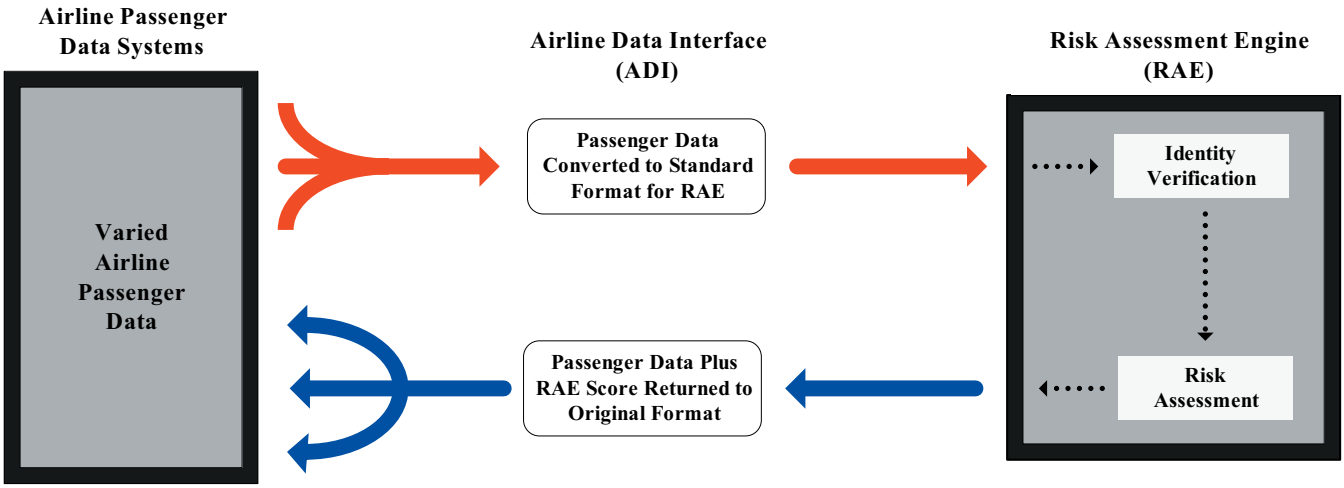
[14] Regarded as experts in automated risk assessment and systems development, the DARPA staff who helped evaluate proposals in the spring of 2002 were affiliated with DARPA's now defunct Total Information Awareness project. The Total Information Awareness project, which was later renamed "Terrorism Information Awareness," aimed to help predict terrorist attacks by creating an electronic network with the capability to identify patterns of suspect activity in commercial and government data systems. After expressions of concern by privacy advocates, Congress eliminated funding for the project in the 2004 Department of Defense appropriation (Public Law No. 108-87 § 8131(a)). Apart from this limited consultation, we found no other linkage between the CAPPS II program and the Total Information Awareness effort.

Customs. The MITRE Corporation also supported the CAPPS II proposal review and contracting process.

During the July through August 2002 time frame, management and oversight of CAPPS II development efforts shifted from the DOT chief information officer's (CIO's) office to the TSA CIO's office. Both the executive sponsor[15] and the program manager for the initiative changed. Program management changed once more in November 2002, when the project was moved to TSA's Office of National Risk Assessment (ONRA).

Despite changes in program management, the fundamental concept behind CAPPS II remained constant. From early 2002 forward, plans for an effective CAPPS II system depended on the interplay of two major system components. One system component, the Risk Assessment Engine (RAE), was to confirm the identity and assess the risk of passengers to aviation security. The other system component, the Airline Data Interface (ADI), in turn, was to serve as the conduit for passenger data to and from the RAE.

Figure 1. Overview of Major CAPPS II System Components



[15] An executive sponsor is typically responsible for: (1) providing general guidance to the project team, (2) serving as liaison between departmental leadership and the program manager, and (3) advocating for changes needed for effective program development at the leadership level.

Prior to the system's deployment, TSA needed to establish that CAPPS II and its constituent parts would function properly in a real world setting. Therefore, it was necessary to test the system's prototypes and components. The ADI component required testing to demonstrate that it could process large volumes of diversely structured data into a common format and return data in its original format with an appended passenger risk indicator. Testing was necessary because airline passenger data is maintained in a number of Computerized Reservation Systems (CRSes) and Global Distribution Systems (GDSes) that accumulate disparate sets of passenger data in varied formats. While some passenger data systems host limited information, others possess extensive data on individuals, including the details of past travel, car and hotel reservation plans, dates of birth, phone numbers, e-mail addresses, residential and business addresses, and credit card information. Records that reflect detail on individual passengers' travel plans and booking information are known as Passenger Name Records (PNRs). ADI specifications required that it have the initial capability to process two million individual PNRs daily.

For the RAE component, a demonstration was necessary to prove that the system could perform identity authentication functions using commercial data and cross-reference passenger data against government watch lists. The effectiveness of matching watch list information with commercial databases could be tested only using information on real people. Accordingly, on some scale it was necessary to use data on real people for RAE testing.

Statutory Requirements

In addition to the technical and functional challenges that TSA faced in pursuit of its mandate to pre-screen airline passengers, two statutes affected CAPPS II development: the Privacy Act and the E-Government Act.[16]

The Privacy Act contains a number of noteworthy data privacy protections. Provisions of the law, for example, restrict improper access to and disclosure of personal information. The Privacy Act also includes requirements that federal agencies publish information about records systems they maintain. The failure to comply with these and other aspects of the law can result in civil or criminal penalties.

[16] See Appendix G for further information on the Privacy Act and the E-Government Act.

These provisions of the Privacy Act are invoked, however, only when an agency's records meet the legal standard for a "system of records." A number of criteria must be met for a set of records to meet the standard for a system of records under the law. One criterion for meeting this standard is that an agency's records must be retrieved or accessed by the agency, or a proxy for the agency, using an individually identifying particular, such as name or social security number.

Under the Privacy Act, notices for all government systems of record are to be published in the Federal Register. Published systems of record notices document the authorities under which the government agency maintains the system of records, the purpose the system serves, the types of records contained in the system, and their routine uses. In response to this provision of the Privacy Act, DOT published an initial system of records notice for CAPPS II on January 15, 2003.[17] After reviewing public comments on the initial CAPPS II notice, TSA issued a revised Interim Final Notice for CAPPS II on August 1, 2003.[18]

Important provisions of the E-Government Act, a more recent statute applicable to CAPPS II development, took effect in April 2003. The E-Government Act requires all agencies to conduct Privacy Impact Assessments (PIAs) for new information technology investments and new electronic information systems and collections. The PIA development process was designed to ensure that data handling complies with relevant laws, that agencies consider the risks and effects of their data systems, and that they examine system design alternatives to reduce privacy risks. Ultimately, PIAs result in published documents that address the above specified issues and provide greater detail about government information systems than are required for Privacy Act system of records notices.[19]

Public Disclosure of Information

To foster development and testing of CAPPS II and support improvements to the original CAPPS, TSA participated in twelve airline passenger data transfers in 2002 and 2003. TSA had a role in two additional passenger data transfers in 2002 to support the work of other agencies. The public's first awareness of any of these transfers came in September 2003.

In September 2003, the media reported on a transfer of JetBlue Airways passenger data to DOD subcontractor Torch Concepts. TSA's initial explanations regarding

[17] 68 Fed. Reg. 2101 (Jan. 15, 2003).
[18] 68 Fed. Reg. 45265 (Aug. 1, 2003).
[19] See Appendix G for more information on the Privacy Act and E-Government Act.

this transfer indicated that the agency had provided only an introduction between the two parties. Later, TSA disclosed that it had requested in writing that JetBlue provide passenger data to Torch Concepts.

Senators, privacy advocacy groups, and the media initiated a series of requests for information following the release of these stories and statements regarding the data transfer to Torch Concepts. The DHS Privacy Office and the Army OIG later conducted inquiries into the data transfer.

On February 20, 2004, the DHS Privacy Office issued a *Report to the Public on Events Surrounding jetBlue Data Transfer* that addressed the transfer of airline passenger data from JetBlue to Torch Concepts. The DHS Privacy Office found no violations of the Privacy Act on the part of TSA employees. However, according to the report, it was "beyond the scope of the Privacy Office to determine whether these employees may have otherwise exceeded the normal scope of TSA operations."[20] Accordingly, we decided to review TSA's use and dissemination of airline passenger data in this and all other relevant cases.

The Army OIG conducted a separate inquiry into the same transfer and issued a report on June 21, 2004.[21] The Army OIG report found that its subcontractor, Torch Concepts, did not violate the Privacy Act in its receipt and analysis of the JetBlue data.

In April 2004, American Airlines released a statement saying that in June 2002, at the request of TSA, some passenger travel data was turned over by an American Airlines vendor to four research companies vying for contracts with TSA. The same month, the vendor, Airline Automation, Inc. (AAI), released a press statement saying that it provided American PNR data in 2002 to four companies that were then testing aviation security systems for TSA.

In light of past TSA statements that the CAPPS II program had not used airline passenger data for testing, the disclosure that companies working with TSA obtained airline passenger data in 2002 to test aviation security systems fueled public assertions and reports that the agency was withholding information about its operations.

[20] Department of Homeland Security, Privacy Office, *Report to the Public on Events Surrounding jetBlue Data Transfer,* February 20, 2004, p. 9.
[21] U.S. Department of Defense, Department of the Army, Office of the Inspector General, *Report of Investigation 04-007, JetBlue*, (hereinafter referred to as Army OIG Report), June 21, 2004.

These reports were reinforced by later TSA disclosures that it had used airline passenger data for testing CAPPS II prototypes. On June 23, 2004, TSA's Acting Administrator, in a nomination hearing to become Assistant Secretary of Homeland Security for TSA, revealed more information about TSA's role in the transfer of airline passenger data. The Acting Administrator submitted a document for the congressional record that specified the use of six airlines' passenger data for CAPPS II prototype testing.

Purpose, Scope, and Methodology

We conducted this review to determine whether TSA's role and actions in the use and dissemination of airline passenger data were appropriate. Also, the review was conducted to resolve confusion about TSA's involvement in cases of airline passenger data sharing and to identify the cause of this confusion.

We framed our review around three objectives:

- Present a comprehensive summary of TSA's role in the analysis and transfer of airline passenger data;
- Assess the extent to which TSA was forthcoming in disclosing information related to these transfers; and
- Evaluate TSA's current operating environment with respect to matters of privacy and the sharing and exchange of passenger data.

Our fieldwork was carried out from April to August 2004. This fieldwork included substantial file reviews and more than 40 interviews. We interviewed TSA personnel at headquarters and several TSA field offices, as well as personnel from other agencies. Among those interviewed were: the former Deputy Secretary of Transportation; the former DOT chief information officer designate; the former TSA deputy administrator; the DHS chief privacy officer (CPO); the Office of National Risk Assessment director; the TSA chief information officer; the TSA associate director of the Freedom of Information Act and Privacy Act Division; and the TSA chief counsel.

Additionally, we interviewed or queried CAPPS II program contractors, cooperative agreement recipients, and grantees; select airlines; global distribution systems; and airline data aggregators. We contacted all of the early CAPPS II prototype vendors: Ascent Technology, Inc.; HNC Software, Inc.; Infoglide Software Corporation; International Business Machines Corporation (IBM);

and the Lockheed Martin Corporation. After identifying contacts for each firm, we requested interviews. Each of the companies made it clear that they were not willing to submit to an interview. As a substitute for interviews, we sent questionnaires to each of the companies. HNC Software/Fair Isaac was the only vendor that did not respond to our questionnaire. We incorporated the other companies' responses in the draft where appropriate. We also interviewed representatives from Acxiom, Airline Automation, Inc., Delta Air Lines, Galileo, JetBlue Airways, Sabre Holdings, and Torch Concepts.

These efforts were supplemented by the review of CAPPS II program and contracting files, as well as materials that TSA components submitted to the TSA FOIA office in response to related FOIA requests.

TSA's leadership, persons involved in CAPPS II development, and TSA's rank and file staff all made themselves available to us during the course of our inquiry and, in many cases, provided indispensable support.

This special review was conducted under the authority of the Inspector General Act of 1978, as amended and according to inspections standards promulgated by the President's Council on Integrity and Efficiency.

TSA's Role in Airline Passenger Data Transfers

To repeat, we reviewed TSA's role in airline passenger data transfers in three operational contexts. First, we reviewed TSA's role in airline passenger data transfers to support other federal agencies. Second, we explored airline passenger data transfers associated with CAPPS II. Third, we reviewed TSA's role in obtaining airline passenger data to improve the current CAPPS system.

Data Transfers to Support Other Federal Agencies

TSA facilitated airline passenger data sharing to support the national security functions of other agencies in two cases. In the first instance, TSA assisted the U.S. Secret Service (USSS) in obtaining data to assist with the security efforts at the Salt Lake City Winter Olympics in early 2002. In the other case, CAPPS II program staff requested that JetBlue furnish passenger records to an Army subcontractor, Torch Concepts, for its work on a base security enhancement project.

United States Secret Service

The 2002 Winter Olympics in Salt Lake City, Utah, was designated a "National Security Special Event." With this designation, the USSS became the lead agency for designing, planning, and implementing security.[22] USSS security coordination for the Olympics included collaboration with TSA.

The USSS assistant director for Protective Research sent a letter, dated January 11, 2002, to the FAA deputy associate administrator for Civil Aviation Security requesting a civil aviation security directive authorizing dissemination of airline passenger information to the USSS to support efforts to coordinate security at the Olympics. In addition, this information would facilitate the evaluation of a new project that included a process "to allow federal law enforcement the capability of name checking passengers against selected law enforcement databases." The project drew on coordination among the USSS, Delta Air Lines, ARINC Incorporated (an aviation communications and engineering company), and InRange Technology Corporation, an information technology firm.

