U.S. ARMY INSPECTOR GENERAL AGENCY
REPORT OF INVESTIGATION (ROI)
(ROI 04-007)

21 JUN 2004

SUBJECT: Release of personal information related to a security enhancement study for Army installations and facilities contracted for by the Office of the Deputy Assistant Secretary of the Army (Research and Technology) (ODASA (R&T})

1. AUTHORITY: On 24 November 2003, the Acting Secretary of the Army directed the Department of the Army Inspector General Agency (DAIG) to conduct an investigation to determine the facts and circumstances surrounding the alleged release of personal information related to a security enhancement study for Army installations and facilities contracted for by the ODASA (R&T). (EXHIBIT A)

2. BACKGROUND:

a. In April 2002, the ODASA (R&T) awarded a task order (TO) for a security enhancement study to Torch Concepts [hereinafter Torch], a subcontractor of SRS Technologies. The OOASA (R&T) utilized an existing contract with SRS Technologies to subcontract with Torch to conduct a security enhancement study for Army installations and facilities. The strategy for the Torch study was to test their proprietary ACUMEN algorithm on a timely, relevant, representative database to assess the algorithm's potential application to the evaluation of data collected from persons seeking entry to Army bases, in an effort to improve security at such locations. Torch proposed the use of airline passenger data in order to test the ability of the algorithm to screen real world data. The study examined whether the ACUMEN technology could differentiate between passengers who required enhanced security screening and those who did not, by employing the ACUMEN machine-learning algorithm to identify passenger deviations from the "norm."

b. On 10 October 2003, Senator Patrick Leahy forwarded a letter to the Secretary of Defense (SECDEF) requesting answers to specific questions regarding potential violations of the Privacy Act associated with the alleged release of JetBlue Airlines customer data by the Department of Defense (DOD). (EXHIBIT B-1)

c. On 17 October 2003, the Senate Committee on Governmental Affairs forwarded a letter to the SECDEF requesting answers to specific questions regarding potential violations of the" Privacy Act associated with the alleged release of JetBlue Airlines customer data by the DOD. '(EXHIBIT B-2)

3. SYNOPSIS OF THE FINDINGS:

a. The evidence indicated that Torch neither created nor maintained a system of records as defined by the Privacy Act of 1974 with regard to the JetBlue passenger name record (PNR) and Acxiom demographics databases. The Privacy Act of 1974 defines a "system of records" as 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. There was no evidence that Torch retrieved information from the databases discussed above by name or by any other identifying particular assigned to an individual. Names were eliminated as soon as practicable and social security numbers (SSNs) were deleted with the exception of the fourth and fifth digits. The software required grouping the records to analyze the data. [redacted]

b. The study data records were maintained on one internal computer system that was accessible to only one Torch employee. In addition, reports and briefing slides on the program findings were prepared for the Army and controlled by the chief executive officer's (CEO's) office. On 4 April 2003, Torch presented a *Homeland Security - Airline Passenger Risk Assessment* briefing at the Homeland Security Session of the_____ Southeastern Software Engineering Conference.

[redacted]

Unfortunately the <redacted> communications were either unclear or were misinterpreted and, in preparing for the briefing, the Torch presenter inadvertently removed the wrong briefing/data from the office. Slide 20 of the Torch briefing presented at the Southeastern Software Engineering Conference depicted demographic information. The data on this slide included multiple addresses and multiple SSNs, with a common date of birth for passengers whose identities were never further ascertained. The [redacted] The composition of the slide supported Torch's testimony as the slide did not indicate that Torch retrieved records by identifying particulars assigned to an individual. The only common data element on this'slide was the date of birth. The only circumstance in which it appeared that Torch disclosed potentially personal information was this presentation. Torch displayed the slide in an effort to explain to Conference attendees the confusion and inherent errors involved in a real world database employed in the study and to demonstrate the types of records that had been discarded before applying the ACUMEN algorithm. Because the information disclosed was not derived from a Privacy

Act system of records, the disclosure was not a violation of the Privacy Act; however, the disclosure violated provisions of Torch's subcontract with SRS Technologies. Specifically, the contract provided that the subcontractor would not disclose information concerning work under this subcontract to any third party, unless such disclosure was necessary for the performance of the subcontract effort. The Torch presentation at the Southeastern Software Engineering Conference was not part of the subcontract performance.

