



# Homeland Security

*Privacy Office, Mail Stop 0550*

October 1, 2007

Mr. David L. Sobel  
Electronic Frontier Foundation  
1875 Connecticut Avenue, N.W.  
Suite 650  
Washington, DC 20009

**Re: DHS/OS/PRIV 07-160/Sobel request**

Dear Mr. Sobel:

This is our sixth partial release to your Freedom of Information Act (FOIA) requests to the Department of Homeland Security (DHS), dated November 7, 2006 and December 6, 2006, requesting DHS records concerning the Automated Targeting System (ATS). These two requests were aggregated to simplify processing. The following is a consolidated list of records requested:

1. All Privacy Impact Assessments prepared for the ATS system or any predecessor system that served the same function but bore a different name.
2. A Memorandum of Understanding executed on or about March 9, 2005 between Customs and Border Protection (CBP) and the Canada Border Services Agency to facilitate the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information.
3. All records, including Privacy Act notices, which discuss or describe the use of personally-identifiable information by the CBP (or its predecessors) for purposes of screening air and sea travelers.
4. All System of Records Notices (SORNs) that discuss or describe targeting, screening, or assigning "risk assessments" of U.S. citizens by CBP or its predecessors.
5. All records that discuss or describe the redress that is available to individuals who believe that the ATS contains or utilizes inaccurate, incomplete or outdated information about them.
6. All records that discuss or describe the potential consequences that individuals might experience as a result of the agency's use of the ATS, including but not limited to arrest, physical searches, surveillance, denial of the opportunity to travel, and loss of employment opportunities.
7. All records that discuss or identify the number of individuals who have been arrested as a result of screening by the ATS and the offenses for which they were charged.
8. All complaints received from individuals concerning actions taken by the agency as a result of ATS "risk assessments" or other information contained in the ATS, and the agency's response to those complaints.
9. All records that discuss or describe Section 514 of the Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441) and its prohibition against the development or testing of "algorithms assigning risk to passengers whose names are not on Government watch lists."
10. All records that address any of the following issues:
  - a. Whether a system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights may appeal such decision and correct erroneous information contained in the ATS;
  - b. Whether the underlying error rate of the government and private databases that will be used in the ATS to assign a risk level to an individual will not produce a large number of false

- positives that will result in a significant number of individuals being treated mistakenly or security resources being diverted;
- c. Whether the agency has stress-tested and demonstrated the efficacy and accuracy of all search tools in the ATS and has demonstrated that the ATS can make an accurate predictive assessment of those individuals who may constitute a threat;
  - d. Whether the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which the ATS is being developed and prepared;
  - e. Whether the agency has built in sufficient operational safeguards to reduce the opportunities for abuse;
  - f. Whether substantial security measures are in place to protect the ATS from unauthorized access by hackers or other intruders;
  - g. Whether the agency has adopted policies establishing effective oversight of the use and operation of the system;
  - h. Whether there are no specific privacy concerns with the technological architecture of the system;
  - i. Whether the agency has, pursuant to the requirements of section 44903(i)(2)(A) of Title 49, United States Code, modified the ATS with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger a high risk status; and
  - j. Whether appropriate life-cycle estimates, expenditure and program plans exist.

Our September 1, 2007 letter summarized our processing of your request; however, we failed to take into account records released to you in our August 1, 2007 letter. Therefore, our searches directed to the DHS Office of the Executive Secretariat (ES), DHS Office of Policy (PLCY), DHS Privacy Office (PRIV), DHS Office of General Counsel (OGC), the Transportation Security Administration (TSA), and the U.S. Customs and Border Protection (CBP) have thus far produced a combined total of 648 pages. Out of those 648 pages, we provided you with a combined total of 235 pages with certain information withheld pursuant to the FOIA. We have continued to process your request within PRIV, PLCY, OGC, the DHS Office of the Inspector General (OIG), and CBP.

Upon further review of a December 18, 2006 memorandum for Secretary Chertoff, which was released to you in our second partial response, we have decided that additional information is available for release. Accordingly, that 3-page document is enclosed with revised redactions made pursuant to Exemption 7E of the FOIA.

A search directed to PRIV has produced an additional 47 pages of records responsive to your request. Of those 47 pages, we have determined that 1 page is releasable to you in its entirety, 18 pages are releasable to you with certain information withheld pursuant to Exemptions 2, 5, 6, and 7E of the FOIA, and 28 pages are withheld in their entirety pursuant to Exemptions 2, 5, and 7E of the FOIA. PRIV has completed its search for documents, and no other responsive documents were located.

A search directed to PLCY has produced an additional 24 pages of records responsive to your request. Of those 24 pages, we have determined that 5 pages are releasable to you in their entirety, 13 pages are releasable to you with certain information withheld pursuant to Exemptions 2, 5, and 6 of the FOIA, and 9 pages are withheld in their entirety pursuant to Exemption 5 of the FOIA. PLCY has completed its search for documents, and no other responsive documents were located.

A search directed to OGC has produced an additional 18 pages of records responsive to your request. Of those 18 pages, we have determined that 2 pages are releasable to you in their entirety, 10 pages are releasable to you with certain information withheld pursuant to Exemptions 2, 5, 6 and 7E of the FOIA, and 6 pages are withheld in their entirety pursuant to Exemption 5 of the FOIA. OGC has completed its search for documents, and no other responsive documents were located.

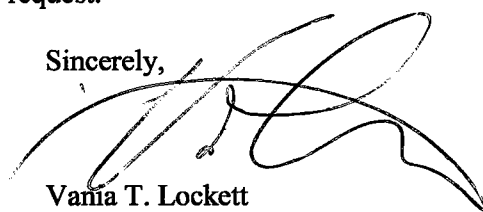
A search directed to OIG has produced 641 pages of records responsive to your request. Of those 641 pages, we have determined that 13 pages are releasable to you in their entirety, 66 pages are releasable to you with certain information withheld pursuant to Exemptions 2, 5, 6, 7C, and 7E of the FOIA, and 562 pages are withheld in their entirety pursuant to Exemption 5 of the FOIA. For your information, in the redacted final report entitled, "Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry," an asterisk has been placed next to information pertaining to ATS. OIG has completed its search for documents, and no other responsive documents were located.

A search directed to CBP has produced an additional 97 pages of records responsive to your request. Of those 97 pages, we have determined that 18 pages are releasable to you in their entirety, 53 pages are releasable to you with certain information withheld pursuant to Exemptions 2, 5, 6, and 7E of the FOIA, and 26 pages are withheld in their entirety pursuant to Exemptions 2, 5 and 7E of the FOIA.