On February 5, 2002, TSA directed Delta to provide airline passenger data to the USSS to enhance security for the 2002 Winter Olympic Games.[23] TSA issued this authorization by security directive, a power the administrator of TSA may use to mandate actions on the part of aviation sector entities to respond to threat assessments or specific threats against civil aviation.[24] In this case, TSA's security directive expressly ordered Delta to provide PNR and other customer information details, including dates of birth, to the USSS. It authorized Delta to provide this information for all passengers traveling on flights through February 26, 2002, to locations hosting Olympic events and any other venues selected by the USSS or its partners.[25] In addition, it specified that data recipients were to limit dissemination of the passenger data strictly to personnel in their organizations with an operational need-to-know. No airline other than Delta was subject to this security directive.

[22] 18 U.S.C. § 3056(e)(1).
[23] Security Directive 108-02-02, signed February 5, 2002.
[24] 14 CFR § 108.305. Effective February 17, 2002, this provision was transferred to 49 CFR § 1544.305, 67 Fed. Reg. 8340 (Feb. 22, 2002).
[25] According to the TSA security directive, Delta was authorized to provide passenger data for passengers on flights beginning on February 1, *2001*. Delta officials report, however, that this was a typographical error in the security directive and that the TSA administrator manually changed the date to February 1, *2002*, on Delta's signed copy. Because the security directive also notes that the USSS believed data collected a year before the Olympics may be relevant to event security, we believe the authorization was intended to apply to data from February 1, *2001* forward.

Pursuant to the security directive, Delta provided airline passenger data to the USSS. To set out parameters for USSS handling of its passenger data, Delta signed a Memorandum of Understanding (MOU) with the USSS on February 8, 2002. The MOU set boundaries on data disclosure and specified that the data would be destroyed as soon as possible following the security directive's expiration date. Passenger data disclosure was restricted to the following parties:

- USSS staff with an operational need to know;
- Other governmental agencies, as necessary, to execute legitimate law enforcement activities; and
- USSS partners, ARINC and InRange.

Delta officials said that its airline passenger records were transferred over a private, secure encrypted network. The passenger records that it furnished to the USSS corresponded to incoming flights to airports in the vicinity of Salt Lake City, Utah. The USSS received only a subset of information contained within Delta's passenger name records, including first and last name, address, phone number, and flight information. The airline said it restricted the information it shared with the USSS to a minimum.

Once received, according to the USSS, the records were stored on a stand-alone computer in a secure location and were not shared with any parties outside the USSS. The USSS does not know the exact number of records it received, but it reports that they were all destroyed following the Olympics. The USSS used the data to determine whether individuals of interest to the agency were traveling in the vicinity of the Olympics. In the process, the USSS also assessed the quality of its pilot program with Delta, InRange, and ARINC.

At no time were Delta passenger records relating to this transfer transmitted or otherwise provided to TSA. TSA did not facilitate the transfer of any additional passenger data in relation to the Olympics. TSA's security directive expired with the conclusion of the Olympics.

At the time of the passenger data transfer, the USSS maintained a declared system of records that TSA asserts applied to the acquisition and analysis of these passenger records. In particular, TSA holds that the USSS August 28, 2001, Privacy Act systems of record notice for its Protection Information System covers the airline passenger data it received in February 2002.[26] The declared categories

[26] U.S. Department of Homeland Security, Transportation Security Administration, Office of Chief Counsel, *Report on Passenger Name Record Data Exchanges Involving Projects to Improve Passenger Screening*, August 18, 2004, p. 62.

of records associated with this USSS system include "records containing information compiled for the purpose of identifying and evaluating individuals who may constitute a threat to the safety of persons or security of areas protected by the USSS."[27]

Army Subcontractor Torch Concepts

JetBlue Passenger Data Transfer

Torch Concepts is a small Huntsville, Alabama, firm with proprietary data analysis software that it operates under the name "Acumen." According to Torch Concepts' Chief Executive Officer, the firm previously had done work for the military and considered applying its technology to a broader array of homeland security efforts after September 11, 2001.

In March 2002, Torch Concepts became a subcontractor of SRS Technologies on the Army's Base Security Enhancement Study.[28] The Army enlisted Torch Concepts' services to prove the feasibility of its approach to uncovering terrorist activities. Under the terms of its task order, Torch Concepts was to use its software to search airline passenger data for terrorists whose records were to be added to the passenger data set used in the analysis.

Torch Concepts had difficulty securing the data that were essential to meet the terms of its subcontract. After initial overtures to Delta and American failed to yield data, Torch Concepts sought TSA's assistance.[29]

On June 4, 2002, Torch Concepts met with the Army technical representative for the firm's subcontract, the CAPPS II executive sponsor, the CAPPS II program manager, and a DOT congressional liaison. At the meeting, Torch Concepts discussed its work for the Army and gave a presentation on its Acumen software. According to Torch Concepts, CAPPS II was not discussed during the meeting. By the date of this meeting, the CAPPS II program team had agreements with four companies to develop CAPPS II risk assessment prototypes. Because they

[27] Treasury/USSS.007, United States Secret Service Notice of Systems of Records, 66 Fed. Reg. 45362 (Aug. 28, 2001).
[28] SRS Technologies was the prime contractor for this study, while Torch Concepts received funding for its proof-of-principle. A proof-of-principle establishes that a given tool or concept can be used to solve a given kind of problem. In this case, Torch Concepts was to prove that its Acumen software was capable of solving problems similar to those encountered in base security settings.
[29] These overtures to Delta and American occurred during December 2001 and January 2002, months before the Army subcontract with Torch Concepts.

had already selected vendors for this aspect of CAPPS II, program staff did not consider Torch Concepts a prospective partner in system development.

The former CAPPS II program manager said that, following the initial meeting with Torch Concepts, the CAPPS II's executive sponsor instructed him to assist Torch Concepts. In our interview with the former CAPPS II executive sponsor, he could not recall having given such an instruction, but said that it was possible that he did so. We could find no documentary evidence that would settle the matter.

On June 12, 2004, the Army's technical representative overseeing the Torch Concepts subcontract e-mailed the CAPPS II program manager. It is clear from this e-mail that the technical representative understood TSA was to provide a "sample airline reservation data set" for Torch Concepts. An attachment setting out Torch Concepts' program scope and plans for its proof-of-principle specifically itemizes the airline reservation data elements Torch Concepts required.

Three additional meetings between CAPPS II program representatives and representatives of the Army or Torch Concepts took place during June and July 2002. Over the course of these meetings, Torch Concepts developed an understanding that TSA would provide the company with a PNR database.

In late July, the CAPPS II program manager contacted JetBlue Airways to request the airline's assistance in securing passenger data for Torch Concepts. After soliciting JetBlue's assistance over the phone, the CAPPS II program manager followed up with an e-mail on July 31, 2002, to JetBlue's director of Corporate Security. This e-mail included an attached memorandum titled "Request for PNR Data for a Department of Defense (DOD) Proof of Concept." The memorandum briefly described Torch Concepts' DOD related work, requested the assistance of JetBlue in providing passenger data, and articulated the process whereby JetBlue passenger data should be provided to Torch Concepts. The memorandum specified that JetBlue should provide PNRs to Torch Concepts via a JetBlue contractor, Acxiom, Inc.[30] It also stated that "any non-disclosure agreements that need[ed] to be executed [could] be exchanged directly between the parties with copies provided to both DOD and TSA."

The former CAPPS II program manager said that he did not believe that he had the authority himself to send such a request, but that he had received general

[30] Acxiom is a commercial database management company that provides data services to a wide range of clients, including several airlines.

authorization from the CAPPS II executive sponsor to assist Torch Concepts. Neither the CAPPS II executive sponsor, nor the DOT Deputy Secretary who had an active role in CAPPS II planning, reports having had any contemporaneous knowledge of the JetBlue data transfer to Torch Concepts.

In September 2002, Acxiom provided Torch Concepts with approximately five million JetBlue PNRs representing 2,226,715 passengers. These records corresponded to JetBlue passengers traveling over a 33-month period. Torch Concepts received this data set in an encrypted format via a File Transfer Protocol (FTP) web site maintained by Acxiom. Before the data transfer, Torch Concepts and Acxiom entered into a confidentiality agreement that bound both parties to maintain the confidentiality of passenger data.[31]

After evaluating the JetBlue PNRs, Torch Concepts found that the data did not have certain elements the firm anticipated using to establish its proof.[32] Torch Concepts then purchased supplementary demographic information on passengers from Acxiom. This commercially available dataset of demographic information included social security numbers, salary data, housing ownership indicators, and length of residence, among other information. Acxiom matched the demographic data to the JetBlue airline passenger data and provided it to Torch Concepts.

The combined data set contained certain ambiguities and anomalies that Torch Concepts believed it had to resolve before proceeding with its proof. To study ways to resolve these data issues, Torch Concepts accessed a limited number of records corresponding to individual passengers. After discarding certain anomalous records, Torch Concepts stripped passenger names and deleted all but two digits of passengers' social security numbers.

Torch Concepts followed the same internal security procedure each time it received data from Acxiom. In each case, Torch Concepts decrypted the files it received via Acxiom's FTP site and then disconnected the host computer from the internet and intranet. Only one Torch Concepts employee was permitted access to the data.

According to Torch Concepts, the data on JetBlue passengers remained secure and was not disclosed in violation of Torch Concepts' confidentiality agreement

[31] Torch Concepts and Acxiom entered into a confidentiality agreement on April 25, 2002.
[32] Torch Concepts specifically mentioned passenger miles flown during the past year and over the passengers' lifetime, and frequent flier club membership.

until April 2003, when a representative of the firm gave a presentation at a software developers' conference. On April 4, 2003, Torch Concepts delivered a presentation at the Southeastern Software Development Conference. Torch Concepts reports that this presentation was intended for delivery to the Army and was inadvertently given to a wider audience.

A slide in the presentation displayed "Anomalous Information on One Passenger." This slide presented forty-two lines of data with addresses, social security numbers, dates of birth, and indicators of length of residence. Torch Concepts developed this slide to highlight the challenges it faced in analyzing the sometimes confusing data it received on individual passengers. To support this point, Torch Concepts displayed mixed information from Acxiom's demographic data set that had been matched to data from a single JetBlue passenger. According to an attorney for Torch Concepts, this data was selected because it contained numerous anomalies. The demographic data presented on the slide includes twenty-three different addresses and three social security numbers. To present anomalous demographic data that had been matched to one passenger instead of several, Torch Concepts picked out and displayed records with the same identifying key.[33]

Together with the rest of Torch Concepts' April 2003 presentation, this slide was later posted on the internet. As a result, sensitive information associated with a JetBlue passenger became freely and publicly available. Torch Concepts' subsequent efforts to remove the presentation from the internet have failed.

In September 2003, Torch Concepts attempted to delete all electronic passenger and demographic data associated with its subcontract. A subsequent audit of Torch Concepts' files, however, revealed that traces of some data remained. Torch Concepts forwarded these to its attorney, who retains the system hardware with the data in a secure setting.

After 2002, TSA did not coordinate with Torch Concepts on the progress or results of the Army Base Security Enhancement Study. Despite the CAPPS II program manager's request for copies of non-disclosure agreements executed in support of the JetBlue data transfer, Torch Concepts never provided a copy of its confidentiality agreement to TSA.

[33] This identifying key was developed by Acxiom and provided to Torch Concepts as a data element in the demographic data set.

Summary Findings

Early TSA and CAPPS II efforts were pursued in an environment of "controlled chaos" and "crisis mode" after the September 11 attacks. Management changes were frequent and chains of command were blurred. Two years later, a clear line of authorization for TSA's request to JetBlue cannot be established. Despite the former CAPPS II program manager's belief that he did not have authority to make a request of JetBlue, many of TSA's current and former staff, including TSA's former deputy administrator and an attorney with TSA's chief counsel, believe that he did. The former DOT Deputy Secretary said that while he did not authorize TSA's involvement in the Torch Concepts transfer at the time, he accepted responsibility for it. The former Deputy Secretary's "titular accountability," however, does not answer the question of whether the CAPPS II program manager had actual authority to authorize the exchange or had been authorized by someone with authority to do so. We found no regulation or directive that explains how requests like Torch Concepts' are to be evaluated or by whom they may be approved.

Despite the ambiguity in how the request from Torch Concepts was processed for approval, TSA's limited role in this data transfer was in compliance with its governing statutes. TSA is responsible for security in all modes of transportation.[34] Among TSA's duties and powers is transportation security planning, which includes "coordinating countermeasures with appropriate departments."[35] TSA also has power to require airlines to produce passenger data.[36]

In a communication with the CAPPS II program manager, the Army's technical representative listed security enhancements to "transportation transactions" as one of four issues that the Army sought to determine whether Torch Concepts' software could address.[37] Because Torch Concepts' work supported the transportation security objective of another department, the CAPPS II program manager's request for JetBlue to provide data to Torch Concepts was within the scope of TSA's transportation security planning duties.

[34] 49 U.S.C. §114(d).
[35] 49 U.S.C. §114(f)(4).
[36] 49 U.S.C. §114(d) (1), §114 (e), §114 (h)(4), and §44901(a).
[37] This reference to "transportation transactions" is present in the program scope document that was e-mailed to the CAPPS II program manager by the Army technical representative on June 12, 2002.

TSA's request for JetBlue to provide PNRs to a DOD subcontractor fell within the scope of TSA operations. Analysis of related documentation and discussions with past and present staff support the position that TSA's assistance to Torch Concepts stemmed from an interest in supporting the national security mission of another department as it applied to transportation security.

Data Transfers Associated with CAPPS II Development

Eleven airline passenger data transfers took place during CAPPS II development efforts. In each case, the transfers were pursued to establish the operability of prototype and component systems. Four of the data transfers resulted from the independent efforts of vendors associated with the CAPPS II program, while seven took place as a result of TSA's direct involvement.[38] Of these seven transfers, five were the result of a grant FAA awarded on TSA's behalf, and the remaining two occurred during subsequent efforts to test CAPPS II system components.