c. The information on the slide Torch presented at the Southeastern Software Engineering Conference on 4 April 2003 w^as the same information that it provided to the Army in a study update on 30 August 2003, except that the Army study update slide also included the names associated with the other passenger data depicted on the 4 April 2003 slide. The only data point common to all passenger information reflected on the slide was date of birth. Because the 30 August 2003 slide contained multiple names of passengers and multiple SSNs, there was no evidence the records were retrieved by any identifying particular assigned to an individual. That Torch used briefing slides to update the Army on the status of performance under the Task Order corroborates the statement by Torch that in preparing for the Southeastern Software Engineering Conference, the individual presenter inadvertently removed the wrong briefing, one that had been intended for an internal Army audience, from the <redacted> office.

d. The Army did not authorize Torch to use the JetBlue customer data for the 4 April 2003 briefing at the Homeland Security Session of the Southeastern Software Engineering Conference or for any other purpose unrelated to the military base security study. The Army was not aware of the presentation's existence until 12 September 2003. Prior to that date the Army had no knowledge of the presentation's contents and was not aware that any potentially personal information was disclosed in a public forum.

Abbreviations, Acronyms, and Definitions used in this ROI

ACUMEN
Advanced Pattern Recognition Software

CAPPS II
Computer Assisted Passenger Pre-Screening System

COTR
Contracting Officer Technical Representative

DA
Department of the Army

DAIG
Department of the Army Inspector General

DD Form DOD
Form

DFARS
DOD FAR Supplement

DOD
Department of Defense

DOT
Department of Transportation

CY Calendar Year

FAR
Federal Acquisition Regulations

FOIA
Freedom of Information Act

FOUO
For Official Use Only ,

ftp
File Transfer Protocol

FY
Fiscal Year

IAW
In Accordance With

IO
Investigating Officer

LTC
Lieutenant Colonel

ODASA (R&T)
Office of the Deputy Assistant Secretary of the Army (Research and Technology)

OGC
Office of the General Counsel

PGP
Encryption Program

PM
Program Manager

PNR
Passenger Name Record

ROI
Report of Investigation

SECDEF Secretary of
Defense

SRS Technologies
Contractor

SSN
Social Security Number ,

SAIG-IN(20-1b)

TIA
Total Information Awareness

TSA
Transportation Security Administration

SA!G-IN(20-1b)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

ROI Personnel List

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

SAIG-IN(20-1b)

1. STANDARD: The Privacy Act of 1974, U.S. Code, Title 5, Section 552a, Records Maintained on Individuals, provided in relevant part:

a. A "system of records" was a group of any records under the control of any agency from which information was retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

b. No agency could disclose any record which was contained in a system of records by any means of communication to any pe/son, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertained, unless disclosure of the record would be to a recipient who had provided the agency with advance adequate written assurance that the record would be used solely as a statistical research or reporting record, and the record was to be transferred in a form that was not individually identifiable.

c. Each agency that maintained a system of records would, at least 30 days prior to publication of information, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and if such agency was a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision. (EXHIBIT C)

2. DOCUMENTS:

a. An unsigned Subcontract Agreement between SRS Technologies, Inc. and Torch, dated 12 December 2001, reflected the terms of the subcontract.

(1) Section 24.0 (page 15) stated no news release (including photographs and films, public announcements or denial/confirmation of the same) on any part of the subject matter of this subcontract or any phase of any program hereunder would be made without the prior written approval of the SRS Program Manager. The subcontractor would not disclose information concerning work under this subcontract to any third party, .unless such disclosure was necessary for the performance of the subcontract effort. The restrictions of this paragraph would continue in effect upon completion or the parties could mutually agree upon termination of this subcontract for such period of time as in writing. In the absence of a written established period, no disclosure was authorized. Failure to comply with the provisions of this clause could be cause for termination of this subcontract.

(2) Part 2.0 (page 19), Government Provisions, reflected the following clauses set forth in the FAR and the DFARS, in effect on 1 July 1999, were incorporated herein by reference with the same force and effect as if given in full text. Subcontractor hereby agreed to flow-down the applicable FAR/DFARS clauses to its lower-tier subcontractor. FAR clauses applicable to the TO included Privacy Act notification and the Privacy Act.