Enclosed are 202 pages of releasable information. The withheld information, which will be noted on the Vaughn index when completed, consists of names, telephone numbers, email addresses, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, 7C, and 7E of the FOIA, 5 U.S.C. §§ 552 (b)(2), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E). Exemption 2(high) protects information applicable to internal administrative matters to the extent that disclosure would risk circumvention of an agency regulation or statute, impede the effectiveness of an agency's activities, or reveal sensitive information that may put the security and safety of an agency activity or employee at risk. Included within such information may be operating rules, guidelines, manuals of procedures for examiners or adjudicators, and homeland security information. Exemption 2(low) protects information applicable to internal administrative personnel matters to the extent that the information is of a relatively trivial nature. Exemption 5 exempts from disclosure certain inter- and intra-agency communications protected by deliberative process privilege, attorney work-product privilege, and attorney-client privilege. Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Exemption 7C protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. Exemption 7E protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Our office continues to process your request as it pertains to CBP. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-160/Sobel request**. This office can be reached at 866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,

A handwritten signature in black ink, appearing to read "Vania T. Lockett", written over a horizontal line.

Vania T. Lockett  
Associate Director, Disclosure & FOIA Operations

Enclosures: 202 pages

December 18, 2006



MEMORANDUM FOR SECRETARY CHERTOFF

FROM: Commissioner

SUBJECT: Automated Targeting System for Passengers Update

I am writing to provide you an update on the performance of U.S. Customs and Border Protection's (CBP) Automated Targeting System for Passengers (ATS-P) and its role in preventing known national security risks and serious criminal violators from entering the United States.

On a daily basis, ATS-P generates a significant number of referrals for further follow-up by CBP Officers. The encounters described below underscore how the use of automated tools is critical to identifying travelers who present potential security threats while at the same time keeping the vast majority of the traveling public safe and moving expeditiously.

- At the Minneapolis-St. Paul Airport in September 2006, CBP Officers used ATS-P to select a high-risk passenger for further examination. As a result of the examination CBP determined that the individual was in possession of video clips of various Improvised Explosive Devices (IEDs) being used against soldiers and vehicles. The subject was also carrying a manual on how to make IEDs and a video on martyrdom. (

[ b7E ]

) On December 6, 2006, the subject agreed to plead guilty to Visa Fraud and agreed to not contest his prompt removal from the United States.

- In October 2006, a CBP Officer using ATS-P identified an individual traveling into Atlanta-Hartsfield Airport as a subject of interest. Intelligence reports linked this person to earlier attempts to observe security practices at a U.S. Embassy, as well as the surveillance of other sensitive sites. (

[ b7E ]

) All three

<sup>1</sup> The U.S. Customs Service began using automated targeting systems as a law enforcement tool in the early 1990's to help Customs Inspectors identify cargo entering the United States in violation of U.S. law. These early targeting systems were expanded to the passenger environment in the mid-1990's and the web-based ATS-P became operational in October 2000.

subjects were traveling separately and applied for admission as tourists. CBP Officers confirmed during their interviews of the individuals that they knew each other and were traveling together. All three were refused admission.

- In May 2005, ATS-P enabled CBP to identify three passengers with travel histories indicating that they might be using fraudulent travel documents to enter the United States. CBP alerted the air carrier, which performed a thorough review of all three travelers' documents prior to boarding. The airline denied one passenger boarding because he was in possession of a fraudulent travel document. The two others were referred for an additional examination upon arrival in the United States. Both subjects were determined to be part of a human smuggling organization and they were preparing to smuggle the first victim. Additionally, one of the smugglers was identified as a member of a Japanese crime syndicate.
- At Boston's Logan Airport in April 2006, CBP Officers used ATS-P to identify two passengers ( [ b7E ] ) The examination of the subject's baggage revealed images of armed men, one of which was labeled "Mujahadin." Both passengers were refused admission.
- In May 2006, ATS-P identified a high-risk traveler arriving at Atlanta Hartsfield airport from Europe. CBP Officers determined that the individual's visa was issued one week prior to September 11, 2001, yet he had never traveled to the United States. The subject's passport listed him as a "flight instructor" and his reasons for traveling to the United States included the plan to "see a man in New York for two days." The individual was ultimately linked to numerous individuals who U.S. law enforcement regards as security risks and immigration violators. The passenger was denied admission.
- In May 2006, CBP Officers at Minneapolis St. Paul used ATS-P to identify a high-risk passenger ( b7E ) Upon arrival the subject requested political asylum. During the course of the interview by the CBP Officer, the subject admitted to being associated with a terrorist organization, which had led to a criminal conviction and incarceration 6 years prior. The subject also admitted to having lied on his U.S. visa application regarding his conviction and terrorist associations. The subject eventually abandoned his request for political asylum and was expeditiously removed from the United States.
- In June 2003, CBP Officers, using ATS-P, identified Ra'ed Mansour Al-Banna as a subject of interest prior to his flight's arrival at Chicago

O'Hare Airport. Upon arrival, Al-Banna was referred to secondary for further inspection. As a result of further research in ATS-P and through the CBP interview, CBP Officers determined Al-Banna to be inadmissible and he was refused entry into the United States. On February 28, 2005, Ra'ed Mansour Al-Banna carried out a suicide bomb attack in Hilla, Iraq, killing 32 people.

Annually, 87 million air travelers and 26 million cruise ship passengers and crew arrive in the United States, the majority of which arrive during an three-hour window. In each of the cases detailed above, the intensive work of CBP Officers in identifying and interviewing the individuals was conducted and completed while a huge flow of legitimate and law-abiding travelers, both U.S. citizens and non-citizens, transited the international arrival areas within minimal delay.

My staff and I are available to provide additional information or answer any questions you may have regarding this update.

( b6 )

---

**From:** Teufel, Hugo  
**Sent:** Friday, November 03, 2006 1:37 PM  
**To:** Richards, Rebecca; Mortensen, Kenneth; Levin, Toby  
**Subject:** FW: JUST THE FACTS

( b5 )

---

**From:** Knocke, William R (mailto: { b2 } )  
**Sent:** Friday, November 03, 2006 1:19 PM  
**To:** Sweet, Chad; ( b6 ) ; Baker, Stewart; Teufel, Hugo; Perry, Phil; Coldebella, Gus; Rosenzweig, Paul  
**Cc:** Agen, Jarrod; Gonzalez, Joanna  
**Subject:** RE: JUST THE FACTS

The WashPost is contemplating a correction. We have firm ground on the points below. Please let me know, by 3:30 PM, if there are any other points that we can raise with them and correct with fact based data. Thanks.

- 1) "The federal government disclosed details yesterday of a border-security program to screen all people who enter and leave the United States, create a terrorism risk profile of each individual and retain that information for up to 40 years."

**Correction:**

- "This system of records notice does not identify or create any new collection of information, rather DHS is providing additional notice and transparency of the functionality of these systems." (DHS Notice of Privacy Act System of Records, Vol. 71, No. 212, Nov. 2, 2006)
- 2) "While long known to scrutinize air travelers, the Department of Homeland Security is seeking to apply new technology to perform similar checks on people who enter or leave the country 'by automobile or on foot.'"