Two TSA vendors independently obtained airline passenger data in order to prove the effectiveness of RAE prototypes. Four transfers of airline passenger data resulted, as follows:

- In June 2002, Ascent Technology, Inc. received data on Delta Air Line passengers.
- In mid-2002, HNC Software, Inc. received data on Continental Airlines, Frontier Airlines, and America West Airlines passengers from the SHARES reservation system.
- In mid-2002, HNC received data on JetBlue passengers from Acxiom.
- In mid-2002, HNC received data on passengers from various airlines through its E-Tickets system.

TSA, through the FAA, also awarded a grant to Airline Automation, Inc., to furnish the RAE vendors with airline passenger data for prototype demonstrations. Five transfers of airline passenger data took place as a result of this grant:

- In May and June 2002, Ascent received data on American Airlines passengers.
- In May and June 2002, HNC received data on American passengers.

[38] See Appendix E and Appendix F for summary information on these transfers.

- In May and June 2002, Infoglide Software Corporation received data on American passengers.
- In May and June 2002, Lockheed Martin Corporation received data on American passengers.
- In June 2002, TSA's CAPPS II program viewed data on American passengers.

Later efforts to test both the ADI and RAE components of the system resulted in additional passenger data sharing:

- In early 2003, Delta staff inadvertently provided IBM access to its passenger data.
- In May 2003, TSA received passenger data from Sabre Holdings to test CAPPS II.

Although the parties to these exchanges did not always execute appropriate non-disclosure agreements in advance of data transfers, we have not found any evidence of data disclosures to third parties or misuse of the data. In all but four cases, we have been assured that data disseminated in association with these transfers is held in a secure environment or has been destroyed. Citing pending class action lawsuits, the two firms associated with the four remaining transfers did not provide related information for our review. As a result, we have no information on the final disposition of the airline passenger data that HNC Software and Ascent Technology independently obtained for RAE prototype development efforts.

TSA directly received airline passenger data in only two of these CAPPS II development cases.[39] Although TSA received data, in neither case did it directly access any records associated with these data submissions. DOT staff on the CAPPS II program team did, nonetheless, view passenger data from other transfers. DOT staff evaluating RAE prototype development efforts viewed passenger data from one of Airline Automation, Inc.'s transmissions. In this instance, DOT staff only confirmed previous accounts that the data initially supplied by AAI was not in a usable format. DOT staff may have also viewed Delta passenger data in a presentation by one of the prototype vendors.

[39] TSA directly received airline passenger data in one additional case in connection with CAPPS improvement.

Risk Assessment Engine Prototype Vendors

On March 8, 2002, the FAA issued a solicitation for white papers from software developers to address solutions for the risk assessment component of CAPPS II, the RAE.[40] This request for white papers targeted the identification of software capable of delivering a substantial improvement in risk assessments using passenger data. Among other matters, the solicitation required that applicants submitting white papers "discuss and demonstrate [their] ability to link with airline computer reservation systems and extract PNRs for risk assessment."[41]

Approximately 30 firms responded with white papers. On April 1, 2002, a proposal evaluation team affiliated with CAPPS II selected four vendors to submit detailed proposals for the development and evaluation of their proposed prototypes. The four firms selected were: Ascent Technology, Inc.; HNC Software, Inc.; Infoglide Software Corporation; and the Lockheed Martin Corporation. In May 2002, the FAA signed cooperative agreements with each company on TSA's behalf.

These cooperative agreements established a 60-day performance period for the vendors to establish their proofs of concept.[42] The agreements bound the vendors to deliver risk assessment prototypes for preliminary testing. Operating with government support and guidance, each vendor was asked to create a working prototype for the CAPPS II team to test and evaluate. The agreements stipulated that software applications developed to support CAPPS II risk assessment functions meet "appropriate network security levels," but did not place any restrictions on the use or disclosure of sensitive personal information.

In-depth testing of the feasibility and effectiveness of these prototypes required the use of authentic data corresponding to real people. This "real" data was useful in RAE prototype testing for two reasons. First, such data was important to assess whether the public database linkages underpinning the various prototypes were viable. Passenger records on fictitious individuals would not have matched to information in public databases and could not establish the viability of a prototype's interface with public data. Second, it was useful to the CAPPS II team to determine whether a prototype system could effectively process

[40] This solicitation appeared as a Broad Agency Announcement under the title "Announcement for Submission of White Papers for CAPPS II Software Evaluation." Broad Agency Announcements articulate, in general terms, an agency's research goals in a particular area and solicit qualified respondents interested in pursuing future funding awards in that area.
[41] Ibid., 2.
[42] A proof of concept demonstrates the feasibility of an approach to solve a given problem.

authentic records from public databases with all of their associated anomalies and inconsistencies. This key system capability could not be evaluated without data on real individuals.

While the four vendors were initially selected in part for their ability to link with reservations systems and to extract PNR, their cooperative agreements with the FAA did not assign responsibility for obtaining passenger data. The CAPPS II program staff sought a uniform set of PNR data to test each of the vendors against a common standard. During the same period, two of the RAE prototype vendors – Ascent and HNC – accessed airline passenger data without TSA coordination or assistance.

Ascent accessed PNRs from Delta's reservation system in early June 2002, during the development of its RAE prototype. As suggested in Ascent's RAE development proposal, these PNRs may have corresponded to flights departing from Boston Logan International Airport in Massachusetts. Citing ongoing litigation related to its work for TSA, counsel for Ascent has advised that the firm cannot release any further information on the PNR data it received from Delta.

Ascent reported to us that it "never accessed or retrieved data by individual identifier" and that the data was stored in a "password-protected environment." Ascent further said that access to the passenger data was limited to employees working on the firm's RAE prototype development efforts. Some evidence suggests the possibility, however, that these Delta passenger records were also viewed by CAPPS II program staff. According to a written evaluation of Ascent's prototype, the firm "demonstrated real live feed of PNR" to prototype evaluators from the CAPPS II team. However, we were unable to confirm that the records used for Ascent's demonstration were records corresponding to actual passengers, or that they corresponded to Delta passengers in particular.

HNC Software obtained a more varied set of PNR data for prototype testing than the other vendors. In its final report, HNC Software reported independently obtaining airline passenger data from at least four airlines. During the course of its cooperative agreement performance period, HNC received airline passenger data from three sources: the SHARES reservation system, Acxiom, and HNC's own E-Ticket operations. HNC's collaboration with SHARES netted it passenger data from Continental Airlines, Frontier Airlines, and America West Airlines corresponding to flights between June 20 and July 3, 2002. In total, HNC accessed 787,081 Continental PNRs, 70,523 Frontier PNRs, and 589,515 America

West PNRs through the SHARES system.[43] For its part, Acxiom furnished HNC Software with 2,725,352 JetBlue PNRs. These records corresponded to JetBlue passengers who flew between January 13 and September 5, 2002. Finally, HNC E-Tickets provided HNC's RAE prototype development team with 400,000 PNRs from "various" airlines for testing purposes. According to HNC's final report, these passenger records came from flights during the June 20 to June 25, 2002, time frame.

Because of three pending class action lawsuits on work related to TSA, the current owner of HNC Software, FairIsaac, would not provide information for our review. As a result, we were unable to determine to which airlines the HNC E-Ticket PNRs corresponded. For the same reason, we could not determine how many individual passengers were associated with the PNRs that HNC used in its prototype development and testing. Questions also remain on the final disposition of this data.

Infoglide reports that it did not independently access PNR data. According to a MITRE employee monitoring Infoglide's progress in prototype development, however, it had 13 million PNRs from WorldSpan, a firm that manages travel data. Nonetheless, Infoglide reported to us that it never received real PNRs from WorldSpan. Instead, according to Infoglide, the firm requested and believes it received "mock" data with fabricated records on fictitious passengers from WorldSpan. We have not been able to confirm this claim.

The final cooperative agreement recipient, Lockheed Martin, maintains that it did not use any independently procured airline passenger data in the development or testing of its RAE prototype. For the purposes of developing and demonstrating its RAE prototype, Lockheed Martin did use a small demographic data sample from its partner, commercial data provider ChoicePoint. As this limited data set did not include any authentic airline data, we did not address it further in our review.

RAE prototype vendors' independent pursuits of PNRs were not directly overseen by TSA. TSA did, however, weigh the implementation of sound privacy and information security practices in its appraisals of vendor performance during its prototype evaluation process. One of the five technical factors used to assess the quality of vendors' prototypes was their adequacy with respect to privacy and

[43] According to HNC Software's final report, data from SHARES included frequent flier information and seating data.

civil rights, and data confidentiality. Evaluators specifically considered whether the vendors' software solutions would:

- meet legal requirements related to information privacy and civil rights;
- ensure information security;
- protect against unauthorized access to, use of, or disclosure of information; and
- protect individual privacy rights.

Evaluators' appraisals on these grounds provide insight into the likely confidentiality and security of the airline passenger data obtained by the RAE prototype vendors. In the final analysis, the four prototypes' approaches to privacy and confidentiality were scored on two scales. Overall solutions in this area were rated for the basic quality of the solution and its associated risks. Three of the prototype solutions were rated "adequate" on the quality of their solutions with respect to privacy and confidentiality, while one firm's solution was rated "strong." In terms of risk, one prototype was adjudged "low risk," two "medium risk," and one "high risk." Risk ratings in this context refer to the risks TSA might experience in working with a given vendor to develop a full-scale RAE system for CAPPS II.

Airline Automation, Inc.

Airline Automation, Inc. (AAI) is a firm that provides data services to a number of domestic and international air carriers. By 2002, AAI had software applications running on a range of airline reservations systems and operated processes for several systems hosting passenger data for travel agencies.

AAI said that following the attacks of September 11, 2001, it sought to contribute to improving the aviation security environment and engaged in related discussions with the Federal Bureau of Investigation, Customs Service, and TSA. AAI contact with the CAPPS II executive sponsor and program manager in March 2002 was followed by a meeting to discuss the means by which AAI could support CAPPS II development.

As a product of these discussions, AAI submitted a white paper to the CAPPS II program manager in early April 2002. The AAI white paper offered a solution for providing a data conduit to and from the RAE component. AAI offered to convert the tangle of disparate airline reservations data into a common format for the CAPPS II risk assessment engine to read. To feed information from

the RAE to the reservations systems, in turn, AAI offered to pair reservations data with risk assessment information and return the "enhanced" data to its source in its original format.

After evaluating AAI's white paper and a subsequent proposal, the FAA awarded the firm a research grant of approximately $61,000 on May 31, 2002. Covering a two-month term, the research grant award itemized several deliverables including the:

- development of "secure data access consistent with fundamental security and privacy needs;"
- certification that AAI has legal authorization or licenses for all of the data accessed and processed by the prototype systems;
- development of a detailed plan on security protocols and procedures to restrict access to the data and a confidentiality statement;
- provision of sample airline passenger data with a description of the databases, sources, and content; and
- transfer of aggregated sample airline passenger data received to the RAE system component.

The CAPPS II program team viewed AAI's research grant as an opportunity to enlist the firm in the effort to furnish PNR data for RAE prototype testing. By the date of the AAI research grant award, the FAA had signed cooperative agreements with all four of the RAE prototype vendors. With AAI's parallel grant award, the firm's aggregated sample airline passenger data could be distributed to each of the four vendors. Using AAI's data set, the CAPPS II program team could measure the performance of the RAE prototypes in processing a uniform set of data.

After AAI's proposal received a favorable evaluation from the FAA research grants staff, the CAPPS II program manager appealed to two airlines to use their passenger data for CAPPS II development. On May 15, 2002, the CAPPS II program manager drafted a memorandum to Continental requesting that the airline furnish TSA and its RAE prototype vendors with PNRs through TSA's grantee, AAI. Five days later, the program manager sent a similar request to American soliciting PNR data through AAI.

In apparent anticipation of PNR data transfer, both American and Continental signed non-disclosure agreements with TSA in late May 2002.[44] While there is no

[44] American signed a non-disclosure agreement with TSA on May 20, 2002. Continental signed a non-disclosure agreement with TSA eight days later on May 28, 2002.

evidence that Continental ever provided airline passenger data in furtherance of its non-disclosure agreement, American authorized AAI to provide its passenger data to TSA for "testing CAPPS II programming" on May 22, 2002. American's e-mail communicating authorization to provide passenger data for CAPPS II did not expressly provide for the release of data to any party other than TSA.

On May 24, 2002, AAI sent one compact disc (CD) with an indeterminate quantity of American passenger data directly to each of the four RAE prototype vendors. AAI obtained the data on the CDs from the Sabre reservations system, which hosts reservations for American, among other airlines.

AAI sent these CDs seven days before FAA awarded the firm a research grant, and weeks before it signed non-disclosure agreements with the recipients. Due to the configuration of the airline passenger data on the CDs, the RAE prototype vendors complained that they could not effectively open, access, or interpret the records. At least two RAE prototype evaluators on the CAPPS II team viewed data from the CDs and confirmed that the data supplied by AAI in this first instance was not in a usable format.

In mid-June 2002, AAI made another attempt to transmit PNRs to the RAE prototype vendors. The firm provided TSA and the RAE vendors with passwords to access airline passenger data uploaded onto a file transfer protocol (FTP) server. On June 17, 2002, AAI placed approximately 500,000 American passenger records on the server. On the same day, two of the RAE prototype vendors entered into non-disclosure and confidentiality agreements with AAI. These agreements stipulated to basic data security safeguards and barred data disclosure to third parties without the execution of another non-disclosure agreement. The non-disclosure agreements also required the vendors to limit the internal distribution of the data to those employees with a "need to know" and restricted data use to analysis and data assessment work for the FAA. Finally, the agreements mandated the return or destruction of all related data and information within 10 days of the end of the vendors' related work.