(3) Attachment 1 (page 26) explained the description of work to be performed. The description stated military and government ground facilities were undoubtedly potential terrorist targets. Timely identifications of abnormal events or activities as they occur offered the potential to immediately intercept terrorist activities and avoid their damaging consequences. Today, data was collected from many different sources. However, even though the data was available, identification of the events that lead to terrorist activities were often not discovered until after the fact. Many of the algorithms, which had been developed over the years, offered potential application to these problems. The contractor would assess existing data collection and data analysis algorithms for their potential ability to identify and/or predict terrorist activities in a timely manner. In order to prove this potential ability, the contractor would test existing algorithms against one or two data collections. Tests would be focused on data from the September 11 terrorist incident assuming said data was available. The contractor would assess the potential of using machine-learning algorithms to discover patterns and apply high-speed pattern matching tools to identify hidden relationships and behaviors. The contractor would then analyze and review significant patterns in the data that could be a signal of terrorist activities.

(4) Attachment 2 (page 28) explained the organizational conflict of interest certification. The certification stated when access to proprietary information of other companies was required, the subcontractor would enter into a written agreement with the other company(ies) to protect their proprietary information from unauthorized use or disclosure for as long as it remained proprietary; and refrain from using such proprietary information for any purpose other than providing advisory and assistance service to the Government under this contract. (EXHIBIT D-1)

b. TO 02-2037, dated 21 February 2002, reflected the general task and level of effort for the contract.

(1) The general Task Description stated "As a consequence of the 9-11 terrorist attacks on this Nation, the Deputy Assistant Secretary of the Army for Research and Technology (DAS(R&T)) changed the focus of his program to place additional focus on Counter Terrorism. In particular DAS(R&T) has directed that Torch conduct an experiment with their proprietary software, ACUMEN, to evaluate its potential for identifying future terrorist attacks. The general approach will be to abstract appropriate

pre-attack data based for consumption by ACUMEN to determine if its product is sufficiently robust to have predicted the attacks of 11 September 2001."

(2) The Technical Support section stated the contractor would access appropriate databases such as those residing at Los Alamos National Laboratories, and the Federal Bureau of Investigation (Integrated Intelligence Application DataBase, the Multi domain Expert Systems, and the Telephone Analysis System).

(3) The ODASA (R&T) would provide the contractor with information required to perform the tasks articulated and would facilitate the interface of contractor personnel with other Army staff offices as required to complete the effort. (EXHIBIT D-2)

c. A memorandum, dated 26 March 2002, subject: Technical Monitor Appointment, Contract DASG62-99--d-0005 TO 02-2037, reflected that <redacted> was appointed as the <redacted> (EXHIBIT D-3)

d. A Torch briefing, *Terrorist Identification ACUMEN - An Advanced Methodology and Technology to Flag Potential Terrorist Actions,* dated 27 March 2002, reflected the proposal that Torch initially presented to ODASA (R&T) for consideration of a contract. The proof of principle included a test of airline passenger screening data where passengers would be checked against "normal" travel modes. The data input included passenger ticketing information. The data output identified whether a passenger fit a given "normal" model or the passenger was an anomaly who may require enhanced security screening . (EXHIBIT D-4)

e. A Torch *Introduction Briefing,* dated 3 April 2002, reflected the program objectives and background of the ACUMEN technology. The briefing identified ACUMEN as a proactive expert system that could handle a million ticketing transactions per day to identify potential terrorists by identifying deviations from normal passenger behavior. Proof-of-principle funding was available and work had been done with National Lab to validate the potential of the system. (EXHIBIT D-5)

f. A DD Form 448, Military Interdepartmental Purchase Request, dated 4 April 2002, reflected that the U.S. Army Research Laboratory approved funding for Contract DASG62-99-D-0005/TO 02-2037 to be performed by Torch. The estimated total price was $250,000. .'(EXHIBIT D-6)