**Correction:**

- "CBP has used the advance submission of traveler information to aid in screening travelers to facilitate its border enforcement mission." (DHS Notice of Privacy Act System of Records, Vol. 71, No. 212, Nov. 2, 2006)

---

**From:** Sweet, Chad  
**Sent:** Friday, November 03, 2006 12:56 PM  
**To:** Knocke, William R; ( b6 ) ; Baker, Stewart; Teufel, Hugo; Perry, Phil; Coldebella, Gus; Rosenzweig, Paul  
**Cc:** Agen, Jarrod; Gonzalez, Joanna  
**Subject:** RE: JUST THE FACTS

Appreciate the rapid reaction.

( b6 )

CCS

---

Chad C. Sweet  
Deputy Chief of Staff  
Department of Homeland Security

[ ba ]

---

**From:** Knocke, William R  
**Sent:** Friday, November 03, 2006 12:21 PM  
**To:** ( ~~ba~~ ); Baker, Stewart; Teufel, Hugo; Perry, Phil; Coldebella, Gus; Rosenzweig, Paul; Sweet, Chad  
**Cc:** Agen, Jarrod; Gonzalez, Joanna  
**Subject:** FW: JUST THE FACTS

All-

Please find a DRAFT Just the Facts document. This could be used with stakeholders and press if there is additional follow-up later in the day. Please let us know ASAP if you have any feedback... Russ

**From:** Agen, Jarrod  
**Sent:** Friday, November 03, 2006 12:12 PM  
**To:** Knocke, William R; Gonzalez, Joanna; Bergman, Cynthia  
**Subject:** JUST THE FACTS

Press Office  
U.S. Department of Homeland Security

# Just the Facts

November 3, 2006

## WASHINGTON POST STORY ON AUTOMATED TARGETING SYSTEM

**A WASHINGTON POST STORY CLAIMS THAT DHS IS CREATING A NEW SCREENING PROGRAM AT U.S. BORDERS:** "The federal government disclosed details yesterday of a border-security program to screen all people who enter and leave the United States, create a terrorism risk profile of each individual and retain that information for up to 40 years." ("U.S. Plans to Screen All Who Enter, Leave Country Personal Data Will Be Cross-Checked With Terrorism Watch Lists; Risk Profiles to Be Stored for Years," *Washington Post*, 11/03/06)

### **BUT AS CLEARLY STATED IN THE NOTICE, THERE IS NO NEW SYSTEM BEING CREATED:**

- "This system of records notice does not identify or create any new collection of information, rather DHS is providing additional notice and transparency of the functionality of these systems." (DHS Notice of Privacy Act System of Records, Vol. 71, No. 212, Nov. 2, 2006)

( ba )



**THE STORY ALSO CLAIMS THAT A NEW PROCESS WILL BE USED FOR TRAVELERS ENTERING THROUGH OUR LAND BORDERS:** "While long known to scrutinize air travelers, the Department of Homeland Security is seeking to apply new technology to perform similar checks on people who enter or leave the country 'by automobile or on foot.'" ("U.S. Plans to Screen All Who Enter, Leave Country Personal Data Will Be Cross-Checked With Terrorism Watch Lists; Risk Profiles to Be Stored for Years," *Washington Post*, 11/03/06)

**AGAIN, THIS IS NOT A NEW SYSTEM. AS THE NOTICE STATES:**

- "CBP has used the advance submission of traveler information to aid in screening travelers to facilitate its border enforcement mission." (DHS Notice of Privacy Act System of Records, Vol. 71, No. 212, Nov. 2, 2006)

**THE WASHINGTON POST INCORRECTLY STATES THAT EACH PASSENGER IS DESIGNATED A RISK SCORE:** "Each traveler assessed by the center is assigned a numeric score: The higher the score, the higher the risk." ("U.S. Plans to Screen All Who Enter, Leave Country Personal Data Will Be Cross-Checked With Terrorism Watch Lists; Risk Profiles to Be Stored for Years," *Washington Post*, 11/03/06)

**DHS USES DATABASES ONLY TO DETERMINE RISKS TO NATIONAL SECURITY:**

- "The Automated Targeting System (ATS) associates information obtained from CBP's cargo, travelers, and border enforcement systems with a level of risk posed by each item and person..." (DHS Notice of Privacy Act System of Records, Vol. 71, No. 212, Nov. 2, 2006)

**THE STORY ALSO CLAIMS THAT DHS WILL RETAIN INDIVIDUALS' INFORMATION FOR UP TO 40 YEARS:** "In yesterday's Federal Register notice, Homeland Security said it will keep people's risk profiles for up to 40 years." ("U.S. Plans to Screen All Who Enter, Leave Country Personal Data Will Be Cross-Checked With Terrorism Watch Lists; Risk Profiles to Be Stored for Years," *Washington Post*, 11/03/06)

**THE NOTICE STATES THAT DATA IS REGULARY REVIEWED AND IRRELEVANT DATA IS DELETED:**

- "The retention period for data specifically maintained in ATS will not exceed forty years at which time it will be deleted from ATS. Up to forty years of data retention may be required to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities." (DHS Notice of Privacy Act System of Records, Vol. 71, No. 212, Nov. 2, 2006)
- "CBP will regularly review the data maintained in ATS to ensure its continued relevance and usefulness. If no longer relevant and useful, CBP will delete the information." (DHS Notice of Privacy Act System of Records, Vol. 71, No. 212, Nov. 2, 2006)

( b6 )

From: ( b6 ) ( b7 )  
 Sent: Friday, November 03, 2006 10:55 AM  
 To: Rosenzweig, Paul; ( b6 ), Agen, Jarrod; Knocke, William R  
 Cc: Teufel, Hugo; Mortensen, Kenneth; ( b6 ); ( b6 )  
 Subject: RE: Talking point on new ATS Fed Register Announcement  
 Importance: High

Russ:  
 Here are just a few more points based on our conversation this morning.  
 GENERAL

[ b5 ]

SORN UPDATE

[ b5 ]

RETENTION

[ b5 ]

From: Rosenzweig, Paul  
 Sent: Friday, November 03, 2006 9:46 AM

( b2 )

To: [ b6 ] Agen, Jarrod  
Cc: [ b6 ]  
Subject: RE: Talking point on new ATS Fed Register Announcement

Suggest something along the following lines:

[ b5 ]

( b6 ) - anything to add?

Paul Rosenzweig

[ b2 ]

From: ( b6 ) [mailto: ( b2 ) ]  
Sent: Friday, November 03, 2006 9:42 AM  
To: Agen, Jarrod  
Cc: Rosenzweig, Paul  
Subject: Talking point on new ATS Fed Register Announcement

Jarrod:

Do we have any talking points or press guidance on this? Need something ASAP as Paul Rosenzweig and I are going to brief the Canadian Embassy at 10:30 and this could come up

Thanks.

Theresa

( b6 )  
Director for Canadian Affairs  
DHS Policy  
Office of International Affairs

[ b2 ] (desk)  
( b2 ) (cell)

## U.S. Plans to Screen All Who Enter, Leave Country

Personal Data Will Be Cross-Checked With Terrorism Watch Lists; Risk Profiles to Be Stored for Years

By Ellen Nakashima and Spencer S. Hsu  
Washington Post Staff Writers  
Friday, November 3, 2006; A18

The federal government disclosed details yesterday of a border-security program to screen all people who enter and leave the United States, create a terrorism risk profile of each individual and retain that information for up to 10 years.