AAI did not sign non-disclosure agreements with the two other RAE prototype vendors, Infoglide and HNC Software, until June 25, 2002, seven days after these two vendors received passwords to access AAI's airline data. Although the non-disclosure agreements were not signed by AAI until June 25th, Infoglide and HNC Software had signed the agreements before they received access to AAI's data. As signatories of non-disclosure agreements, both of these vendors were bound

to maintain the confidentiality of passenger data during this interim. Neither firm inappropriately used or disclosed the data it may have accessed at the time.

Certain data elements that TSA deemed important to RAE prototype development and testing were absent from the passenger information that AAI had posted to the FTP site on June 17, 2002. In particular, TSA requested that additional information useful in authenticating identity and data important to risk scoring be included with the airline passenger data. After consultations to clarify the additional information that TSA wished to have included in the data submissions to the RAE prototype vendors, AAI transmitted an e-mail with sample records. The e-mail, which included an attachment with approximately 10,000 American PNRs, was sent to TSA and each of the four vendors on June 27, 2002. According to AAI, its copy of the e-mail was automatically returned to AAI unopened, because it was too large for the agency's e-mail system to process.

On June 28 and 29, 2002, AAI loaded an additional 1,331,640 American PNRs to the FTP server. These records corresponded to the period from June 22 to June 29, 2002, and included passengers' full name, itinerary, phone number, e-mail address, and credit card number when available.

Passenger data provided by AAI were used differently by each of the four RAE vendors. Ascent reported that it used only a subset of about 900,000 of the records that it received from AAI for RAE prototype demonstration purposes. The firm also said that it did not access or retrieve or match the data by individual identifier. With one exception, access to the records was limited to Ascent employees connected to the project. During Ascent's final presentation to the CAPPS II team in late July 2002, the firm included American passenger data in sample RAE system display screens. Ascent will not disclose information about the final disposition of this data.

HNC applied the data it received from AAI to the adjustment of its passenger risk assessment scoring scheme and RAE prototype testing. According to the vendor's final report, it used 1,302,468 of the PNRs from AAI for these purposes. The more than 1.3 million American PNRs were supplied to HNC's partner, Acxiom, and matched to demographic information in Acxiom's commercial databases.[45] Acxiom, in turn, transmitted the matched records back to HNC, which used the passengers' amplified demographic information to develop risk ratings. Counsel

[45] HNC's non-disclosure agreement with AAI listed Acxiom as an approved third party, eligible for receipt of passenger data.

for Fair Isaac, the firm that now owns HNC, advised TSA that HNC had deleted the data it received from AAI.

Infoglide used the American PNRs it received from AAI in a limited fashion. The company's prototype development team evaluated the completeness of the fields within the data set it received and made determinations about what data elements it could effectively use in passenger risk assessment. Infoglide did not use data from AAI to test its RAE prototype. After the expiration of its cooperative agreement, Infoglide returned PNR data to AAI and attempted to destroy all copies of it. Infoglide has reported that a copy of the AAI data was later found on a CD. According to the firm, this data "is being maintained in a secure place."

Lockheed Martin used a subset of the data it received from AAI in the performance of its RAE testing. Lockheed Martin formatted approximately 32,000 of the American PNRs and used them for prototype testing in an off-line setting. In July 2002, Lockheed Martin demonstrated its RAE prototype to TSA with about 50 of the formatted records. After the conclusion of its cooperative agreement, Lockheed Martin destroyed media containing the original American PNRs that it had received from AAI. Nevertheless, Lockheed Martin has retained copies of the approximately 32,000 PNRs it formatted. The company maintains that access to these records is "strictly controlled" and told us that it notified AAI of their status.

CAPPS II program staff maintained that TSA did not access passenger data on the FTP site at any point. This account is supported by AAI, which reported that TSA's password to access the FTP site was never used. At least two RAE prototype evaluators viewed the passenger data AAI initially supplied by CD. These staff members did not retain the data and only viewed it at a remote location. Other officials involved in CAPPS II development viewed airline passenger data that was displayed in prototype demonstrations performed for the Deputy Secretary of Transportation in late July 2002. An audience member witnessing these presentations recalled that attendees were required to sign non-disclosure agreements.

In late July 2002, AAI requested a one-month extension of its research grant at no cost to the government. As the basis for this extension, AAI stated that the DOD had requested that it provide Torch Concepts with airline reservations data. Several days later, the FAA approved AAI's one-month extension and set the research grant completion date for August 29, 2002. Despite these preliminary efforts, according to both AAI and Torch Concepts, no airline passenger data was

exchanged during the grant extension period. AAI submitted its final project report for its FAA research grant on September 30, 2002.

In addition to supplying passenger information to RAE prototype developers, AAI made a bid to be the CAPPS II ADI contractor. As the concept behind the ADI component of the CAPPS II program matured, TSA released an announcement requesting contact information from potential offerors on June 20, 2002. AAI provided TSA information as an interested potential offeror and later submitted a proposal. After submitting its proposal, on July 18, 2002, AAI received authorization from American to use the airline's PNRs in the process of ADI development and testing. TSA's evaluation of AAI's proposal, however, did not result in an award; another proposal was selected.[46] As a result, AAI did not use American passenger data for ADI development and testing.

Airline Data Interface Testing

On December 5, 2002, TSA awarded IBM a contract for an ADI solution for CAPPS II. The ADI's function was to extract, process, transfer, and load reservations and travel agency data and pass it to the CAPPS II risk assessment component. Once the RAE processed passenger risk assessment scores, the ADI was to transmit the scores to the airlines.

TSA's contract with IBM included certain privacy and confidentiality safeguards. According to the contract, data in the ADI system was to be regarded by IBM as sensitive but unclassified information and to be shared exclusively on a need-to-know basis. The contract also required that IBM provide for a data system meeting security and privacy needs and develop a detailed plan outlining data security protocols and procedures.

Access to airline passenger data was an important requirement for testing the ADI. Prior to the contract award, IBM and TSA engaged in discussions about how IBM would be provided access rights to passenger data. An early draft of the contract indicated that IBM was responsible for obtaining passenger data on its own. The final contract, however, specified that it was the government's responsibility to provide access and rights to "PNR and other related data sources and/or records accessed and processed by the ADI system…"

[46] TSA's Technical Evaluation Panel selected IBM's proposal for ADI development on July 26, 2002.

In December 2002, TSA and Delta officials met to discuss the airline's potential role in providing test data. A TSA official reported, and Delta officials confirmed, that Delta was agreeable to working with TSA if: TSA issued a security directive requiring Delta to give access to PNRs; TSA and Delta entered into an MOU governing use and retention of the data; and TSA's CAPPS II development contractors signed confidentiality agreements regarding the data.

Shortly following the IBM contract award, TSA staff contemplated the use of a security directive to mandate PNR data for testing, and coordinated with Delta to develop a draft MOU. In late February 2003, an official at Delta Technology mistakenly thought that TSA and Delta's attorneys had agreed on a final security directive ordering the airline to provide passenger data. As a result, Delta opened up a "real time" connection between IBM's system and a portion of Delta's airline reservations system over a secure virtual private network. Delta estimated that fewer than 1,000 Delta passenger records were transferred to IBM and Infoglide between February 27 and March 3, 2003. The records corresponded to Delta reservations system records that were updated or modified between those dates, and were limited to records for passengers on flights with an origin or destination of Birmingham International Airport in Alabama.[47]

On March 3, 2003, a Delta Technology official instructed IBM via e-mail to delete all transmitted data, including all copies and derivations of that data. The Delta Technology official further said that no data could be shared until Delta received an order from TSA compelling it to share the data and an MOU governing the use of the information. On the same day, an IBM representative instructed the IBM and Infoglide development teams to delete all Delta passenger data that they had received. Later that day, IBM confirmed that all of the data had been deleted. IBM advised that it did not access or retrieve any of these passenger records by individual identifier. Infoglide said that it never received or accessed passenger data from Delta.

Delta officials said that a pre-existing non-disclosure agreement with IBM protected the confidentiality of the passenger data that the airline transferred in February and March 2003.

[47] In the past, Delta asserted to TSA that the real passenger records that it had provided to IBM and Infoglide were mock records. TSA reported that, as of December 2004, Delta had not revised its statement to TSA on this point.

Sabre Holdings

Sabre Holdings is a company with businesses that serve travelers, corporations, travel agents, and travel suppliers around the world. In May 2003, the TSA entity managing CAPPS II at the time, the Office of National Risk Assessment (ONRA), received approximately one million airline passenger records from Sabre. However, ONRA returned them to Sabre in September 2003, never having accessed or shared the data.

In the spring of 2003, ONRA contacted Sabre. ONRA had committed to provide airline reservations and travel agency system data to its CAPPS II contractors in February 2003 and its communications with Sabre were an attempt to follow through on that commitment. In a May 9, 2003, letter, ONRA asked that Sabre provide it with airline passenger data to complete CAPPS II program testing. ONRA said that any passenger data that ONRA received would be used exclusively for CAPPS II design, development, and testing purposes, and would not be used for production processing or be shared outside the program.

In anticipation of the receipt of PNRs from Sabre, ONRA's privacy officer began coordinating with contractors to draft a privacy policy to govern use of the data. Written specifically for data from Sabre, the draft policy addressed data access, use, and retention.

Throughout May 2003, TSA attorneys, ONRA staff, and technical experts communicated regarding technical aspects of the system testing and applicability of the Privacy Act. TSA's main concern was whether individuals' records would be retrieved during testing. Based on an understanding that TSA would be testing the efficacy of certain aspects of the system and not making determinations about individuals or retrieving records by passenger name, TSA Office of Chief Counsel (OCC) staff advised that the Privacy Act did not apply to intended data uses. OCC advised, however, that record retrieval based on a person's name rather than random retrieval based on broad categories like date or flight would trigger the Privacy Act.

Sabre sent a CD containing PNR data to ONRA on May 16, 2003. This CD contained approximately one million airline passenger records. It is unclear to which airlines that data corresponded.[48] According to Sabre representatives,

[48] Sabre Holdings representatives reported that data on the CD likely corresponded to passengers from a number of the more than 400 airlines whose seats can be booked through Sabre.

ONRA did not request specific data fields. Sabre representatives said that the data contained airline passengers' first and last names, phone numbers, home addresses, and possibly dates of birth. Sabre representatives also said that the data was not "active" or "current" and it was for only domestic flights.

ONRA staff did not immediately review the information on the CD or provide the CD to its contractors. Instead, ONRA's privacy officer locked the CD in a cabinet pending resolution of all relevant privacy concerns. Sabre representatives said that they did not intend to allow ONRA to use the CD for CAPPS II system testing until a new CAPPS II Privacy Act system of records notice was published. In June or July 2003, Sabre representatives formally notified ONRA of its intent to bar use of the data until this requirement was met. An earlier CAPPS II system of records notice had received substantial comment and Sabre representatives requested that they have an opportunity to review the interim notice before permitting use of the data for CAPPS II.

TSA published an Interim Final Privacy Act Notice for CAPPS II on August 1, 2003.[49] Ten days later, ONRA sent Sabre a letter summarizing certain implications of the notice on CAPPS II system design and testing. After numerous discussions with TSA about privacy and public relations, in September 2003, Sabre asked that ONRA return its CD. Having never accessed, reviewed, or transmitted its contents, ONRA complied.

During the late spring and summer of 2003, ONRA also contacted WorldSpan and Galileo about supplying airline passenger data for the CAPPS II effort.[50] We found no evidence that that data was provided to TSA or any of the CAPPS II contractors by either of these companies in 2003.

Data Transfer in CAPPS Improvement Effort

In May and June 2003, TSA obtained JetBlue passenger data to assist in the identification of changes to the operating passenger pre-screening system. This data was used to weigh possible modifications to CAPPS rules. The data has not been destroyed and remains in TSA's custody.

[49] TSA Interim Final Notice, 68 Fed. Reg. 45265 (Aug. 1, 2003).

[50] WorldSpan and Galileo are firms that maintain and distribute electronic travel data through their GDSes. Subscribers to these companies' systems, including numerous travel agencies, receive travel information and booking capabilities for airlines, hotels, car rentals, cruises, and other related travel options.

CAPPS Improvement

In April 2003, TSA's Aviation Operations division formed a Selectee Checkpoint Program Completion Team (SCPC). As part of its mission, the SCPC focused on evaluating ways to adjust CAPPS selectee rates. This effort was conducted independently of CAPPS II development and within a separate TSA office.

In order to adjust selectee rates, the SCPC team identified possible changes to existing CAPPS scoring rules. A series of rule modifications were then evaluated against airline passenger data to assess relative impacts on selectee rates. Because CAPPS is operated by the airlines, data to make these assessments were not readily available. Accordingly, the SCPC team had to solicit the cooperation of airlines to evaluate the likely impact of different CAPPS rule adjustments. In May 2003, the SCPC team leader enlisted the support of American and JetBlue for this purpose.

The SCPC shared the details of possible changes to the CAPPS rules with American. After testing the proposed modification to the CAPPS rules against its passenger data, American was able to furnish the SCPC with information on how these changes would affect its passenger selectee rates. On the other hand, according to the SCPC team leader, JetBlue lacked the resources to assess the impact of proposed CAPPS changes. Instead, the airline provided passenger data to TSA's SCPC for analysis.

At TSA's request, starting in May 2003, JetBlue sent nine e-mail messages to members of TSA's SCPC with data on the air carrier's passengers. The e-mails included attachments with passenger data presented in spreadsheets. These spreadsheets were not password protected and did not restrict access by any other means.

