Terrorist Identification

ACUMEN – An Advanced Methodology and Technology to Flag Potential Terrorist Actions

May 3, 2002
Roy Nichols
Torch Concepts, Inc.
Torch Concepts Corporate Overview

- Small Business – focused on products and services
- Incorporated in 2000
- Two Locations
  - Huntsville, Alabama – Corporate Headquarters
  - Boston, Massachusetts
- Highly Skilled Technical Expertise
- Strong Intellectual Property
- Seasoned Responsive Executive Management Team
- Exceptional Past Performance
ACUMEN Is A Mature Technology
- Applied Successfully to a Variety of Problems -

- Resource Allocation & Sensor Fusion
- Search & Rescue with Synthetic Aperture Radar
- Unmanned Vehicle Control
- Data Classification, Archival Retrieval, & Compression
- Automatic Target Recognition Algorithm Development & Evaluation
- Medical Image Diagnostics
- Financial Data Analysis & Prediction
- Airborne Target Detection & Classification for Drug Interdiction
- Fingerprint Identification
- Health Care Data Mining Applications
- Submarine Tracking & Classification
- Missile Attack Warning

April 30, 2003
Employing Transactions Across Broad Spectrum
- Deviations From Normal Behavior Point To Terrorists -

Deviations Represent Suspect Actions or Flags!

Transportation Transactions
Investment Transactions
Biochemical Transactions

Shipping  Airlines  Trucking

Traveling  Licensing

Federal
State
Local
International

DIA
CIA
FBI
INS
FAA
Data Bases

April 10, 2002
Prove the Concept for Airline Ticketing Transactions
- The Risk Assessment Process -

I. The Reservation

II. The Payment $$$

III. Pre-Flight Airline Check (based on risk)

IV. Passenger Check-In and Security Checks

Search, Detain, or Pass Through

Consolidate with Other Transactions

April 10, 2002
The "Terrorist Flagging" Program
- Phased Approach to Block 1 Development -

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase I</td>
<td>&quot;Terrorist flagging&quot; proof of principle (2 to 3 months)</td>
</tr>
<tr>
<td></td>
<td>- Identify and develop data base (adequate for POP demonstration) by working with domain experts</td>
</tr>
<tr>
<td></td>
<td>- Demonstrate that logic identifies important terrorist actions and other factors</td>
</tr>
</tbody>
</table>

| Phase II | Develop Block I logic for "flagging terrorists" |
|          | - Identify and develop comprehensive data base |
|          | - Develop Block I "terrorist flagging" logic and demonstrate daily operation (a minimum of one interaction with experts) |

| Phase III | Develop and demonstrate Block I "terrorist flagging" software |
|           | - Develop "terrorist flagging" software |
|           | - Demonstrate daily operation |
Phase 1 - POP

Step 1: Data Acquisition
Step 2: Data Preparation
Step 3: Identification of Key Features
Step 4: POP Model Development
Step 5: Iterative Data Analysis
Step 6: Demonstration/Presentation
Torch Concepts Corporate Overview

- Small Business - focused on products and services
- Incorporated in 2000
  - Huntsville, Alabama - Corporate Headquarters
  - Boston, Massachusetts
- Highly Skilled Technical Expertise
- Strong Intellectual Property
- Seasoned Responsive Executive Management Team
- Exceptional Past Performance
- High Level Government Security Clearances

June 4, 2002
ACUMEN Determines Unique Patterns In Data
This Mature Technology Has Been Applied to Many Problems
Counter Terrorism Initiative -

Breaking the Knowledge Barrier
Security Enhancement Program Objective

Develop Logic and Software Capable of Identifying Potential Terrorist Actions by Detecting Those Actions Which Are Outside the Norm of Daily Activity. Assist Security Experts (1) By Flagging Potential Terrorist Actions, and (2) In Identifying Necessary Data and Operational Steps to Enhance Security.
Employing Transactions Across Broad Spectrum

Deviations Represent Suspect Actions or Flags!