The details, released in a notice published yesterday in the Federal Register, open a new window on the government's broad and often controversial data-collection effort directed at American and foreign

travelers, which was implemented after the Sept. 11, 2001, attacks.

While long known to scrutinize air travelers, the Department of Homeland Security is seeking to apply new technology to perform similar checks on people who enter or leave the country "by automobile or on foot," the notice said.

The department intends to use a program called the Automated Targeting System, originally designed to screen shipping cargo, to store and analyze the data.

"We have been doing risk assessments of cargo and passengers coming into and out of the U.S.," DHS spokesman Jarrod Agen said. "We have the authority and the ability to do it for passengers coming by land and sea."

In practice, he said, the government has not conducted risk assessments on travelers at land crossings for logistical reasons.

"We gather, collect information that is needed to protect the borders," Agen said. "We store the information we see as pertinent to keeping Americans safe."

Civil libertarians expressed concern that risk profiling on such a scale would be intrusive and would not adequately protect citizens' privacy rights, issues similar to those that have surrounded systems profiling air passengers.

"They are assigning a suspicion level to millions of law-abiding citizens," said David Sobel, senior counsel of the Electronic Frontier Foundation. "This is about as Kafkaesque as you can get."

DHS officials said that by publishing the notice, they are simply providing "expanded notice and transparency" about an existing program disclosed in October 2001, the Treasury Enforcement Communications System.

But others said Congress has been unaware of the potential of the Automated Targeting System to assess non-aviation travelers.

"ATS started as a tool to prevent the entry of drugs with cargo into the U.S.," said one aide, who spoke on the condition of anonymity because of the sensitivity of the subject. "We are not aware of Congress specifically legislating to make this expansion possible."

The Senate Homeland Security and Governmental Affairs Committee, chaired by Sen. Susan Collins (R-Maine), yesterday asked Homeland Security to brief staff members on the program. Collins's spokeswoman, Jen Burita, said.

The notice comes as the department is tightening its ability to identify people at the borders. At the end of the year, for example, Homeland Security is expanding its Visitor and Immigrant Status Indicator Technology program, under which 32 million noncitizens entering the country annually are fingerprinted and photographed at 115 airports, 15 seaports and 154 land ports.

Stephen E. Flynn, senior fellow for national security studies at the Council on Foreign Relations, expressed doubts about the department's ability to conduct risk assessments of individuals on a wide scale.

He said customs investigators are so focused on finding drugs and weapons of mass destruction that it would be difficult to screen all individual border crossers, other than cargo-truck drivers and shipping crews.

"There is an ability in theory for government to cast a wider net," he said. "The reality of it is customs is barely able to manage the data they have."

The data-mining program stemmed from an effort in the early 1990s by customs officials to begin assessing the risk of cargo originating in certain countries and from certain shippers. Risk assessment turned more heavily to automated, computer-driven systems after the 2001 attacks.

The risk assessment is created by analysts at the National Targeting Center, a high-tech facility opened in November 2001 and now run by Customs and Border Protection.

In a round-the-clock operation, targeters match names against terrorist watch lists and a host of other data to determine whether a person's background or behavior indicates a terrorist threat, a risk to border security or the potential for illegal activity. They also assess cargo.

Each traveler assessed by the center is assigned a numeric score: The higher the score, the higher the risk. A certain number of points send the traveler back for a full interview.

The Automated Targeting System relies on government databases that include law enforcement data, shipping manifests, travel itineraries and airline passenger data, such as names, addresses, credit card details and phone numbers.

The parent program, Treasury Enforcement Communications System, houses "every possible type of information from a variety of federal, state and local sources," according to a 2001 Federal Register notice.

It includes arrest records, physical descriptions and "wanted" notices. The 5.3 billion-record database was accessed 766 million times a day to process 475 million travelers, according to a 2003 Transportation Research Board study.

In yesterday's Federal Register notice, Homeland Security said it will keep people's risk profiles for up to 40 years "to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities," and because "the risk assessment for individuals who are deemed low risk will be relevant if their risk profile changes in the future, for example, if terrorist associations are identified."

DHS will keep a "pointer or reference" to the underlying records that resulted in the profile.

The DHS notice specified that the Automated Targeting System does not call for any new means of collecting information but rather for the use of existing systems. The notice did not spell out what will determine whether someone is high risk.

But documents and former officials say the system relies on hundreds of "rules" to factor a score for each individual, vehicle or piece of cargo.

According to yesterday's notice, the program is exempt from certain requirements of the Privacy Act of 1974 that allow, for instance, people to access records to determine "if the system contains a record pertaining to a particular individual" and "for the purpose of contesting the content of the record."

# SCREENING | 2 JAN 07 REVIEW

FOCUS ON ATIS-P (passengers)

## DATASETS & SOURCES

API: Gov't issued Travel Docs - from carrier → CBP  
"Advanced passenger info."

Name (last, first)

DOB

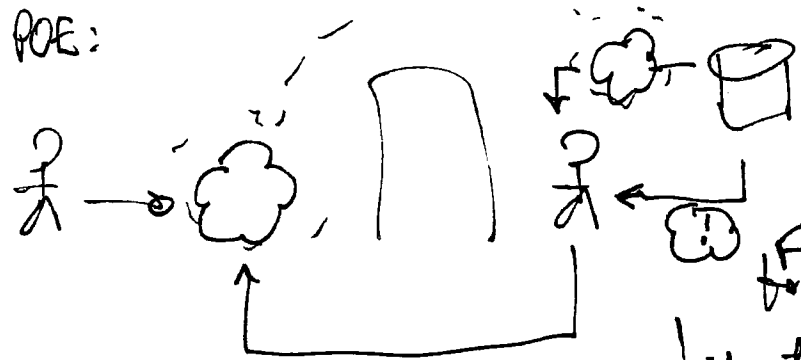
Travel doc (including from foreign gov'ts)

Gender

Status (pass, crew)

Query: shows types of contact & documents

AT POE:



Ⓢ checks match between

there is also warning for action

if there is a discrepancy, the Ⓢ is corrected not the Ⓢ challenged.

APIS: preposition info for Ⓢ screening then for Ⓢ to correct data from Ⓢ to ensure accuracy of the Ⓢ and correct as needed then begin the screening.