The airline provided data for thirty flights with more than 3,900 passengers. Most records included fields for first and last name, PNR number, booking date, flight number, flight date, flight origin and destination, and home phone number. Some transmissions included passengers' e-mail addresses and indicated whether passengers had been selected for further screening. TSA had not requested passenger phone numbers or e-mail addresses for its analysis.

TSA staff used data from a subset of the JetBlue flights to model the prospective impact of CAPPS rules variations under consideration. This model was later presented to TSA leadership to assist in determining which CAPPS changes to

adopt. In a memorandum to TSA leadership, the SCPC team leader reported that these data were saved on two computer hard drives, and were accessible by only two employees. Data were not accessible via TSA's network.

TSA did not discuss passengers' data privacy, confidentiality, or security by TSA in advance of the transfer. Neither TSA nor individual staff working on the project signed confidentiality or non-disclosure agreements with JetBlue pursuant to the data exchange. Despite this, TSA did not release or transfer the SCPC passenger information to another party. Furthermore, TSA states that it did not access or retrieve any data on any passengers by individual identifier.[51] TSA told us that no other airlines transferred passenger data to TSA for this project.

The JetBlue passenger data received by the SCPC has not been returned or destroyed due to pending FOIA requests. At this time, TSA has not determined whether the passenger data is responsive to the FOIA requests.[52]

Conclusions

Although we found no evidence of harm to individual privacy, TSA could have taken more steps to protect privacy. TSA did not consistently apply privacy protections in the course of its involvement in airline passenger data transfers. This inconsistency pertained to TSA's efforts in acquisitions, contract enforcement, and internal practice.

Although TSA and the FAA, acting on TSA's behalf, included language guarding data security and confidentiality of personal information in some acquisition instruments used in CAPPS II development, they did not do so in all cases. The May 2002 research grant to AAI and the December 2003 contract with IBM both included text requiring the funding recipients to implement and report on data security and data privacy protection efforts. The May 2002 cooperative agreements signed with the four RAE prototype vendors, however, did not contain provisions limiting the use or disclosure of personal information.

TSA did not completely monitor or enforce adherence to good privacy practices among the parties involved in passenger data transfers. CAPPS II management was not acquainted with the details of related airline passenger data exchanges

[51] Department of Homeland Security, Transportation Security Administration, Office of Chief Counsel, *Report on Passenger Name Record Data Exchanges Involving Projects to Improve Passenger Screening*, August 18, 2004, p. 36.
[52] Ibid., p. 36.

and, therefore, could not determine whether these transfers were appropriate. Although TSA evaluators of the RAE prototype vendors assessed their performance in the area of data security and privacy protection, evaluators did not track the vendors' independent efforts to obtain passenger data.

CAPPS II program staff facilitated the transfer of JetBlue passenger data to Torch Concepts, but did not keep tabs on the resulting data exchange.
CAPPS II program staff did not follow up on a request for copies of relevant non-disclosure agreements, nor did TSA request an accounting of Torch Concepts' utilization or disposition of the passenger data that it received.

This pattern also characterized TSA's oversight of the RAE prototype vendors. TSA did not carefully track vendors' independent progress in obtaining airline passenger data to develop, test, and demonstrate their prototype systems. In addition, the agency neglected to inquire whether airline passenger data used by the vendors had been returned or destroyed.

In the case of the data transfer to support CAPPS improvement efforts, TSA staff did not follow accepted privacy procedures in obtaining passenger data for internal use. First, TSA did not obtain non-disclosure or confidentiality agreements with JetBlue before receiving airline passenger data in May 2003. These agreements could have provided a declaration of data usage and set important restrictions on disclosure. Second, TSA did not ensure that data security measures were in place during the data transfer. As a result, passenger data was transmitted to TSA in unencrypted files without password protection.

Despite TSA's intermittent lack of sound privacy practices enforcement among its partners and its own staff, only one inappropriate public disclosure of personal information apparently occurred. Torch Concepts' inadvertent disclosure of sensitive information associated with a single JetBlue passenger occurred in breach of its confidentiality agreement with the data provider, Acxiom.

Finally, airline passenger records were not maintained in such a way as to have required TSA to publish a Privacy Act system of records notice. Neither TSA nor its contractors accessed or retrieved airline passenger records by individually identifying particular. As a result, none of the passenger data received or maintained by TSA or its proxies may be considered a system of records under the Privacy Act.

We recommend that the Assistant Secretary for Transportation Security, in coordination with the Chief Privacy Officer, as appropriate:

Recommendation 1: Develop clear protocols for obtaining airline passenger data and facilitating its exchange among other parties.

Recommendation 2: Ensure privacy and personal data protections are written into acquisition documents where performance may involve the collection, maintenance, use, or dissemination of individually identifiable data.

Recommendation 3: Require final reporting for acquisitions with intensive data analysis or processing components that addresses data receipt, processing, distribution, utilization, and disposition, as well as attention to data security and privacy.

Recommendation 4: Require entities performing work for TSA to report to the agency on how they are addressing data security, privacy protections, and confidentiality.

Information Disclosure Regarding Airline Passenger Data Transfers

Statements TSA officials made about the agency's role in passenger data sharing in response to FOIA requests, U.S. Senate testimony, and media inquiries were at times incorrect. The fact that accurate information about data transfers was not immediately disclosed to the public fueled perceptions that TSA was withholding information about its use of airline passenger data.

FOIA Requests

In September 2003, TSA received hundreds of electronic and paper FOIA requests soliciting all agency records regarding the accessing or use of JetBlue passenger data that were indexed or maintained under the requester's name or other identifying information in connection with various security systems. These FOIA requests were prepared using a template available on the American Civil Liberties Union (ACLU) web site.

In coordination with the TSA FOIA office, the agency's OCC contacted ONRA and asked it to search for relevant documents. On September 25, 2003, ONRA

replied that it did not have JetBlue records.[53] On that same day, OCC staff wrote to the CPO that ONRA had no responsive records. Replying to the OCC's e-mail, the CPO wrote, "Is there elsewhere in TSA that we should search?" OCC responded, "There is no other office in TSA that would get PNR data except ONRA." Nonetheless, OCC also consulted with staff from the agency's CIO to determine whether they had any JetBlue passenger data.

When ONRA and CIO staff reported that neither had records responsive to the FOIA requests, TSA drafted a response, which is still posted on the agency's FOIA reading room web site. The response asserts that TSA does not have JetBlue Airways passenger data; that response remained on the web site for over a year.

It is standard practice to assign FOIA requests to numerous offices within the agency to cast the widest net possible for document collection. We interviewed FOIA office staff on two occasions and reviewed their methods for assembling documents responsive to FOIA requests. Procedures pertaining to document collection for FOIA requests require FOIA office staff to ask TSA entities that might reasonably be expected to possess responsive documents to search their records. Searching for records responsive to FOIA requests is an agency-wide responsibility. To conduct thorough searches for documents, FOIA office staff often require input from other agency offices with broad based knowledge of TSA operations. Although TSA's Aviation Operations (AVOPS) was later found to possess JetBlue records, OCC and the FOIA office never asked AVOPS to search its files for documents responsive to these FOIA requests.

In September 2003, the ACLU and Electronic Privacy Information Center (EPIC) sent FOIA requests to TSA for, among other items, records "regarding access and/or use of JetBlue Airways … passenger data in connection with various security systems," and "documents or materials related to JetBlue Airways Corporation." TSA's FOIA office asked AVOPS to search for responsive records to these FOIA requests in late September, before reporting on the agency web site that TSA had no JetBlue Airways passenger data. Documents indicate, however, that TSA posted the statement that it had no JetBlue Airways passenger data before AVOPS responded to the ACLU and EPIC FOIA requests. When AVOPS reported to the FOIA office on these requests, it stated that it had "no records relative to the request[s]." The JetBlue passenger records in AVOPS possession were not

[53] In two separate visits to ONRA, we reviewed records related to PNR data and documentation of attempts to obtain PNR data. We found no evidence of JetBlue or any other airline PNR data at ONRA, except those limited staff records that had been reported on by the GAO.

reported to FOIA staff until May 2004.[54] When AVOPS provided the JetBlue passenger records to the FOIA office, staff there took precautions not to copy or distribute them and locked them in the office document room, where they remain.

In April 2004, Wired News and ACLU sent additional FOIA requests to TSA asking broadly for any records related to the sharing or acquisition of airline passenger records. Along with the September requests from the ACLU and EPIC, these FOIA requests were transferred to DHS' departmental disclosure officer who, as of November 2004, was processing documents for release to the requesters.

We recommend that the Assistant Secretary for Transportation Security, in coordination with the Chief Privacy Officer, as appropriate:

Recommendation 5: Re-evaluate TSA's response to FOIA requesters who solicited information in September 2003 regarding their airline passenger data. Such a reevaluation should, at minimum, involve the removal or amendment of the letter posted on TSA's FOIA reading room web site to reflect the fact that TSA is in possession of JetBlue passenger data.

U.S. Senate Testimony

TSA employees assisted in preparing responses to a pre-hearing questionnaire for the DHS Deputy Secretary's November 18, 2003, confirmation hearing before the U.S. Senate Committee on Governmental Affairs.[55] One question sought information about TSA's role in the transfer of JetBlue passenger information to Torch Concepts. The November 18, 2003, response to the question stated that TSA provided assistance "…only in the form of an introduction for DOD to JetBlue Airlines [sic]."

In late November or early December 2003, TSA staff located a July 30, 2002, memorandum from the CAPPS II program manager to JetBlue's security director requesting that the airline provide PNR data to Torch Concepts. Because this memo contradicted the Deputy Secretary's November 18, 2003, response to the Committee on Governmental Affairs, on February 23, 2004, the Deputy Secretary sent a letter to the Chairman of the Committee amending his prior statement. His

[54] These passenger records related to the effort to improve the existing CAPPS program.
[55] At the start of the 109th session of Congress, the U.S. Senate Committee on Governmental Affairs became the Senate Committee on Homeland Security and Governmental Affairs.

statement was amended to read, "In a July 30, 2002 memorandum, TSA requested that JetBlue provide archived passenger data to the DOD." TSA staff did not provide a clear explanation as to why this memorandum was not brought to the Deputy Secretary's attention before the November 18, 2003, hearing.

In another confirmation pre-hearing question, the U.S. Senate Committee on Governmental Affairs asked whether contractors working on CAPPS II had used any real world data for testing purposes. The Deputy Secretary's response was that "TSA has not used any PNR data to test any of the functions of CAPPS II. TSA is using certain information provided by volunteers, many are DHS employees," including senior DHS officials.[56] TSA did use volunteered information to test CAPPS II; however, PNR data also was used to test some of the system's functions.[57]

Government Accountability Office and Media Reports

In February 2004 testimony before Congress on CAPPS II implementation challenges, the Government Accountability Office (GAO) said, "…TSA has only used 32 simulated passenger records – created by TSA from the itineraries of its employees and contractor staff who volunteered to provide the data – to conduct [passenger risk assessment] testing."[58] On this point, Wired News questioned whether TSA intentionally withheld information from GAO.[59] After reviewing GAO documents relating to the above statement in its testimony and interviewing TSA employees, we have found no evidence that TSA provided misleading or inaccurate information to the GAO.

As the basis for the above statement in its CAPPS II testimony, GAO relied on interviews with ONRA staff. Records of meetings between GAO and ONRA staff show that GAO specifically asked about ONRA's access to airline passenger data. GAO's questions concentrated on stress tests and systemwide testing for CAPPS II and not the testing of system prototypes or components. Furthermore, when asked about ONRA's relationship with Delta and travel data systems, ONRA staff

[56] Pre-hearing questionnaire for the nomination of the DHS Deputy Secretary, November 18, 2003, hearing to the Senate Committee on Governmental Affairs, question number 64.
[57] IBM and Infoglide received PNR data from Delta to test CAPPS II components. In addition, RAE prototype vendors used PNR data on numerous occasions to demonstrate and test their prototypes.
[58] Government Accountability Office, *Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385, February 2004, p. 17.
[59] "More False Information from TSA," Wired News, June 23, 2004.

told GAO that Delta had supplied data for testing the CAPPS II ADI component and that ONRA was in discussions with Sabre about using its data for testing.

GAO's report about CAPPS II testing specifically referred to demonstrating the full CAPPS II system. Although partial system testing occurred for a short time in February 2003, Delta data and prototype testing occurred in mid-2002. Full CAPPS II system testing never occurred because airline passenger data was not available.

In September 2003, a TSA spokesman told Wired News that CAPPS II had not been tested on any historical travel data and that only fake passenger data had been used.[60] Wired News also asked a separate TSA spokesman in September 2003 whether TSA's four contractors had used real passenger records to test and develop their systems. According to the article, the spokesman denied that four contractors had used real passenger records and said TSA had only used "dummy data."[61]

The responses that the TSA spokesmen provided to Wired News were not accurate. CAPPS II prototypes and components were tested using authentic passenger data on eleven occasions. Moreover, eight of the cases involved the CAPPS II program's RAE prototype vendors.

Disclosure of Information to the DHS Privacy Office

The CPO expressed concern that TSA had not been fully forthcoming in providing information requested from the agency for the February 20, 2004, *Report to the Public on Events Surrounding JetBlue Data Transfer*. We reviewed eight written requests for information that the CPO sent TSA prior to February 20, 2004, and reviewed TSA's responses. We concluded that TSA was promptly responsive to most of the CPO's requests. However, in one case, TSA was not promptly forthcoming with the CPO.