g. An incomplete draft Information Paper, dated 8 April 2002, subject: Terrorist Identification Program, reflected the ODASA (R&T) draft response to a potential FY03 Congressional add-on, which included a $6.0 million cost, which supported the ACUMEN program. (EXHIBIT D-7)

h. A DD Form 1155, Order for Supplies or Services, dated 12 April 2002, reflected the award of the TO 02-2037 to SRS Technologies. It was through this TO that SRS Technologies subcontracted with Torch to conduct the study. (EXHIBIT D-8)

i. A Confidentially Agreement between Torch and Acxiom, dated 25 April 2002, reflected each party agreed to hold the other's confidential information in strict confidence and not to disclose such information to any third party or to use it for any purpose other than as specifically authorized by the other party. Each party agreed that it would employ all reasonable steps to protect the confidential information of the other party from unauthorized or inadvertent disclosure, including without limitation all steps that it took to protect its own information that it considered proprietary. The parties could disclose each other's confidential information only to those employees having a need to know and only to the extent necessary to enable the parties to adequately perform their respective responsibilities to each other and, in the case of any product tests, only to those of its employees who were directly involved with the testing of such product. (EXHIBIT D-9)

[IO Note: Acxiom, Inc. was a commercial database management company, and the PNR database manager for JetBlue Airlines.]

j. An e-mail, dated 26 April 2002, subject: Assistance with Acquiring Airline Passenger Data, reflected Torch's request for assistance from ODASA (R&T) to obtain airline data from TSA. Because the data was similar to that collected from persons seeking entry to Army bases, airline data was deemed suitable for use in conducting the proof-of-principle study to validate ACUMEN technology. (EXHIBIT D-10)

k. An undated table reflected the passenger data elements that Torch requested from TSA. (EXHIBIT D-11)

l. An undated table reflected elements of both the JetBlue PNR data and the commercially available Acxiom demographics data Torch used in the study. (EXHIBIT D-12)

m. Torch news release, dated 8 May 2002, subject: Torch, Inc. Wins Contract to Develop Technologies to Identify Terrorists Threats, reflected the announcement that Torch would petform a security enhancement study for the Army, using its ACUMEN technology. The ACUMEN technology used advanced pattern recognition algorithms to identify abnormal behaviors hidden in large blocks of data. (EXHIBIT D-13)

n. A hand-written note, dated 5 June 2002, subject: Meeting with TSA/DOT, by <redacted> reflected discussjons that took place on now to obtain airline passenger data from TSA. <redacted> that it should not be a problem to provide access to the data as long as there were not issues with ISA's acquisition process on CAPPS II, currently under a separate procurement process. Follow-on actions required an agreement between ISA and DA, checking with legal, and ensuring the data type obtained would be the data needed to meet requirements of the Torch study. (EXHIBIT D-14)

o. An e-mail, dated 12 June 2002, with an enclosed memorandum, subject: Inputs for TSA Agreement, dated 7 June 2002, from <redacted> reflected the following ACUMEN Project details:

• <

(1) Program Scope Considerations (enhance security of military facilities)

(2) Proof-of-Principle Demonstration (large amount of ground truth data such as an airline database)

(3) Data Element Requirements (passenger, reservation, billing, check-in)

(4) Data Volume Requirements (two to three years worth of data) (EXHIBIT D-15)

p. A hand-written note, dated 14 June 2002, subject: Meeting with TSA/DOT, by <redacted> continued discussions on how to obtain airline passenger data via TSA. In order to obtain access to the data, permission was required from all the participating airlines that contributed to the PNR database. Follow-on actions included providing non-disclosure agreements to Torch, with <redacted> coordinating with <redacted> for for agency-to-agency requirements. <redaacted> assured <redacted> that the process was not difficult and would not be a problem. (EXHIBIT D-16)

q. A Torch briefing, *Homeland Security - Airline Passenger Risk Assessment,* dated 25 February 2003, reflected the information that was presented at the Homeland Security Session of the Southeastern Software Engineering Conference on 4 April 2003.

(1) The.objectives of the study were to demonstrate that airline passenger data and reservation data could be clustered to form groups of "conventional" travelers; to characterize each group of travelers; and to show how this type of characterization, when extended to a more complete and representative database, could be used to identify high-risk passengers requiring enhanced security screening.