Transportation Transactions
Facility Visits
Biochemical Transactions

Shipping
Airlines
Trucking

People and Products

Licensing
Federal
State
Local
International

DIA
CIA
FBI
INS
FAA
Data Bases

Find a "Needle in a haystack"
without knowing what the needle looks like!

June 4, 2002

Breaking the Knowledge Barrier
The Demonstration Approach
For Security Enhancement of Military Facilities

- Conduct a Proof-of-Principle Demonstration which extracts potential terrorist action from a large complex data base, preferably relying on ground truth to verify capability.

- Address an application where ground truth is available; e.g.,
  - Airline passenger screening to identify risk level
  - INS database screening to identify suspect patterns
Proof-of-Principle Demonstration  
- Risk Assessment for Passenger Screening -

**The Travel Process**

1. The Reservation
   - Compare Individual Reservations to Travel Models

2. The Payment
   - Compare All Passengers on Flight to Travel Models
   - Compute Payment to Models
   - $\$\$

3. Pre-Flight Airline Check (based on risk)
4. Passenger Check-In and Security Checks

**The Airline**

- Flight Ticketing
- Travel Models (A, B, C, ..., N)
- Flight Data Bases (From CIA, FBI, INS, FAA)
- Search, Detain, or Pass Through

Consolidate with Other Transactions

---

June 4, 2002

Breaking the Knowledge Barrier
The Security Enhancement
- Phased Approach to Development Software

Phase I  "Terrorist flagging" proof of principle (2 to 3 months)
  - Identify and develop database (adequate for POP demonstration) by working with domain experts
  - Demonstrate that logic identifies important terrorist actions

Phase II  Develop logic for enhancing base security
  - Identify critical base security issues
  - Identify and develop comprehensive database
  - Develop "flagging" logic and demonstrate daily operation

Phase III  Develop and demonstrate software

June 4, 2002
What We Need for the Demonstration

- Agreement with TSA/DOT to address airline passenger screening
- An Airline Data Base including all available data regarding passenger reservation, billing, payment, check-in, and security checks
  - Preferably one which includes ground truth data
  - Passenger names not critical as long as identification number is provided
  - Specifics on credit not critical: would like to differentiate between credit, check, cash, etc.
- A CAPPS II an airline employee interface (domain experts) to insure problem and solution understanding

- In return
  - TSA/DOT and DOD would be joint beneficiaries of contract deliverables
  - Torch Concepts would treat the data and results at an acceptable security level
Torch Concepts
4650 Whitesburg Drive
Suite 101
Huntsville, Alabama 35802
phone 256.885.0148
dan@torchconcepts.com
Torch Concepts
4650 Whitesburg Drive
Suite 102
Huntsville, Alabama 35802
phone 256.885.0168
fax 256.885.2368
nikholer@torchconcepts.com

Bill Roark
President
www.torchconcepts.com
roark@torchconcepts.com

Roy Nichols
Co-Chairman of the Board
www.torchconcepts.com
nikholer@torchconcepts.com

The Army

66
To: The Army

From: Roy Nichols

Date: June 7, 2002

Subject: Inputs for TSA agreement

Steve, attached are the terms I promised you:

1.0 Program Scope Considerations

2.0 Proof-of-Principle Demonstration

2.1 Data Element Requirements

2.2 Data Volume Requirements

1.0 Program Scope Considerations - Security Enhancement of Military Facilities -

The Army has contracted with Torch Concepts to develop software to enhance the security of military facilities. Security has always been a concern, but the recent Middle-East terrorist actions and the 9-11 attack on the Pentagon have raised this concern to a new level.

Issues include:

- Transportation Transactions - Deliveries of people and products by air, ship, truck and mail
- Base Visitations
- Communications
- Intrusion of information systems

Each of these issues have one thing in common, specifically the lack of an understanding of potential terrorist actions, i.e. there is no way that one could predict the means by which intrusion of an information system would be used for terrorist purposes.