We reviewed requests the CPO sent to the following offices: TSA Public Affairs; ONRA; the assistant administrator for Policy; the administrator, deputy administrator and chief of staff; the FOIA office; and the Office of Chief Counsel (OCC). The CPO's requests for information were for documents specifically related to the transfer of JetBlue PNRs to DOD subcontractor Torch Concepts. In

[60] "JetBlue Data to Fuel CAPPS Test," *Wired News*, September 16, 2003.
[61] "More False Information from TSA," *Wired News*, June 23, 2004.

requesting information, the CPO expressed a sense of urgency; however, only one of the eight requests that we reviewed contained a specific response deadline.[62]

In one case, TSA was not promptly forthcoming in providing documents to the CPO. In November and December 2003, TSA sought information from its employees to respond to a letter that the Ranking Member of the U.S. Senate Judiciary Committee had sent to the DHS Secretary inquiring about TSA's role in the JetBlue data transfer to Torch Concepts.[63] TSA forwarded a draft response and eleven supporting documents to DHS for review in January 2004. Although all of these materials were germane to the CPO's inquiry, a list of the supporting documents was not provided by TSA to the CPO until February 17, 2004. The CPO said that receipt of a list of these documents six weeks after they had been compiled, and three days before publication of the DHS Privacy Office report, gave the impression that TSA had withheld the documents.

The TSA employee who drafted the response letter and compiled the supporting documents said that, at the time, she believed that the documents in question had been included in the materials that TSA had provided the CPO on another occasion. The DHS Privacy Office had received these materials earlier, but the documents had not been furnished by TSA. Instead, the DHS Privacy Office received the documents on February 13, 2004, from headquarters staff at DHS' Border and Transportation Security directorate. Had TSA provided these materials to the DHS Privacy Office when they became available, the CPO would have had substantially more time to review them before the DHS Privacy Office's report was issued. OCC staff reported, however, that TSA did not know when the DHS Privacy Office intended to publish its report.

Neither TSA nor the DHS Privacy Office had a system to track or locate documents provided in response to requests of this nature. Since TSA had provided thousands of pages of documents to the CPO as they became available, it is likely that the documents associated with the congressional response letter were overlooked.

In addition to these documented requests, the CPO said that she asked TSA for information about other airline data transfers before her office's report was released in February 2004. The CPO reports that TSA responded that the JetBlue matter was unique and suggested that TSA did not have a role in any other airline data transfers. We have been unable to find documentation that unequivocally

[62] See Appendix I for additional details about the CPO's eight requests to TSA.
[63] The letter from Senator Patrick Leahy was dated October 10, 2003.

corroborates this account and TSA staff we interviewed do not recall a broad request for information about airline passenger data transfers during that period. TSA responded to a March 2004 request from the CPO for information about other airline passenger data transfers the following month, after gathering relevant documents.

Conclusions

These cases illustrate weaknesses and a lack of reliability in the way that TSA processes requests for information. Although we found no evidence of deliberate deception, the evidence of faulty processes is substantial.

At least three factors contributed to TSA's shortcomings in its disclosure of information on its role in the transfer of airline passenger data. First, management of the CAPPS II program team had shifted three times since its formation. These management changes included significant staff turnover. This, in turn, hampered TSA's ability to gather and interpret information and documents related to early program developments quickly.

Second, TSA staff who gathered information for requesters were sometimes provided with inaccurate or misleading information. Relying on his memory of events, the former CAPPS II program manager who wrote JetBlue to request that the airline provide data to Torch Concepts initially said he had only introduced Torch Concepts to JetBlue. In another case, until recently, Delta asserted that the real passenger records that it had provided to IBM and Infoglide were simply mock records.

Third, TSA did not have systems in place to support effective searches for materials responsive to document requests. In the case of a FOIA request, TSA did not solicit information from all relevant components. In another case, TSA staff were unable to determine what had been provided to the CPO, so important documents were not forwarded in a timely manner.

TSA's inadequate performance in disclosing information on its role in the transfer of airline passenger data indicates a need for closer tracking of requests and greater internal accountability for responses. Accordingly, we recommend that the Assistant Secretary for Transportation Security:

Recommendation 6: Adopt procedures for responding to external and intra-departmental requests for information that help guarantee a comprehensive, timely, and reliable response. At minimum, these procedures should include the:

- Designation of a primary point of contact and responsible staff person;
- Documentation of the scope of the search conducted for each request;
- Listing of materials provided to the requester; and
- Issuance of a formal written response indicating that the search for related documents and information has concluded.

TSA Privacy Focus

Personal privacy issues have commanded attention within TSA since its inception in November 2001. In the spring of 2002, attorneys with the OCC prepared and presented analyses of legal issues pertaining to the agency's collection and use of data. Early legal analysis detailed, for example, the statutory basis for TSA's authority to collect airline passenger data. Contemporary OCC guidance also addressed questions about the statutory rules regarding the use of particular types of personal information. OCC staff monitored CAPPS II developments through regular attendance of weekly program meetings and consulted with program staff.

Early CAPPS II development work centered on system conceptualization and the identification of technical solutions to implement the system. As the planning and basic technical feasibility work drew to a close, CAPPS II program staff drafted and published an initial system of records notice for the program in January 2003. This first broad-scale announcement of the general outline of the program was performed in concert with outreach efforts to a wide-ranging group of stakeholders. In January and March 2003, TSA convened stakeholders from across government and the private and nonprofit sectors to discuss CAPPS II.[64] The meetings were called to gather input on how TSA could best address privacy concerns in structuring CAPPS II.

Over the past twenty months, a number of important changes have expanded the prominence of privacy concerns in the TSA's operations. In March 2003, TSA was incorporated into DHS. With a new department came a new privacy oversight system. Enabling legislation for the department called for hiring a chief privacy officer with authority to rule on internal privacy procedures and report

[64] Attendees included senior executives from the ACLU, American Conservative Union, Center for Democracy and Technology, Eagle Forum, and Potomac Institute for Policy Studies.

to Congress.[65] DHS' chief privacy officer, appointed on April 16, 2003, was an active agent in privacy discussions relating to CAPPS II from mid-2003 forward.

Provisions of the E-Government Act requiring agencies to perform PIAs under a number of circumstances became effective on April 17, 2003. Under most circumstances, these PIAs are publicly available and offer detailed information on all new and modified systems maintained by federal agencies that include information on more than ten individuals. Systems with data on foreign nationals and federal employees are exempt from this requirement.

In this new legal and organizational context, TSA released a second CAPPS II notice. After reviewing public comments on its initial notice, on August 1, 2003, TSA published an Interim Final Notice on CAPPS II.[66] Consistent with an operating environment increasingly sensitive to public concerns regarding privacy, this second notice provided substantially more detail on system plans and design.

In March 2004, TSA unveiled a plan to support good privacy practice within the organization. The TSA Assistant Secretary affirmed the agency's commitment to privacy by declaring that, "in carrying out the TSA mission to secure our nation's transportation systems, we must respect and protect the privacy rights of all individuals we serve." This five-point plan included the:

- Implementation of ongoing educational and training programs for all employees;
- Appointment of an external privacy advisory board;
- Dissemination of a privacy statement specific to the tasks and circumstances at TSA;
- Enforcement of specific internal policies and controls on use of data and private information; and
- Hiring of a privacy officer to oversee compliance and to report on agency performance.

TSA has successfully implemented three of the five privacy plan elements. TSA issued a privacy statement and hired a privacy officer in March 2004, and is engaged in the development and delivery of staff training programs. On March

[65] DHS' chief privacy officer is responsible for department-wide compliance with the Privacy Act and for evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the federal government.
[66] 68 Fed. Reg. 45265 (Aug. 1, 2003).

8-12, 2004, TSA conducted a privacy education week with a series of programs emphasizing the roles and responsibilities of employees in protecting individual privacy. Additionally, TSA has mandated that all staff members participate in multimedia training on protection of personal privacy rights. According to TSA, 98% of its headquarters staff and 81% of field employees had completed a Privacy Act training program as of early August 2004.[67]

Before testing its new passenger pre-screening system, Secure Flight, TSA opened information on program testing to public comment. On September 24, 2004, TSA published in the Federal Register a Secure Flight Privacy Act system of records notice, a PIA, and a proposed order to airlines to provide PNR data for system testing.[68] These documents describe the data to be used in system testing, the purpose of the testing, and the types of testing that will occur. They also articulate TSA's commitment to implement data security and privacy protections during the testing process and provide for strict oversight and appropriate personnel training.

From the prototype development stage of CAPPS II in mid-2002 to the present, TSA has evolved with respect to its approach to privacy. This transition is still under way as the agency weighs the sometimes competing values of security and privacy in the execution of its critical aviation security function.

We recommend that the Assistant Secretary for Transportation Security, in coordination with the Chief Privacy Officer, as appropriate:

Recommendation 7: Appoint a TSA external privacy advisory board, as specified in TSA's five-point plan, to review all agency privacy impact assessments, and, to provide consultation regarding the scope and methods of TSA supported data analysis and research involving individually identifiable data.

Recommendation 8: Develop procedures that will provide a clear process to: (1) approve the agency's role in data sharing that involves individually identifiable information; and, (2) identify a particular employee responsible for monitoring the data security, usage, and final disposition of each transfer of individually identifiable information in which TSA becomes involved.

[67] TSA has approximately 53,000 employees.
[68] 69 Fed. Reg. 57342-57348 and 57352-57355 (Sept. 24, 2004).

U.S. Department of Homeland Security
Office of the Administrator
601 South 12th Street
Arlington, VA 22202-4220

JAN 14 2005

Transportation Security Administration

MEMORANDUM FOR: Richard L. Skinner, Acting Inspector General
Department of Homeland Security

THROUGH: Asa Hutchinson, Under Secretary
Border and Transportation Security

FROM: David M. Stone, Assistant Secretary
Transportation Security Administration

SUBJECT: Transportation Security Administration Response to The "Review of the Transportation Security Administration's Role in the Use and Dissemination Of Airline Passenger Data"

This memorandum constitutes the Transportation Security Administration's (TSA) response to your Draft Report on the "Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data." Thank your for your efforts to provide a clear and thorough account of TSA's involvement in the activities relevant to this report.

The accompanying attachment is TSA's official agency comment on the recommendations raised in the Draft Report, as well as additional comments on the overall Report. We look forward to an ongoing relationship with your office as we work towards improving our data management practices.

Attachment

TSA Response to DHS OIG Report:
"Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data"

Recommendation 1: Develop clear protocols for obtaining airline passenger data and facilitating its exchange among other parties.

The Transportation Security Administration (TSA) agrees with this recommendation and has taken the steps to implement it in its recent efforts to develop a new passenger prescreening program. On November 15, 2004, TSA obtained, pursuant to an order to U.S. air carriers issued after a period of extensive review and public comment, historical passenger name records (PNR) to support testing of a new advance passenger prescreening program known as Secure Flight. TSA issued an accompanying Privacy Impact Assessment and Privacy Act System of Records notice specifying the manner in which PNR data was to be delivered and the safeguards TSA would employ in protecting the data from unauthorized use and disclosure. Prior to implementation of Secure Flight, TSA will prepare a Concept of Operations (CONOPS) document to address the means by which airline passenger data will be obtained and the required format for delivery.

Using the approved CONOPS document, Operational Procedures will be developed, approved, and tested for each key activity prior to live operations with the first participating airline and documented in an Interface Control Document. Memoranda of Understanding will be negotiated and executed with all departments or agencies that will manage or handle data as they participate in the development and implementation of the Secure Flight program. In these agreements, all of the required activities and responsibilities of the parties will be clearly defined.

TSA worked diligently with the air carriers prior to the test phase of the Secure Flight program to ensure that air carriers could comply with TSA's order to submit PNR in a secure manner. TSA also instituted internal procedures, including a chain of custody procedure for the receipt, handling and transmission of the data sent to TSA.

Recommendation 2: Ensure privacy and personal data protections are written into acquisition documents where performance may involve the collection, maintenance, use, or dissemination of individually identifiable data.

TSA agrees with this recommendation. TSA has developed a Data Security and Control Policy that governs the procedures for handling and safeguarding Personally Identifiable Information provided to a contractor as Government Furnished Information. TSA also has developed a supplement to the policy that outlines procedures for the collection, receipt, handling, storage, and destruction of PNR data by designated individuals. For the Secure Flight program test phase, the TSA Privacy Officer is the point of contact for receipt of all passenger data sent to TSA. The Privacy Officer developed and implemented a Chain of Custody procedure for the handling of such data.

TSA's Acquisition Management System has standard privacy and personal data protection clauses (including Privacy Act and Privacy Act Notification clauses) that are included in all contracts and agreements where privacy and personal data are involved. The clauses are provided as Attachment 1, and require TSA contractors and their subcontractors comply with the Privacy Act. TSA requires that all contractors, in addition to all employees, receive appropriate training in Privacy Act matters prior to handling personally identifiable information.

Recommendation 3: Require final reporting for acquisitions with intensive data analysis or processing components that address data receipt, processing, distribution, utilization, and disposition, as well as attention to data security and privacy.

TSA agrees with this recommendation and will ensure these items are covered in the appropriate acquisition documents. Data security and privacy issues will be coordinated with the TSA Chief Information Security Officer and TSA Privacy Office. TSA is considering revising the standard Privacy Act clause (see response to Recommendation 2) to incorporate standard periodic and final reporting requirements for data-intensive contracts.

Recommendation 4: Require entities performing work for TSA to report to the agency on how they are addressing data security, privacy protections and confidentiality.

TSA agrees with this recommendation. As discussed in response to the previous three recommendations, TSA's acquisition documents will require compliance with established policies, procedures, and reporting related to data security, privacy protection, and confidentiality as established by the Department of Homeland Security (DHS) and TSA Privacy Offices.

In addition to revising the standard Privacy Act clause, in the pre-award phase of data-intensive contracts TSA intends to evaluate offerors' plans for ensuring the security and privacy protection of personal data throughout the lifecycle of the contract, regardless of the source of information.