Ⓢ the watch/action alert  
Standard of practice

- owner (must already have author. by cleared) to create entry
- duration
- approved by supervisor

Matches could be false positives and they are vetted  
prior to arrival :: prior to primary

APIS - used to match against knows

PVR - used to match against patterns used to indicate risk

APIS data →



PRIMARY

data matched for (+) and vetted for false (+)

( b2, b7E )  
Based on cleared for mismatched

b6

### Internal Audit of I use

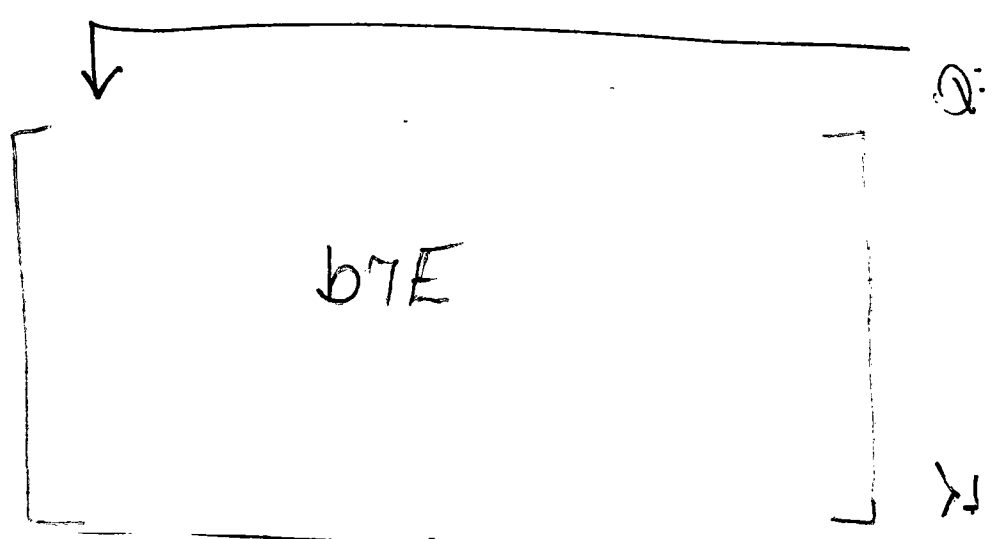
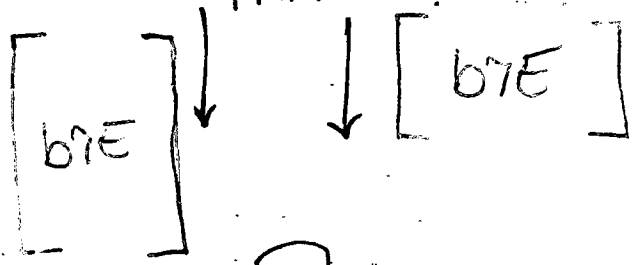
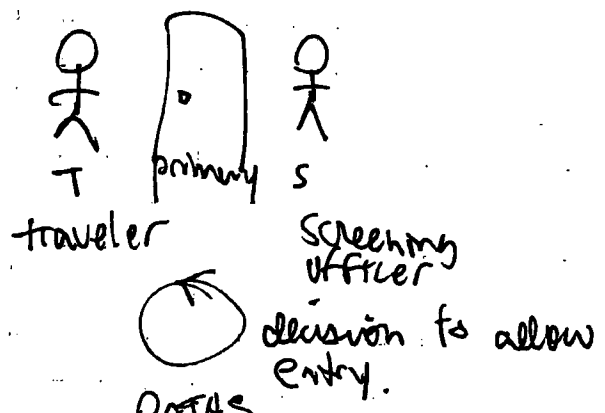
- automated flagging: patterns/rules
- data captured at key stroke + timestamp level
- <sup>for full play back</sup> plus periodic review of the logs by Internal Affairs
- specific case-driven
- \* all screen is actually captured (payload)
- access to the full audit info is governed at a higher level

### ACCESS TO SYSTEM

#### More than Role

- Background Check
- Direct approval from supervisor: Actual vetted Need to know
- Separate request for access to system at system level
- Separate access to mainframe
- Separate requirement to manage all approved users
- 2 year repeated tests include PVT + Sec

# SCREENING ~~cm4~~ cm4



## PATTERN-BASED RI

cloud icon: detailed info

⊕ } some internal threshold to create Rule based on nature of, details, of info

⊕ Create rule

⊕ implement rule

~~list of satisfying R~~

KNOWN : match-based rules

OR UNKNOWN : pattern-driven rules

∴ for every rule there is a history of the logic that led to the creation of the rule

End: as threat expires, the Rule EXPIRES



SUBJECT MATTER

# DATA MINING

PLATE-BASED PROCESS  
QUESTIONS FOR DM CONTINUUM

b7E

[ b6 ] - Act Exce Dir. Natl Targeting Security oversees NTC

[ b6 ] - Assoc. Chief Counsel CBP for enforcement

( b6 ) Targeting Centre

( b6 ) - pgm manager for ATS

( b6 )

( b6 )

( b6 )

### Data sets & sources

APIS - collected by ocean or air carriers to CBP  
advanced passenger info

now mandatory

Air passenger data - name, DOB, travel doc (PP, US issued LPR card  
or reentry permit  
other govt's doc.)  
passenger or crew,

run against TECS & pulls back query

NIV - non-migrant visa

frequent docs - 1 w/in 18 mos.

airline transmit info & run ag the db. Any match that  
requires an action will appear on primary for the officer

Purpose of APIS was to do processing ahead of time &  
allow officer to check data matches on TD

running ag TECS & NCIC

subject look out

Look out records: MOUs w/ NTC to access TECS.  
Incorp. info into TECS - look out info from  
( b7E )  
(list duration for look out) must be approved by agency  
immigr. visa info from State Dept.  
CLASS

T Screening DB

( b7E )  
→ NCTC controls the classified

( b7E )  
'vetted before person arrives so they are not inconvenienced

APIS used to match against knowns

PNR used to assess risk (PNR is dirty data w/ last name reversed etc.)

( b2, b7E ) - began last Febr.  
20,000 now enrolled.

Who has access - each officer has a profile - need to know - all officers have access & audit tracking (some automatic rules & internal affairs reviews) query flags down to keystroke level screens are captured

PNR

voluntary basis pre-2001  
Aviation Transp Security Act 2001 made it mandatory prior to departure (72 hrs)

diff airlines provide diff data sets  
push vs pull issues, worked out w/

NO PNR in TECS

only in ATS-P - TW3 is unique to ATS-P

ATS-P



must have access permission  
mainframe access reviewed at 6 mos.  
only accessed w/ need to know

admin. Certif.  
biannual exams every 2 yea.  
(privat/audit)

( b7E ), Lost & Stolen PP  
for outbound provided no later than 15 min.