(2) Slide 19 reflected the passenger demographics that were modeled in the study. The records were categorized into two groups and SSNs were depicted by only two digits. >

(3) Slide 20 reflected demographic information for unnamed passengers. The data included multiple addresses and multiple SSNs. The only characteristic common to all entries was the date of birth. (EXHIBIT D-17)

r. An und ated Torch briefing, *The Security Enhancement Study,* reflected what the<redacted> presented to the Army in CY02 and CY03 in updating the status of the study. The briefing provided a general overview of the study; however, there were no slides containing passenger records or data. (EXHIBIT D-18)

s. In a memorandum dated 30 July 2002, subject: Reguest for PNR Data for a DOD Proof of Concept,<redacted> made a request to the <redacted>. The memorandum referenced a prior discussion and noted that DOD was involved in a proof of concept program for the purposes of improving military base security. DOD engaged the TSA to assist in securing of PNR data required to assess the concept. For this reason, TSA requested the use of archived PNR data belonging to JetBlue. TSA requested that Acxiom, the contractor who managed JetBlue passenger data provide the PNR data to Torch. The memorandum reflected that any nondisclosure agreements that needed to be executed could be exchanged directly between the parties with copies provided to both DOD and TSA. (EXHIBIT D-27)

9

t. A Torch Final Report, A Feasibility Study on Security Enhancement, dated 30 August 2003, documented the draft findings of the study.

(1) Page 62 reflected anomalous information for passengers. The data included different names, multiple addresses, and multiple SSNs. The only characteristic common to all entries was the date of birth.

(2) Page 63 reflected information as to how certain SSN digits corresponded to *a* person's age.

(3) Pages 67-70 reflected demographic data on six of the eleven terrorists involved in the September2001 airline hijackings. (EXHIBIT D-19)

[IO Note: This Version was the first draft Torch presented to ODASA (R&T).]

u. A Torch Final Report, A Feasibility Study on Security Enhancement, dated 30 August 2003, documented the draft findings of the study. (EXHIBIT D-20)

SAIG-IN(20-1b)

[IO Note: This version was the third draft Torch presented to ODASA (F &T). The second draft

to the issues addressed.]

v. A fax from <redacted> dated 22 September 2003, to <redacted> reflected a packet of e-mails dated between 8 -17 Oct 2002 between Torch, ODASA (R&T), and TSA personnel on privacy issues related to the CAPPS II program. The packet also included a draft DOT Privacy Impact Assessment used by the IRS. (EXHIBIT D-21)

w. An e-mail, dated 30 September 20Q3, from <redacted> to <redacted> reflected that the JetBlue reservation data and the Acxiom demographics data had been treated as FOUO documents at all times. The data was transferred electronically as PGP-encrypted files. During analysis, the data was on a file system that was isolated from the Internet. Access to the machine was limited by password to the single analyst involved. All hardcopy outputs were shredded. No backups of the source data were ever performed during the course of the analysis; and, when the project was completed the data was backed up and deleted from the file system. The media produced were stored in a locked fire-proof safe. The machine employed in the analysis used the Linux operating system, which was very secure relative to the retrieval of deleted files. All backup media were recently destroyed. (EXHIBIT D-22)

[IO Note: PGP was a commercial company that provided encryption software used to encrypt computer files.]

x. An email, dated 2 October 2003, subject:Fact Paper -17 September 2003, from<redacted> to <redacted> reflected a request for additional

information to address privacy issue questions raised by <redacted> indicated he would have to get approval from <redacted> to release any further information, as <redacted> was not aware that <redacted> had approved the 17 September 2003 fact paper for release. (EXHIBIT D-23)

y. A memorandum, dated 2 October 2003, subject: JETBLUE/Torch, by[reflected the events of the past year regarding the use/purchase of the Acxiom demographics.database and extending the contract completion date to March 2003. The packet also contained two documents, dated 11 and 19 September 2002, which supported the timeline discussed in the main document. These documents reflected the use of the Acxiom database and extension of the contract completion date with no cost increase. The Torch PM of the Security Enhancement Study acknowledged that he made the decision to purchase the Acxiom database and understood that Torch might have to absorb the cost if the Army did not approve the purchase. (EXHIBIT D-24)

z. A Torch Final Report, A Feasibility Study on Security Enhancement, dated 15 December 2003, documented the findings of the study. (EXHIBIT D-25)