Recommendation 5: Re-evaluate TSA's response to FOIA requesters who solicited information in September 2003 regarding their airline passenger data. Such a reevaluation should, at a minimum, involve the:

- **Review of JetBlue airline passenger data under TSA's control to determine whether this data includes the records of any individual submitting a certified FOIA request for information regarding his or her JetBlue records; and**
- **Removal or amendment of the letter posted on TSA's FOIA reading room website to reflect the fact that TSA is in possession of JetBlue passenger data.**

The Freedom of Information Act (FOIA) requires agencies to undertake a search reasonably calculated to discover responsive records. TSA fully complied with its obligations to process the referenced FOIA requests at the time the requests were received. The few JetBlue airline passenger data records recently discovered in an electronic file with access restricted to only two TSA employees underscores the reasonableness of the TSA search and does not support a further review of TSA's response to FOIA requesters who solicited information regarding their data.

TSA has removed the letter posted on TSA's electronic FOIA reading room. TSA requests that this recommendation be considered closed.

Recommendation 6: Adopt procedures for responding to external and intra-departmental requests for information that help guarantee a comprehensive, timely, and reliable response. At minimum, these procedures should include the:

- **Designation of a primary point of contact and responsible staff person;**
- **Documentation of the scope of the search conducted for each request;**
- **Listing of materials provided to the requester; and**
- **Issuance of a formal final response indicating that the search for related documents and information has concluded.**

TSA agrees with this recommendation. In the case of information requests involving privacy-related issues originating from the DHS Chief Privacy Officer, TSA has designated its Privacy Officer as the principal point of contact with the office of the DHS Chief Privacy Officer to coordinate and track responses to information requests from that office.

Recommendation 7: Appoint a TSA external privacy advisory board, as specified in TSA's five-point plan, to review all agency privacy impact assessments, and, to provide consultation regarding the scope and methods of TSA supported data analysis and research involving individually identifiable data.

TSA recognizes the importance of effective oversight of privacy impact assessments and data analysis and has taken a number of steps to enhance privacy oversight, including some specific to passenger prescreening and PNR. TSA has hired a Privacy Officer who provides guidance to TSA's program offices regarding all issues related to the collection and use of personally identifiable information. The TSA Privacy Officer also coordinates and approves the preparation of Privacy Impact Assessments (PIAs) for TSA programs. Program offices are given guidance by the TSA Privacy Officer in developing their programs and PIAs to include careful consideration of privacy risks and mitigation measures. The TSA Privacy Officer also works to obtain review and approval of PIAs from the DHS Chief Privacy Officer.

In relation to passenger prescreening and PNR, now a function of the "Secure Flight" program, TSA has established an external working group consisting of members from the privacy community as well as IT specialists, who will be responsible for evaluating the

privacy standards and practices as well as the security mechanisms for the program. TSA will carefully review the findings of the working group and, where appropriate, incorporate them into the Secure Flight program.

Finally, the Department's Privacy Office is creating a department-wide privacy oversight group to review all programs involving personally identifiable data.

Recommendation 8: Develop procedures that will provide a clear process to: (1) approve the agency's role in data sharing that involves individually identifiable information; and, (2) identify a particular employee responsible for monitoring the data security, usage, and final disposition of each transfer of individually identifiable information in which TSA becomes involved.

TSA agrees with this recommendation. Currently, the TSA Privacy Officer, in coordination with Office of Chief Counsel and the DHS Privacy Office, advises program offices on applicable requirements governing sharing of personally identifiable information. For the Secure Flight program, TSA has designated the Information System Security Officer for the Office of Transportation Vetting and Credentialing as the individual responsible for the receipt, control, storage, and tracking of the data as well as for conducting periodic audits of contractor workstations and storage devices to ensure compliance with established policies and procedures.

Attachment 1

3.7-1 Privacy Act Notification (February 2003)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations (49 CFR Part 10). Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

3.7-2 Privacy Act (February 2003)

(a) The Contractor agrees to--

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations (49 CFR Part 10) issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies--

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract that requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c) (1) 'Operation of a system of records,' as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

Attachment 1

(2) 'Record,' as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) 'System of records on individuals,' as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of clause)

We evaluated TSA's written comments to the draft report and made changes, as appropriate, to the final version. Below is a summary of our analysis of TSA's response to the recommendations contained in the draft report.

Recommendation 1: Develop clear protocols for obtaining airline passenger data and facilitating its exchange among other parties.

TSA Response: TSA concurs with this recommendation and writes that it has taken steps to address it. Citing its efforts related to the Secure Flight passenger pre-screening system as evidence of progress in this area, TSA points to its published PIA and Privacy Act system of records notice that indicate how test data is to be transferred and outline safeguards TSA will use to protect this data from unauthorized use or disclosure. In its remarks, TSA also highlights plans to prepare a Concept of Operations document stipulating how PNR data is to be obtained for Secure Flight, as well as related Operational Procedures. In addition, TSA discusses plans to execute MOUs that clearly define roles and responsibilities with other agencies and departments that will handle data in the development and implementation of Secure Flight. Importantly, TSA also reports that it has instituted internal procedures covering the receipt, handling and transmission of data sent to the agency.

OIG Evaluation: TSA has pursued a more formalized process for obtaining and sharing data in its efforts regarding the Secure Flight system than in the past. To determine whether TSA has developed clear protocols for obtaining and exchanging airline passenger data, however, we will need to review the agency's related internal procedures. Recommendation 1 is resolved – open.

Recommendation 2: Ensure privacy and personal data protections are written into acquisition documents where performance may involve the collection, maintenance, use, or dissemination of individually identifiable data.

TSA Response: TSA concurs with this recommendation. TSA states that it now includes clauses on privacy and personal data protection in all contracts and agreements in which privacy and personal data are involved.

OIG Evaluation: The incorporation of clauses on privacy and personal data protection into applicable contracts and agreements is responsive to this recommendation. Recommendation 2 is closed.

Recommendation 3: Require final reporting for acquisitions with intensive data analysis or processing components that addresses data receipt, processing, distribution, utilization, and disposition, as well as attention to data security and privacy.

TSA Response: TSA concurs with this recommendation and has committed to ensure that final reporting of this kind occurs. In addition, TSA is considering revisions to standard acquisitions language to require periodic and final reporting for data-intensive contracts.

OIG Evaluation: TSA's commitment to ensure final reporting on data receipt, processing, utilization, and disposition, as well as data security and privacy in acquisitions is promising. The revision of standard contract language to require periodic and final reporting for data-intensive contracts will be fully responsive to this recommendation. Recommendation 3 is resolved – open.

Recommendation 4: Require entities performing work for TSA to report to the agency on how they are addressing data security, privacy protections, and confidentiality.

TSA Response: TSA concurs with this recommendation and has taken steps to implement it. TSA states that, for agency acquisitions, it will require compliance with data security, privacy protection, and confidentiality policies, procedures, and reporting set forth by the DHS and TSA Privacy Offices. TSA also expresses its intent to evaluate offerors' data security and privacy protections in the pre-award phase of data-intensive contracts.

OIG Evaluation: TSA's commitment to evaluate offerors' plans for ensuring data security and privacy protection is partially responsive to this recommendation. Coupled with this, the planned revision of standard contract language described in the agency's response to the previous recommendation would be fully responsive to this one. Recommendation 4 is resolved – open.

Recommendation 5: Re-evaluate TSA's response to FOIA requesters who solicited information in September 2003 regarding their airline passenger data. Such a reevaluation should, at minimum, involve the removal or amendment of the letter posted on TSA's FOIA reading room web site to reflect the fact that TSA is in possession of JetBlue passenger data.

TSA Response: TSA believes that it fully complied with its obligation to conduct a reasonable search for records responsive to FOIA requests submitted using a template on the ACLU web site. TSA also reports that it has removed the letter asserting that the agency had no JetBlue passenger data from its FOIA reading room website.

OIG Evaluation: We modified this recommendation in response to comments from TSA and the DHS Privacy Office. TSA's removal of the letter in question from its FOIA reading room web site is an acceptable response to this recommendation in its current form. Recommendation 5 is closed.

Recommendation 6: Adopt procedures for responding to external and intra-departmental requests for information that help guarantee a comprehensive, timely, and reliable response. At minimum, these procedures should include the:

- Designation of a primary point of contact and responsible staff person;
- Documentation of the scope of the search conducted for each request;
- Listing of materials provided to the requester; and
- Issuance of a formal written response indicating that the search for related documents and information has concluded.

TSA Response: TSA concurs with our recommendation to adopt procedures for responding to external and intra-departmental requests for information. For privacy-related information requests originating from the DHS Privacy Office, the TSA privacy officer is the now the principal point of contact. The TSA privacy officer is now responsible for coordinating and tracking responses to information requests from the DHS Privacy Office.

OIG Evaluation: TSA's designation of its privacy officer as the principal point of contact for requests from the DHS Privacy Office is partially responsive to this recommendation. The scope of our recommendation extends beyond TSA's interaction with the DHS Privacy Office. Our recommendation is intended to ensure that TSA has a system in place to respond to requests for information and materials not covered under current guidelines or procedures. Before closing this recommendation, we must confirm that TSA's procedures for responding to requests from organizations other than the DHS Privacy Office includes all of the elements described in the recommendation. Recommendation 6 is resolved – open.

Recommendation 7: Appoint a TSA external privacy advisory board, as specified in TSA's five-point plan, to review all agency privacy impact assessments, and, to provide consultation regarding the scope and methods of TSA supported data analysis and research involving individually identifiable data.

TSA Response: TSA acknowledges the importance of effective oversight and describes planned and existing privacy oversight mechanisms. TSA's privacy officer provides guidance on the gathering and utilization of personally identifiable information, and coordinates and approves PIAs for TSA programs in collaboration with the CPO. In its efforts surrounding the development and implementation of the Secure Flight passenger pre-screening system, TSA has constituted an external working group to evaluate privacy standards and practices, as well as program security measures. TSA also notes that the DHS Privacy Office is forming a privacy oversight group that will serve as a future oversight apparatus in this area.

OIG Evaluation: Although TSA acknowledges the importance of effective oversight in its comments, it does not articulate plans for forming a TSA-wide privacy advisory board with a mission as described in our recommendation. Nevertheless, the TSA and DHS privacy officers currently address the intended PIA review function of such an advisory board. Meanwhile, an external working group provides consultation that may address the scope and methods behind the Secure Flight data analysis and research. This working group, however, cannot be expected to provide consultation on the scope and methods of other data analysis and research efforts undertaken by the agency. Absent the formation of a TSA-wide advisory board to address these issues, TSA's declared commitment to form external working groups to perform this function on an ad hoc basis would be considered fully responsive to this recommendation. Recommendation 7 is resolved – open.

Recommendation 8: Develop procedures that will provide a clear process to: (1) approve the agency's role in data sharing that involves individually identifiable information; and, (2) identify a particular employee responsible for monitoring the data security, usage, and final disposition of each transfer of individually identifiable information in which TSA becomes involved.

TSA Response: TSA concurs with this recommendation. The TSA privacy officer, Office of Chief Counsel and the DHS Privacy Office currently advise program staff on requirements on sharing personally identifiable information. For the Secure Flight program, TSA has designated the Office of Transportation

Vetting and Credentialing's Information System Security Officer as responsible for monitoring compliance with privacy and confidentiality policies and procedures.

OIG Evaluation: TSA's response does not suggest that a clear process for approving agency participation in data transfers is in place. Nor does TSA's response identify a procedure for designating employees' responsible for data transfer monitoring activities. Recommendation 8 is resolved – open.

Recommendations

We recommend that the Assistant Secretary of Homeland Security for Transportation Security, in coordination with the Chief Privacy Officer, as appropriate:

Recommendation 1: Develop clear protocols for obtaining airline passenger data and facilitating its exchange among other parties.

Recommendation 2: Ensure privacy and personal data protections are written into acquisition documents where performance may involve the collection, maintenance, use, or dissemination of individually identifiable data.

Recommendation 3: Require final reporting for acquisitions with intensive data analysis or processing components that addresses data receipt, processing, distribution, utilization, and disposition, as well as attention to data security and privacy.

Recommendation 4: Require entities performing work for TSA to report to the agency on how they are addressing data security, privacy protections and confidentiality.

Recommendation 5: Re-evaluate TSA's response to FOIA requesters who solicited information in September 2003 regarding their airline passenger data. Such a reevaluation should, at minimum, involve the removal or amendment of the letter posted on TSA's FOIA reading room web site to reflect the fact that TSA is in possession of JetBlue passenger data.

Recommendation 6: Adopt procedures for responding to external and intra-departmental requests for information that help guarantee a comprehensive, timely, and reliable response. At minimum, these procedures should include the:

- Designation of a primary point of contact and responsible staff person;
- Documentation of the scope of the search conducted for each request;
- Listing of materials provided to the requester; and
- Issuance of a formal written response indicating that the search for related documents and information has concluded.

Recommendation 7: Appoint a TSA external privacy advisory board, as specified in TSA's five-point plan, to review all agency privacy impact

assessments, and, to provide consultation regarding the scope and methods of TSA supported data analysis and research involving individually identifiable data.

Recommendation 8: Develop procedures that will provide a clear process to: (1) approve the agency's role in data sharing that involves individually identifiable information; and, (2) identify a particular employee responsible for monitoring the data security, usage, and final disposition of each transfer of individually identifiable information in which TSA becomes involved.