1-94 data - add in TECS  
Same info in TECS previously, just presented

decision support tool  
above are matching tools

no rules make things happen - to inspect how much inspection  
→ ① ( b7E )

→ ② ( b7E )

# Known and unknown

matches to  
clb  
(persons known due  
to biographical info  
& dis play for  
officer

look for patterns of behavior  
using PNR (

[ b7E ]

& in conjunction w/  
other data make  
person of interest

[ b7E ]

rules derived w/ CBP office of intel  
go thru classified traffic to identify  
threats to US -

see if operational in nature  
& can apply to the border  
& identify how to respond to  
the threat (identify data

sets)  
to address scenarios

( b7E )

ATS - L clb be db of vehicles  
make model's history

that it again  
the data  
to see if it  
is useful  
rule

always reassess threat to see if still valid  
rules reflect particular intelligence  
rules tied to threat analysis  
& may last for limited time

rules apply to unknown  
rules based on intelligence

no score [ b7E ]

Some programs have scoring but not ATS - P  
earlier use of score did not  
require action. <sup>Did have scoring when designed</sup>  
Dec. 04 - stopped feature  
since decided better to use  
human intelligence

it is for targeting terrorism  
(APIS ~~E~~ used for known)  
PNE can use ATS

primary purpose is  
terrorism targeting

### Threshold targeting

[ b7E ]

re rules - oversight  
create & remove process goes to ( b6 )

[ b7E ]

## ATS

### ATS overview and results:

- The Automated Targeting System (ATS) provides decision support functionality for CBP officers working in Advanced Targeting Units (ATUs) at our ports of entry.
- The system supports CBP's targeting efforts for cargo, passengers and land border passenger vehicles.
- ATS-N utilizes manifest and entry declaration data from the Automated Commercial System and enforcement data from the Treasury Enforcement Communications System (TECS) to provide targeting functionality for cargo. National targeting rule sets have been implemented in ATS-N to provide threshold targeting for national security risks for all modes: sea, truck, rail, and air.
- Threshold targeting uses numerous targeting rules that work in combination to vet different shipment information against historical and enforcement records and prioritize "unusual" shipments through automated, relative risk assessments. Additional targeting rules have been developed to address risks associated with agro-terrorism, contraband, intellectual property rights, and pharmaceuticals.
- The Automated Targeting System-Passenger (ATS-P) currently utilizes data elements from TECS and airline reservation data (Passenger Name Records, or PNR) to provide automated risk assessments of arriving and departing international air and sea travelers. ATS-P provides targeting functionality to CBP officers at air and sea ports of entry and to the target analysts at the National Targeting Center, and ATS-L provides similar functionality at the land border ports of entry for targeting conveyances.

### How does the risk assessment work; what does it tell us?

- For risk assessments of cargo, ATS provides different rule sets developed to address security risks for different modes (sea, rail, truck, and air). (

[ b2 high, b7E ]

- These rule sets are comprised of a number of targeting rules that utilize historical information and enforcement information (and intelligence when applicable) that work in combination to systemically assess relative levels of risks for shipments. (

[ b2 high, b7E ]

- The targeting rule sets are reviewed and refined periodically through conferences with subject matter experts from the Field and information technology experts; however,

[ b2 high, b7E ]

· For risk assessments of passengers, CBP develops criteria to target high-risk travelers by creating rules based on actionable intelligence to generate lookouts in ATS-P. Subjects of these lookouts are then referred for examination as necessary. (

b2 high  
b7E

**When did you start using it on travelers; what's been the experience?**

· CBP has used ATS-P since the late 1990's to target high-risk travelers. It was not possible, however, to conduct risk assessments of all travelers until the passage of the Air Transportation and Security Act of 2001, which mandated air carriers to provide Advance Passenger Information for all passengers and crew, and PNR for all passengers.

---



**Differences Between The Automated Targeting System And The Treasury Enforcement Communications System**

These are two different IT systems.

Automated Targeting System (ATS) has three main functions:

- 1. Provides a risk-based system ( b2 high, b7E )
- 2. Retrieves and maintains raw passenger name record (PNR) data
- 3. Provides a graphical user interface (GUI) for many of the underlying legacy systems from which ATS pulls information. This interface improves the user experience by providing the same functionality in more rigidly controlled access environment than the underlying system. ( b2 high, b7E ]

Treasury Enforcement Communications System (TECS) ( b2 high, b7E ) that searches for exact matches of name and date of birth.

- 1. It is the underlying information technology backbone for a number of different DHS data collections including:
  - a. Advanced Passenger Information System (APIS)
  - b. Border crossing information

[ b2 high, b7E ]

- 2. Allows CBP Officers and DHS employees (as appropriate) access to other sources of information for border enforcement purposes. Key systems that can be accessed include:
  - a. FBI's National Criminal Information Center (NCIC)

[ b2 high b7E ]

( b6 )

**From:** ( b6 )  
**Sent:** Friday, December 15, 2006 3:57 PM  
**To:** Sales, Nathan  
**Subject:** FW: ATS Standards  
  
**Importance:** High  
  
**Attachments:** ASbakerats-mseds.doc



ASbakerats-mseds.doc (35 KB)

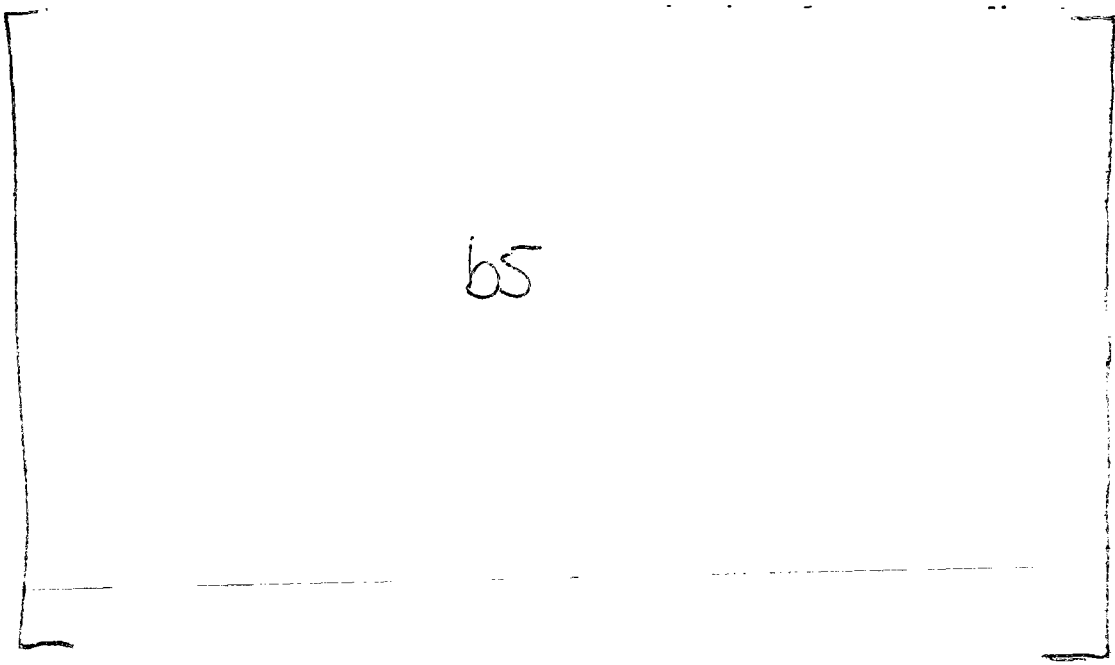
Updated text to reference the standards ID'd by CBP below

( b6 )  
( b6 )

-----Original Message-----

**From:** ( b6 ) ( b2 & b6 )  
**Sent:** Friday, December 15, 2006 2:08 PM  
**To:** Sales, Nathan; ( b6 )  
**Subject:** ATS Standards  
**Importance:** High

( b6 ) he following should assist in answering your questions:



( b6 )