[10 Note: This version was the final product Torch presented to ODASA (R&T).]

aa. Invoice Number FY03-11532, dated 30 July 2003, reflected $250,519.95 as the cumulative amount billed to date for TO 02-2037. (EXHIBIT D-26)

3. TESTIMONY:

[redacted]

SAIG-IN(20-1b)

(b)(7)(C)

[redacted]

(b)(7)(D)

(b)(7)(D)

[IO Note: Although the presentation was dated 25 February 2003, the presentation date at the symposium was 4 April 2003.] ^

(b)(7)(C)

SAIG-IN(20-1b) Note pps 21-24 all redacted

SAIG-IN (20-1 b)

(b)(7)(D)

SAIG-IN(20-1b)

(b)(7)(D)

[redacted]

(b)(7)(D)

[redacted]

[IO Note: Structured Query Language (MySQL) was the world's most popular open source database management system. RDBMS was a relational database management system that stored data in the form of related tables. It was a program that allowed an individual to create, update, and administer a relational database. A relational database was a collection of data items, organized as a set of formally-described tables from which data could be accessed or reassembled in many different ways without having to reorganize the database tables. The standard user and application program interface to a relational database was the SQL.]

(b)(7)(D) [redacted]

[IO Note: Levenshtein distance was named after a Russian scientist who devised an algorithm in 1965 to measure the similarity between two strings of data. Levenshtein distance was a measure of the similarity between two strings, which were referred to as the source string (s) and the target string (t). The distance was the number of deletions, insertions, or substitutions required to transform s into t. The Levenshtein distance algorithm had been used in spell checking, speech recognition, DMA analysis, and plagiarism detection.]

(b)(7)(C) [redacted]

SAIG-IN(20-1b)

[redacted]

[redacted]

[IO Note: The reference to DOD was the ODASA (R&T).]

[redacted]

DISCUSSION:

a. On 12 April 2002, the ODASA (R&T) awarded Torch a TO to an existing Army contract. The TO was for Torch to conduct a security enhancement study for Army installations and facilities for a one year period for a total price of $250,000. At the request of Torch, the Army granted a no cost extension through 3 May 2003. As of 30 July 2003, $250,519.95 had been billed to the Government for Torch's expenditures under the TO.

b. The strategy for the Torch study was to test Torch's proprietary ACUMEN algorithm on a timely, relevant, representative database to assess the algorithm's potential application to the evaluation of data typically collected from persons seeking entry to Army bases, in an effort to improve security at such locations. To accomplish this research goal and assess the algorithm for potential application to Army security functions, Torch needed an actual database with realistic features, such as certain categories of data, errors and inaccuracies. Given the nature of an airline PNR database, Torch decided that using such a representative database was a relevant and reasonable approach for testing and assessing the potential utility of their algorithm.

c. In Spring of 2002, Torch, an Alabama-based company, contacted two airlines (Delta and American), the Department of Transportation, Alabama's Senator Sessions and Congressman Cramer, all in an attempt to obtain PNR data. By April 2002, Torch had not succeeded in obtaining any data. Torch then requested ODASA (R&T) assistance in obtaining PNR data. The ODASA (R&T) needed *a* facilitator to seek approval from an airline for release of its PNR data. Airlines had expressed concerns about releasing PNR data based solely on a request from the DOD. Because TSA was involved with airline security matters, the ODASA (R&T) requested assistance from TSA in facilitating Torch's access to PNR airline data. The ODASA (R&T) contacted TSA and facilitated the discussions between Torch and TSA. On 30 July 2002, the TSA agreed to support the Army request and forwarded a request to JetBlue for its PNR data.