Airline Passenger Data Transfers in this Report
Assistance to Other Agencies
● TSA facilitated the transfer of Delta Air Lines passenger data to the U.S. Secret Service in February 2002.
● TSA requested JetBlue Airways transfer passenger data to U.S. Army subcontractor Torch Concepts. Data was provided in September 2002.
CAPPS II Development Efforts
● While developing a prototype for CAPPS II, Ascent Technology accessed Delta Air Lines passenger data in June 2002.
● While developing a prototype for CAPPS II, HNC Software accessed records for Continental, Frontier, and America West Airlines passengers in mid-2002.
● While developing a prototype for CAPPS II, HNC Software accessed records for JetBlue Airways passengers in mid-2002.
● While developing a prototype for CAPPS II, HNC Software accessed passenger records from various airlines through HNC E-Tickets in mid-2002.
● In association with CAPPS II development efforts, Airline Automation, Inc. provided *TSA* and four CAPPS II vendors with American Airlines passenger records in May and June 2002. Each of these transfers is treated as a separate case. The four CAPPS II vendors were: ○ *Ascent Technology, Inc.* ○ *HNC Software, Inc.* ○ *Infoglide Software Corporation* ○ *Lockheed Martin Corporation*
● While developing another CAPPS II component, IBM accessed Delta Air Lines passenger records in February and March 2003.
● To test CAPPS II, TSA requested and received records for passengers on numerous airlines from Sabre Holdings in May 2003.
CAPPS I Improvement
● To assess ways to improve the existing CAPPS system, TSA requested and received JetBlue Airways passenger records in May and June 2003.

Confidentiality and Disposition of Airline Passenger Data Transferred				
Source Airline	**Data Provider**	**Data Recipient**	**Confidentiality Agreement***	**Final Data Disposition**
Delta	Delta	U.S. Secret Service	Yes	Destroyed
American	AAI	Ascent	Yes	Destroyed
American	AAI	HNC Software	Yes	Destroyed
American	AAI	Infoglide	Yes	Held in Secure Setting
American	AAI	Lockheed Martin	Yes	Held in Secure Setting
American	AAI	TSA - CAPPS II	No	Not Accessed; Not Retained
Delta	Delta	Ascent	Yes	Unknown
Continental, Frontier, America West	SHARES	HNC Software	Unknown	Unknown
JetBlue	Acxiom	HNC Software	Unknown	Unknown
Various	HNC E-Tickets	HNC Software	Unknown	Unknown
JetBlue	Acxiom	Torch Concepts	Yes	Some Data Compromised; Other Data Held in Secure Setting
Delta	Delta	IBM	Yes	Destroyed
Various	Sabre	TSA - ONRA	No	Not Accessed; Returned
JetBlue	JetBlue	TSA - AVOPS	No	Held in Secure Setting

* An agreement between the data provider and data recipient that sets out the intended uses of the data, restricts the sharing of the data, and binds the data recipient to maintain data confidentiality. Contracts, memoranda of understanding, confidentiality agreements, and non-disclosure agreements are examples of types of agreements that may meet this standard.

Summary Detail of Airline Passenger Data Transfers with TSA Involvement

Date(s) of Transfer	Data Transfer Parties			Data Description		
	Airline	Provider	Recipient	Records	Individuals	Travel Dates
February 2002	Delta	Delta	U.S. Secret Service	Unknown	Unknown	02/01/01-02/26/02
05/24/02, 06/17/02, 06/27/02-06/29/02	American	AAI	Ascent	~1,841,640*	Unknown	12/08/01-12/15/01, 06/22/02-06/29/02, …
05/24/02, 06/17/02, 06/27/02-06/29/02	American	AAI	HNC Software	~1,841,640	Unknown	12/08/01-12/15/01, 06/22/02-06/29/02, …
05/24/02, 06/17/02, 06/27/02-06/29/02	American	AAI	Infoglide	~1,841,640	Unknown	12/08/01-12/15/01, 06/22/02-06/29/02, …
05/24/02, 06/17/02, 06/27/02-06/29/02	American	AAI	Lockheed Martin	~1,841,640	Unknown	12/08/01-12/15/01, 06/22/02-06/29/02, …
06/17/02, 06/27/02-06/29/02	American	AAI	TSA - CAPPS II	~1,841,640	Unknown	06/22/02-06/29/02, …
Early June 2002	Delta	Delta	Ascent	N/A	Unknown	Unknown

* "~" denotes approximate figure based on available information.

Summary Detail of Airline Passenger Data Transfers with TSA Involvement

Date(s) of Transfer	Data Transfer Parties			Data Description		
	Airline	Provider	Recipient	Records	Individuals	Travel Dates
Mid 2002	Continental	SHARES	HNC Software	787,081	Unknown	06/20/02- 07/03/02
Mid 2002	Frontier			70,523	Unknown	06/20/02- 07/03/02
Mid 2002	America West			589,515	Unknown	06/20/02- 07/03/02
Mid 2002	JetBlue	Acxiom	HNC Software	2,725,352	Unknown	01/13/02- 09/05/02
Mid 2002	*Various*	HNC E-Tickets	HNC Software	400,000	Unknown	06/20/02- 06/25/02
Mid 2002	Unknown	WorldSpan	Infoglide	~13,000,000	Unknown	Unknown
September 2002	JetBlue	Acxiom	Torch Concepts	~5,000,000	2,226,715	Unknown
02/27/2003	Delta	Delta	IBM	~1,000,000	Unknown	Unknown
May 2003	*Various*	SABRE	TSA - ONRA	~1,500,000	Unknown	Unknown
05/14/03, 05/23//03, 06/04/03	JetBlue	JetBlue	TSA - AVOPS	3,909	Unknown	07/29/02, 01/21/03, 01/23/03, 03/11/03, 05/18/03, 05/20/03, 06/01/03

Privacy Act of 1974

The provisions of the Privacy Act are invoked when a system that meets the legal standard for a "system of records" is created or maintained. Such a system must be under the control of a federal agency and contain individually identifiable information. In addition, a Privacy Act system of records must have records that are retrieved or accessed by a governmental entity or its proxy using an individually identifying particular, e.g., name, social security number, etc. Furthermore, according to TSA, the system must have a decision-making aspect that supports an agency function and has a bearing on individuals.[69] Systems of record covered by the Privacy Act include personnel files maintained in a file drawer as much as databases operating on computer networks.

Under the Privacy Act, notices for all systems of record are to be published in the Federal Register. Published systems of record notices document the authorities under which the government agency maintains the system of records, the purpose the system serves, the types of records contained in the system, and their routine uses. With limited exceptions, records covered by the Privacy Act may only be released in line with the "routine uses" of the system reflected in the system notice or with the consent of the individual to whom the record pertains.

Consistent with the Privacy Act, DOT published an initial system of records notice for CAPPS II on January 15, 2003.[70] After reviewing the substantial volume of public comments on the initial CAPPS II notice, TSA issued a revised Interim Final Notice for CAPPS II.[71] Published on August 1, 2003, the interim notice provided substantially more detail on CAPPS II design and proposed function.

Importantly, the Privacy Act also grants individuals certain rights over records pertaining to them. Provided such records are not maintained in an exempted system, individuals have the right to access, amend, and contest the accuracy of records about them.

[69] Department of Homeland Security, Transportation Security Administration, Office of Chief Counsel, *Report on Passenger Name Record Data Exchanges Involving Projects to Improve Passenger Screening*, August 18, 2004, pp. 50-52.
[70] 68 Fed. Reg. 2101 (Jan. 15, 2003).
[71] 68 Fed. Reg. 45265 (Aug. 1, 2003).

The Privacy Act also affords protections against improper access to and disclosure of information contained in a system of records. Criminal penalties may be applied under the statute in cases where the following has occurred:

- Information barred from disclosure has been disclosed;
- Systems of record have been willfully maintained without adherence to notification requirements; and
- Records have been requested or obtained under false pretenses.

E-Government Act of 2002

Provisions of the E-Government Act, effective on April 17, 2003, mandated that all agencies conduct PIAs for new information technology investments and new electronic information systems and collections. The PIA development process was designed to ensure that data handling is compliant with relevant laws, that agencies consider the risks and effects of their data systems, and that they examine system design alternatives that could mitigate privacy risks. Ultimately, PIAs result in published documents that address the following:

- What information is to be collected
- Why the information is being collected
- What are the intended uses of the information
- With whom the information will be shared
- What opportunities individuals have to decline to provide information or consent to particular uses of the information and how individuals can grant consent
- How the information will be secured
- Whether a system of records is being created under the Privacy Act.

The E-Government Act designated the Office of Management and Budget (OMB) as the entity responsible for detailing certain *E-Government Act* implementation requirements. OMB issued guidelines on when federal agencies are required to conduct PIAs. Specifically, OMB guidance requires the conduct of PIAs before:

- Developing or procuring [information technology] systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public; or
- Initiating a new electronic collection of information in identifiable form for 10 or more persons, excluding agencies, instrumentalities or

employees of the federal government; and, OMB also mandates the conduct of a PIA when changes to existing systems create new privacy risks.[72]

[72] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22 (Sept. 26, 2003).

Date	Flight #	Origin	Destination	Passengers
7/29/2002	47	JFK	FLL	[redacted]
1/21/2003	41	JFK	MCO	
1/23/2003	15	JFK	FLL	
1/23/2003	20	TPA	JFK	
1/23/2003	96	OAK	JFK	
1/23/2003	191	JFK	LAS	
3/11/2003	17	JFK	FLL	
3/11/2003	20	JFK	ROC	
3/11/2003	34	PBI	JFK	
3/11/2003	35	JFK	PBI	
3/11/2003	42	MCO	JFK	
3/11/2003	43	ROC	JFK	
3/11/2003	49	JFK	FLL	
3/11/2003	52	MCO	JFK	
3/11/2003	59	JFK	MCO	
3/11/2003	64	RSW	JFK	
3/11/2003	82	LGB	JFK	
3/11/2003	90	OAK	JFK	
3/11/2003	101	IAD	FLL	
3/11/2003	107	LGB	IAD	
3/11/2003	221	JFK	LGB	
3/11/2003	222	LGB	JFK	
3/11/2003	247	OAK	LGB	
3/11/2003	281	LAS	LGB	
3/11/2003	345	JFK	RSW	
5/18/2003	47	JFK	FLL	
5/20/2003	79	JFK	MCO	
6/1/2003	1	JFK	FLL	
6/1/????	25	JFK	FLL	
6/1/????	81	JFK	FLL	
			TOTAL	**3,925**

We reviewed documentation and conducted interviews regarding eight requests for information and summarized each of these requests and TSA's responses.

1. The CPO sent an e-mail on September 18, 2003, to a TSA public affairs officer requesting any documentation regarding the transfer of data by JetBlue to TSA or DOT. It does not appear from documents that we reviewed that this request was ever answered directly. On November 12, 2003, the TSA chief of staff e-mailed the CPO acknowledging TSA's non-responsiveness and stating that the public affairs officer had no information in response to the request.

2. On October 24, 2003, the CPO e-mailed the ONRA deputy director asking for "a thorough accounting of any contact with Torch Concepts, JetBlue, DOD or others, while at ONRA, DOT, or elsewhere, as it relates to the JetBlue incident." The same day, ONRA's deputy director responded via e-mail suggesting a meeting for November 11, 2003, and the CPO agreed.

3. The CPO sent an e-mail to TSA's Assistant Administrator for Policy on October 24, 2003, requesting that they discuss the JetBlue PNR transfer to Torch Concepts. We did not locate a direct response to the CPO's e-mail in documents we reviewed; however, the Office of the Assistant Administrator for Policy assisted with the document collection effort discussed in the next paragraph. In our May 4, 2004, interview with the CPO, she did not suggest the Assistant Administrator was not responsive to her requests.

4. On November 12, 2003, the CPO sent a request to the TSA Administrator, Deputy Administrator, and Chief of Staff asking for help to ensure a thorough internal review was made of any documents or personnel regarding the JetBlue PNR transfer. The CPO requested a response by November 21, 2003. On November 25, 2003, TSA provided a response to the CPO. Both the CPO and TSA employees said that the response consisted of hundreds of pages of materials. In a February 16, 2004, e-mail, the TSA employee who coordinated the response to this request said that he worked with the Policy Office, the FOIA office, and the CIO's office to collect materials for the CPO.

5. On January 20, 2004, the CPO sent an e-mail to TSA's FOIA officer asking for TSA documents from a 2002 FOIA request about Northwest

Airlines. There was one document responsive to this request and on January 20, 2004, the FOIA officer offered to either fax or hand-deliver it to the CPO.

6. On February 13, 2004, the CPO sent a request to TSA's FOIA officer asking for all documents gathered for FOIA requests related to JetBlue.[73] In the documents we reviewed relating to this request, we found no direct response.

7. On February 16, 2004, the CPO sent a follow-up request to TSA's FOIA officer asking for all documents gathered for FOIA requests. The CPO told us that the FOIA office provided documents in February 2004 and that the FOIA office was very responsive to requests for information.

8. On January 29, 2004, the former CAPPS II program manager sent a letter to the Army OIG and copied TSA's OCC. The letter addressed several of the Army OIG's questions pertaining to their investigation of the transfer of JetBlue PNR data to Torch Concepts. On February 16, 2004, the CPO requested OCC provide the letter and on February 17, 2004, TSA's chief counsel faxed it to the CPO.

[73] The Electronic Privacy Information Center, the ACLU, and Wired News made FOIA requests in September and October 2003. The FOIA requests generally asked for materials related to JetBlue, DOD subcontractor Torch Concepts, Acxiom Corporation, and DOD contractor SRS Technologies. The FOIA documents were later turned over to the DHS Privacy Office.

Carlton Mann, Chief Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Kenneth McKune, Senior Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Frank Parrott, Senior Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Justin H. Brown, Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Patrick Harenburg, Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Department of Homeland Security

Secretary
Deputy Secretary
Under Secretary for Border and Transportation Security
Under Secretary for Management
Director, United States Secret Service
General Counsel
Assistant Secretary for Public Affairs
Chief of Staff
Chief Privacy Officer
Deputy Chief Security Officer
Management OIG Liaison

Transportation Security Administration

Assistant Secretary of Homeland Security for Transportation Security
OIG Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Program Examiner

Congress

Committee on Homeland Security and Governmental Affairs
United States Senate

Committee on the Judiciary
United States Senate

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528, or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.