**[Agency Point of Contact or Agency Official Requesting Access]  
[Agency Name]  
[Agency Address]**

**[Salutation]**

**As a result of the interim agreement between the United States and the European Union on the processing and transfer of passenger name record (PNR) data, dated October 19, 2006, CBP is now permitted to provide direct access to PNR through its Automated Targeting System – Passenger (ATS-P) to officers of U.S. Immigration and Customs Enforcement (ICE) and DHS offices that fall under the Office of the Secretary.**

**[Agency/Office Name] has been identified as an agency or office that may qualify for access to PNR through ATS-P.**

**Access to PNR data may be provided to appropriate personnel in your agency/office upon [Agency/Office Name]'s certification that it will: 1) comply with the terms of the PNR Undertakings, as interpreted in an October 6, 2006 letter from Assistant Secretary Stewart Baker to the European Commission and European Union Presidency (attached as Annex A); and 2) ensure that all personnel authorized to access ATS-P adhere to CBP's PNR Field Guidelines for Use and Disclosure of PNR (attached as Annex B) and are disciplined for any improper activity in a manner consistent with the Undertakings and Field Guidance. A form request letter that contains the necessary requirements for this certification is attached for your consideration and use (Annex C). A CBP Form 7300 (attached as Annex D) will also need to be completed on behalf of any individual for whom your Agency/Office seeks access to ATS-P.**

**All activity within ATS-P is monitored and audited and there are serious consequences for violation of the PNR Field Guidance. As set forth in these policies, CBP considers PNR information to be law enforcement sensitive, confidential personal information of the data subject ("Official Use Only" Administrative Classification"), and confidential commercial information of the air carrier, exempt from disclosure pursuant to 5 U.S.C. 552 (b)(2), (b)(4), (b)(6), and (b)(7)(C). PNR records may also be protected under the Privacy Act if the subject of the record is a U.S. citizen or permanent resident (5 U.S.C. 552a). Furthermore, the Trade Secrets Act (18 U.S.C. 1905) prohibits federal employees from disclosing information defined in that section without authorization and imposes personal sanctions on employees who do so. Per CBP policy, all disclosures must be accounted for in CBP's system.**

If [Agency/Office Name] is interested in obtaining access for certain of its employees who have a specific need for this data in connection with their official duties, please carefully review the attached documents and, if appropriate, return a completed request letter, along with a CBP Form 7300 for each employee for whom you seek access to ATS-P. CBP will promptly review your request and provide access, as appropriate, following the completion of all required CBP training and other conditions for access.

If you have any questions, please contact ( b6 ) at ( b2 )

Sincerely,

[Executive Director, National Targeting and Security]

Enclosure [Field Guidelines for Use and Disclosure of PNR]

( b6 )

From: Sales, Nathan

Sent: Wednesday, January 03, 2007 10:49 AM

To: Rosenzweig, Paul; Baker, Stewart; ( b6 ) White, Brian M; Gus.Coldebella ( b2 )  
Kathryn.Wheelbarger ( b2 ) Levy, Andrew

Subject: Re: Analysis: Dems slam border screening rules

[ b5 ]

-----  
Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Rosenzweig, Paul

To: Sales, Nathan; Baker, Stewart; ( b6 ) White, Brian M; 'Coldebella, Gus' ( b2 )  
'Wheelbarger, Kathryn' ( b2 ) Levy, Andrew

Sent: Wed Jan 03 10:42:39 2007

Subject: RE: Analysis: Dems slam border screening rules

[ b5 ]

P

Paul Rosenzweig

[ b2 ]

-----  
From: Sales, Nathan

Sent: Wednesday, January 03, 2007 9:51 AM

To: Baker, Stewart; Rosenzweig, Paul; ( b6 ) White, Brian M; 'Coldebella, Gus'; Wheelbarger, Kathryn; Levy, Andrew

Subject: RE: Analysis: Dems slam border screening rules

[  
b5  
] ) Thanks very much.

Also, I'm attaching a copy of Chairman Thompson's comments on ATS.

Best regards.

NAS

Nathan A. Sales

Deputy Assistant Secretary for Policy Development

Department of Homeland Security

( b2 )

---

From: Baker, Stewart  
Sent: Tuesday, January 02, 2007 12:13 PM  
To: Rosenzweig, Paul; Bergman, Cynthia  
Cc: Sales, Nathan  
Subject: RE: Analysis: Dems slam border screening rules

( b5 )  
basic thrust of the program.

) These comments really could have been worse. He's endorsed the

Re: Analysis: Dems slam border screening rules

Page 3 of 5

From: Rosenzweig, Paul  
Sent: Tuesday, January 02, 2007 12:08 PM  
To: Baker, Stewart: ( bb )  
Cc: Sales, Nathan  
Subject: RE: Analysis: Dems slam border screening rules

I think we should expect that he will sell everything he writes to the press as a way of enhancing himself.

P

---

From: Baker, Stewart  
Sent: Tue 1/2/2007 12:07 PM  
To: ( bb )  
Cc: Rosenzweig, Paul; Sales, Nathan  
Subject: FW: Analysis: Dems slam border screening rules

Well, that didn't take long ....

I guess we need TPs for when the rest of the press picks up on this.

---

From: Stodder, Seth [mailto:( bb )@AkinGump.com]  
Sent: Tuesday, January 02, 2007 11:46 AM  
To: Baker, Stewart; Rosenzweig, Paul  
Subject: FW: Analysis: Dems slam border screening rules

Looks like the Chairman-to-be might need a little brush-up on some basic Fourth Amendment law . . .

---

From: McComb, Lola  
Sent: Tuesday, January 02, 2007 7:58 AM  
To: Fitzpatrick, Michael; Heimberg, Scott; Lent, Susan; Simmons, John M.; Steele, Bert; Stodder, Seth; Tucker, Jamie  
Subject: Analysis: Dems slam border screening rules

Analysis: Dems slam border screening rules

2007-01-02 10:43 (New York)

By SHAUN WATERMAN

WASHINGTON, Jan. 2 (UPI) -- A computer system that screens those arriving in the United States for potential indicators of terrorist activity is in danger of violating the Fourth Amendment, says the incoming chairman of the House Homeland Security Committee.

In public comments filed Friday on the privacy implications of the Automated Targeting System for Passengers, or ATS-P, operated by U.S. Customs and Border Protection, Rep. Bennie Thompson, D-Miss., expressed several concerns about the system, including the way it makes the travel records of U.S. citizens available to other government agencies.

He accused the agency of creating a "warrantless well of evidence from which any law enforcement, regulatory or intelligence agency could dip at will -- without any probable cause, reasonable suspicion, or judicial oversight." "Without adequate safeguards," he added, routine sharing of the information collected from Americans entering the country "may constitute violations of the U.S. Constitution's Fourth Amendment guarantee against unreasonable searches and seizures."

Some observers predicted ATS-P would become the poster child for concerns on Capitol Hill about the privacy and civil liberties impact of post-Sept. 11 measures aimed at interdicting terrorist travel.