d. In September 2002, JetBlue authorized Acxiom, Inc., JetBlue's PNR data management contractor, to release JetBlue PNR data to Torch. Torch received approximately 5 million JetBlue PNR records associated with 2.2 million JetBlue passengers from Acxiom. The Torch study approach required a data element that would provide a measure of passenger stability. When Torch determined that the JetBlue PNR data did not provide the necessary level of detail for the ACUMEN algorithm to discern normal passenger travel modes, Torch sought to obtain demographics data for the JetBlue passengers. To this end, Torch purchased a separate commercially available demographic database from Acxiom for the passengers for whom they had received JetBlue PNR data. The Acxiom demographics database contained additional information on the JetBlue passengers such as home ownership, length of residency, salary, *etc.* The evidence indicated that Torch chose to purchase the demographics data from Acxiom because Acxiom could provide matching demographic records matching the JetBlue PNR data. The ODASA (R&T) did not authorize additional funds for the contract for Torch's purchase of the demographics data.

e. Torch used a sophisticated computer matching process to merge the JetBlue PNR database and the commercially available Acxiom demographics database. Acxiom assigned a number sequence *to each record and provided the number sequence to Torch to facilitate the computer matching of the PNR and demographics databases. The evidence indicated the records were first merged by Acxiom.

[redacted]

Together, the merged databases constituted a database of sufficient detail to properly test the algorithm. There was no evidence that Torch ever retrieved a record by name, SSN, unique identifying particular assigned to an individual, or other key feature;, either before or after the data was merged.

[redacted]

and model a process to identify potential high-risk passengers. The results of the algorithm were verified using the merged database and statistical characteristics known about the actual 9-11 terrorists. There was no evidence the verification process required any retrieval by name, SSN, or any other unique identifying particular assigned to an individual.

f. Torch considered two groups of criteria in modeling the representative "normal" passenger record: PNR flight information and demographic information. The differentiating factors used to indicate a lesser or greater degree of deviation [and a corresponding lesser or greater degree of risk] from the characteristics commonly associated with the "normal" passenger record were:

[redacted]

Given the data input and the enumerated risk factors, the ACUMEN algorithm identified only 1 percent of the total 873,000 records modeled as requiring enhanced security screening; the remaining 99 percent of records were assessed as "normal," requiring some appropriate baseline level of security screening. To verify these findings, Torch analyzed statistical information known about the actual September 11 hijackers using the ACUMEN-generated model.

[redacted]

The ACUMEN algorithm identified 83% of the September 11 terrorist records as high-risk deviations from the "normal" passenger record pattern, requiring enhanced security screening. According to Torch, the identification of three "high-risk" passengers on a single flight would have lead to that flight's detention in the airport of origin. Accordingly, application of the ACUMEN algorithm to the September 11 flights yielded a 96% probability that at least one of the four hijacked aircraft would have been detained at its airport of origin pending enhanced security screening of passenger records later determined as belonging to the terrorists. There was no evidence that the verification process required the retrieval of any passenger record by name, SSN, or any other unique identifying particular assigned to an individual.

g. The JetBlue PNR and the Acxiom demographics databases on the JetBlue customers were entrusted to a single Torch individual. No one else had access to the data. Torch received the PNR and demographics data as a PGP encrypted file and Torch later decrypted the data. The databases were restricted to a computer system isolated in one room with no connection to either the Internet or an Intranet. Torch handled the JetBlue data as FOUO. Later, at the request of both JetBlue and Acxiom and pursuant to the data disclosure agreement between Torch and Acxiom, Torch attempted to destroy the PNR data, the demographics data, and the merged databases on their computer by overwriting the records with Os and 1s. JetBlue later audited the computer and discovered that some of the data had not been fully destroyed. Torch advised the COTR that due to pending civil litigation, they were unable to complete the destruction of the data. The computer containing the information was bagged and sealed by a JetBlue representative and currently resides in a secure safe in the offices of Torch attorneys.

h. There was no evidence that Torch attempted to merge or merged any database, other than the Acxiom commercially available database, with that of JetBlue. The purpose of the JetBlue PNR and Acxiom demographics data merger was to obtain a database with the level of detail necessary to complete the study. Additionally, there was no evidence that either of the databases were CAPPS II databases, or databases developed for possible use in CAPPS II or related programs. The Army is unaware of any plans to use the analysis of JetBlue's or any other airlines' customer data for any purposes related to TSA's CAPPS II program. There was no evidence the Army planned to use or used analysis of JetBlue's or any other airlines' customer data for any purposes relateci to the now discontinued TIA Program.