Torch Concepts has proposed a unique technology, termed ACUMEN, which has the potential to identify terrorist actions with minimal or no a priori understanding. ACUMEN's approach is to identify and characterize normal transactions, and then to treat deviations from this norm as potential terrorist actions. By flagging deviations from multiple types of transactions and then examining their correlation, Torch believes that analysts will have a much better chance of counter-terrorism.

To determine the feasibility of this approach, Torch will conduct a Proof-of-Principle demonstration. The contractor has recommended that the demonstration be conducted on "airline passenger screening", primarily because of the availability of ground truth data. The ACUMEN technology would be employed to identify and characterize "all" unique travel modes by evaluating a large...
database, potentially as much as several years of data on airline reservations, billing payment, check-in and security check.

Once the Proof-of-Principle demonstration is proved successful, the technology would be considered for one or more facets of security enhancement for military facilities.

2.0 Proof-of-Principle Demonstration for Security Enhancement of Military Facilities

The following paragraphs address an estimate of passenger data requirements to successfully conduct the Proof-of-Principle demonstration of airline passenger screening.

A research effort, such as the subject program, typically delivers these data requirements as one of the program outputs. Indeed the output would provide the relationship between data requirements and the successful identification of terrorist action. However, to facilitate the timely transfer of data, Torch provides the following admittedly coarse estimates of data requirements.

The first paragraph, which follows, addresses data elements, labeling them either important or desirable. The second paragraph, which follows, addresses the volume of data required.

2.1 Data Element Requirements

Data types are labeled as either important or desirable. The "important label" indicates that the data element's availability will have a significant effect on the ability to identify terrorist actions. Note that twenty-seven (27) elements have been placed by this category. Clearly not all of these elements are required. It is estimated that approximately ten (10) of them will be required. The "desirable label" indicates that the data element's availability will have a positive effect. Our guess is that several "desirable" elements would provide a benefit comparable to that provided by an "important" element.
2:00 PM - 2:30 PM
LEO - Data exchange meeting -- WHCC

June 6th 2002
8:00 AM - 8:30 AM
Do Weekly Rpt for Meeting & Forward
Send rpt to

10:00 AM - 12:00 PM
CAPPS II GE Team meeting and Brainstorm -- 6432
Folks:

1:00 PM - 2:00 PM
Torch Meeting -- Rm 10408

---
From:
Sent:
To:
Subject: Thursday, May 30, 2002 5:10 PM
FYI: CAPPS II

FYI:
The meeting with Torch has been set. If any of you are interested feel free to attend.

---Original Message---
From:
Sent: Thursday, May 30, 2002 5:25 PM
To:
Subject: RE: CAPPS II

---

Each copy available
Torch Concepts has requested a meeting with me through some Congressional contacts and the Congressional Affairs office has been attempting to arrange such a meeting. We have agreed to meet with them.
June 04, 2003 - Continued

June 12, 2003

4:00 PM - 5:00 PM
Updated CAPPS II update — GSA 3B09
will present.
Participants will need an active security clearance to attend.

11:30 AM - 1:30 PM
Project Status Meeting - Room 4027 GSA Bldg
Due to conference room conflicts, please note the time change of the Project Status Meeting.
Meeting will begin at 11:30 am vice 12:00 pm

12:00 PM - 2:00 PM
Meeting

12:00 PM - 1:30 PM
Weekly PM Project Status Meetings — TBD
The room number will be sent out every Tuesday before the meeting.

Thema,

Meeting with Nessa 0432-D
9:00 meeting.
Kelly, Nuala

From: Foster, Jason (Govt Affairs) [Jason_Foster@govt-aff senate.gov]
Sent: Friday, February 13, 2004 4:04 PM
To: Kelly, Nuala
Subject: RE: Document Request

JetBlue - TSA lt to Hutchins...

FYI... this just went out. It's a limited request for starters -- just communications from TSA to JetBlue.

-----Original Message-----
From: Kelly, Nuala [mailto:Nuala.Kelly@DHS.GOV]
Sent: Thursday, February 12, 2004 5:09 PM
To: Foster, Jason (Govt Affairs)
Subject: RE: Document Request

That's cool. It'll be a race for me to get the report out before you request the documents!