i. The evidence indicated that Torch neither created nor maintained a system of records as defined by the Privacy Act of 1974 with regard to the JetBlue PNR and Acxiom demographics databases. The Privacy Act of 1974 defines a "system of records" as 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. There was no evidence that Torch retrieved individual records from the databases discussed above by name or by any other identifying particular assigned to an individual at any time in the course of the study. Names were eliminated as soon as practicable and SSNs were deleted with the exception of the fourth and fifth digits. The software required grouping the records to analyze the data. Parameters were established to separate passenger data into groups, based upon certain criteria, *e.g.* short-trippers, short-notice travelers, high-spenders, *etc.* Once the records were grouped by category, Torch uitilized the ACUMEN software to screen the records against criteria,

This screening separated records into potential high- or low-risk categories. The evaluation of the ability of the algorithm to effect this screening was the purpose of this project and its potential future application to Army installation security.

j. As stated above, the data records were maintained on one internal computer system that was accessible to only one Torch employee. In addition, reports onthe program findings were periodically prepared for the Army and controlled by thef office. On 4 April 2003, Torch presented a *Homeland Security - Airline Passenger Risk Assessment* briefing at the_Homeland Securitv Session of the Southeastern Software Engineering Conference. [redacted] Unfortunately the [redacted] communications were either unclear or were misinterpreted and, in preparing for the briefing, the individual presenter inadvertently removed the wrong briefing from the

Slide 20 of the Torch 4 April 2003 briefing reflected demographic information. The data included multiple addresses and multiple SSNs, but the same date of birth for passenqers whose identities were never further ascertained. [redacted] The composition of the slide supported this testimony as the slide did not indicate that Torch retrieved records by an identifying particular assigned to an individual. The only common data element on this slide was the date of birth. The only circumstance in which it appeared that Torch disclosed potentially personal information was this presentation. Torch displayed the slide in an effort to explain to Conference attendees the confusion and inherent errors involved in a real world database employed in the study and to demonstrate the types of records that had been discarded before applying the ACUMEN algorithm. Because the information disclosed was not derived from a Privacy Act system of records, the disclosure was not a violation of the Privacy Act; however, the disclosure violated provisions of Torch's subcontract with SRS Technologies. Specifically, the contract provided that the subcontractor would not disclose information concerning work under the subcontract to any third party, unless such disclosure was necessary for the performance of the subcontract effort. The Torch presentation at the Southeastern Software Engineering Conference by Torch was not part of subcontract performance.

k. The information on the slide Torch presented at the Southeastern Software Engineering Conference on 4 April 2003 was the same information that it provided to the Army in a study update on 30 August 2003, except that the Army study update slide also included the names associated with the other passenger data. The only data point common to all passenger information reflected on the slide was date of birth. Because the 30 August 2003 slide contained multiple names of passengers and multiple SSNs, there was no evidence the records were retrieved by any identifying particular assigned to an individual. The existence of the 30 August 2003 slide, intended for an internal Army audience, and Torch's practice of using briefing slides for its updates to the Army corroborate the statement by Torch that the individual Torch presenter inadvertently removed the wrong briefing from the <redacted> office.

l. The Army did not authorize Torch to use the JetBlue customer data for the 4 April 2003 briefing at the Homeland Security Session of the Southeastern Software Engineering Conference or for any other purpose unrelated to the military base security study. The Army was not aware of the presentation's existence until 12 September 2003. Prior to that date, the Army had no knowledge of the presentation's contents and was not aware that any potentially personal information was disclosed in a public forum.

5. CONCLUSIONS:

a. There was no violation of the Privacy Act associated with the alleged release of personal information related to a security enhancement study for Army installations and facilities.

b. Torch violated the provisions of its subcontract with SRS Technologies by presenting information at the Southeastern Software Engineering Conference. The presentation was not part of the performance of the subcontract effort.

6. RECOMMENDATIONS:

a. This report be approved and the case closed.

b. Refer the matter that Torch violated the provisions of its subcontract with SRS Technologies to the ASA (AL&T) for appropriate action.

b. Respond to the Congressional Inquiries.

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

R. L. Brownlee

F

/ L. BROWNLEE Acting
Secretary of the Army