Seriously, though, we should talk about what they have.

Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
Washington, DC 20528
(202) 772-9848 (voice)
(202) 772-5036 (fax)

-----Original Message-----
From: Foster, Jason (Govt Affairs) [mailto:Jason_Foster@govt-aff.senate.gov]
Sent: Thursday, February 12, 2004 4:49 PM
To: Kelly, Nuala
Subject: Document Request

No problem. Heads up - we may be sending a joint letter with Lieberman (and possibly Levin) seeking some documents from TSA about its role in the JetBlue matter. Give me a call (224-2186) if you'd like to discuss it before it goes out.

Cordially,
Jason A. Foster
Senior Counsel
Committee on Governmental Affairs
United States Senate

phone: (203) 224-4751
fax: (202) 224-9603

-----Original Message-----
From: Kelly, Nuala [mailto:Nuala.Kelly@DHS.GOV]
Sent: Wednesday, February 11, 2004 7:08 PM
To: Foster, Jason (Govt Affairs)
Subject: FW: GAO report on CAPPS II and the AP report
Still Lots of Work to Be Done on Passenger Screening Plan, Congressional Investigators Say

By Leslie Miller Associated Press Writer

Published: Feb 11, 2004
WASHINGTON (AP) - The government has not adequately addressed security and privacy concerns in its plan to use personal information to rank airline passengers as potential security threats, congressional investigators say.

The Bush administration wants to begin testing a new program this spring and put it in place during the summer. The findings by the General Accounting Office, contained in a draft report obtained Wednesday by The Associated Press, could delay the Computer-Assisted Passenger Prescreening System, or CAPPS II.

Congress said the government could not spend any money for testing or putting the program in place until the GAO reported that eight specific concerns were satisfied. Those include assurances the system is accurate, that the technology ensures privacy, that safeguards exist to prevent abuse and that passengers who think they were mistakenly identified as a threat have some recourse.

The investigators did not recommend whether the program should go forward, but said Transportation Security Administration "has not completely addressed" seven of the eight issues. The exception was creation of an oversight board to monitor the system.

The report said the agency "has not yet completed important system planning activities." The program would screen all passengers by checking information such as name, address and date of birth against commercial and government databases. Each passenger would be given one of three color-coded ratings.

Suspected terrorists and violent criminals would be designated as red and forbidden to fly. Passengers who raise questions would be classified as yellow and would receive extra security screening. The vast majority would be rated as green and be allowed to go through routine screening.

Privacy advocates say the program infringes on civil liberties and may label innocent people as security threats.

The report said privacy concerns remained unresolved in part because the system's development was delayed. One reason for that is airlines do not want to turn over information about passengers until the carriers are sure privacy and security concerns are addressed.

Homeland Security Undersecretary Asa Hutchinson said recently that the program is such a priority that the government will compel airlines to share passenger information. He said he was confident that privacy concerns can be resolved.
From: roarkb@torchconcepts.com
Sent: Tuesday, April 3, 2003 3:38 PM
To: [Blacked out]
Cc: [Blacked out]
Subject: passenger data

To all:

We have just established a point of contact with Acciom to facilitate the transfer of the jetBlue data. We need to do the necessary nondisclosures and paperwork and then the data transfer can occur. Since we have had earlier discussions with Acciom, it may be possible to use the previous paperwork we had in place with Acciom, if so, this could go quickly. We will keep you advised of the progress.

Thanks for your help.

Bill Roark
Torch Concepts, Inc.
Bob:
Thank you so much for your quick response and participation in support of this critical project involving base security. We at the TSA are working with DOD to support this effort. In conjunction with this effort, attached please find the letter of request [which includes phone numbers] regarding PNR data being provided to Torch Concepts for this proof of concept.

If you have any questions, please do not hesitate to call. DOD is looking to kick this project off ASAP for all the obvious reasons, so anything you can do to help expedite the movement of the data between Axiom and Torch would be greatly appreciated.

[Handwritten note:]

DOD

[signature]

[Handwritten note:]

no attachment included