ATS-P "is teed up to be the central figure in a round of high-profile hearings," said Jim Harper, director of information policy studies at the CATO Institute and a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

ATS-P automatically checks biographical and other data about those arriving in the United States against criminal and terrorism watch-lists, and performs a so-called terrorism risk assessment for each one. The records of incoming passengers matching a watch-list entry or assessed as a terrorist risk are reviewed by officials at the Department of Homeland Security's National Targeting Center -- and they may be flagged for additional scrutiny by immigration inspectors at ports of entry.

Officials say the system has resulted in several suspected terrorists and other malefactors being turned away or apprehended.

In one case a Jordanian national -- flagged by ATS-P in July 2003 and denied entry after questioning at O'Hare International Airport in Chicago, even though he had a valid visa -- blew himself up in a huge car bomb outside an Iraqi police station 18 months later.

"No one knows what he was going to do in the United States, why he wanted to come in or what he was planning," said Department of Homeland Security Assistant Secretary Stewart Baker.

Baker revealed newly cleared details of two such cases at a little-reported think tank privacy seminar just before Christmas. "Personally, I'm actually grateful that we don't know and that we didn't have a chance to find out," he told the seminar, at the Center for Strategic and International Studies.

"It's nice for Baker," said Harper, another participant in the seminar. "He can reach into the lockbox of secret homeland security information and bring out the best stories and spring them on us.

"But I don't think anecdote is a good basis for policy."

Former U.S. Customs and Border Protection Commissioner Robert Bonner told United Press International that ATS-P was "a vital tool ... (that) has actually made the United States safer" from international terrorism.

With 87 million arriving airline passengers every year, Bonner said, the problem was "how to expedite most of them through the airports, concentrating on those who are identified as a potential risk."

Bonner said the terrorism risk assessment was conducted in the light of a secret and constantly updated set of factors -- travel or other behavior patterns that are thought to be indicators of terrorist activities.

"It's strategic intelligence about who the enemy is and how they travel," he said, declining to comment further.

Baker said part of the assessment was so-called link analysis, looking for

(b2)(c)



credit card or telephone number associated with previously identified terrorist suspects or journeys.

Thompson stated in his filing that "Oral briefings by (Department of Homeland Security) officials have clarified that ATS-P is neither a scoring nor a data-mining process; they have described the assessment as a "flag/no flag" result based on a "links analysis," i.e., looking at links between (travel, identity and other) data ... and known or suspected terrorist activity.

"They have explained that the relevant factors are determined by counter-terrorism experts and as such, are constantly changing as facts on the ground change and more information becomes known.

Thompson said he was "reassured that there is no indiscriminate 'data-dumping' or 'data-mining.'"

But his comments reflect concerns about the other uses that the data, which includes records about the 40 million-plus Americans who arrive at U.S. airports annually -- can be put to.

ATS-P collects and indexes information from the Passenger Name Record, or PNR -- an airline database that includes telephone and credit card numbers, seating and meal preferences, and the names of others traveling in the same party.

"At a minimum," states Thompson in his comments, "any further dissemination of this extensive personal data, either on (U.S. Customs and Border Protection) initiative or upon request, must be documented regarding who is the requestor, what is the legal justification for receiving the data, for what purpose will the data be used, and how it will be protected from further disclosure.

"No such safeguards appear" to exist at the moment, he concludes in the comments, filed on the last day that the ATS-P system of records notice -- a regulatory filing required by the Privacy Act -- was open for public comment. The notice says that ATS-P data will be maintained for 40 years and that sharing it with other law enforcement and government agencies -- either at their request or at customs own initiative -- is a routine use.

Thompson charges the ATS-P notice "does not adequately distinguish between (Custom and Border Protection's) legal authority and processes ... to screen cargo from its legal authority and processes to screen passengers."

"Further, it does not distinguish between its different treatment options for foreign citizens flagged as high risk and high-risk U.S. citizens, whom (Custom and Border Protection) has no authority to exclude from the United States."

--  
Copyright 2007 by United Press International  
All rights reserved.

--  
-0- Jan/02/2007 15:43 GMT

---

**IRS Circular 230 Notice Requirement:** This communication is not given in the form of a covered opinion. within the meaning of Circular 230 issued by the United States Secretary of the Treasury. Thus, we are required to inform you that you cannot rely upon any tax advice contained in this communication for the purpose of avoiding United States federal tax penalties. In addition, any tax advice contained in this communication may not be used to promote, market or recommend a transaction to another party.

The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. If you have received this communication in error, please notify us immediately by e-mail, and delete the original message.

( b6 )

**From:** Scardaville, Michael ( b2 )  
**Sent:** Friday, December 01, 2006 5:05 PM  
**To:** ( b6 )  
**Subject:** FW: ATS Privacy Impact Assessment  
**Attachments:** AP article inaccuracies (12.01.2006).doc



AP article inaccuracies (12.01..  
Of course 2 minutes after I hit send....

Mike  
( b2 )

-----Original Message-----

**From:** Sales, Nathan  
**Sent:** Friday, December 01, 2006 5:03 PM  
**To:** Scardaville, Michael; Agen, Jarrod  
**Cc:** Baker, Stewart; ( b2 ); ( b6 )  
Teufel, Hugo  
**Subject:** RE: ATS Privacy Impact Assessment

Okav. here's the new version with mv edits.(

[ b5 ]

Best,  
NAS

Nathan A. Sales  
Deputy Assistant Secretary for Policy Development Department of Homeland Security  
( b2 )

-----Original Message-----

**From:** Sales, Nathan  
**Sent:** Friday, December 01, 2006 3:18 PM  
**To:** Scardaville, Michael; Agen, Jarrod  
**Cc:** Baker, Stewart; ( b2 ); ( b6 )  
Teufel, Hugo  
**Subject:** RE: ATS Privacy Impact Assessment

Thanks very much, Mike. I will take a crack at revising and then circulate the new version to this group.

Nathan A. Sales  
Deputy Assistant Secretary for Policy Development Department of Homeland Security  
( b2 )

-----Original Message-----

**From:** Scardaville, Michael  
**Sent:** Friday, December 01, 2006 2:55 PM

To: Sales, Nathan; Agen, Jarrod  
Cc: Baker, Stewart; ( b2 ) ( c6 )  
Teufel, Hugo  
Subject: RE: ATS Privacy Impact Assessment

Nathan,

Attached is the side-by-side you requested with input from SCO and PRIV.

Mike  
( b2 )

-----Original Message-----

From: Sales, Nathan  
Sent: Friday, December 01, 2006 8:44 AM  
To: Agen, Jarrod  
Cc: Baker, Stewart; ( b2 ) ( c6 )  
Scardaville, Michael; Teufel, Hugo  
Subject: Re: ATS Privacy Impact Assessment

Yikes. The first four words are factually inaccurate, and the story goes downhill from there. ( b2 )

Mike, will you please go through this article and flag all of the factual inaccuracies, and explain why they are wrong? I'm thinking of a two-column chart; on the left the inaccuracy, on the right the explanation of why. We don't need to look for statements with which we disagree -- only statements that are objectively inaccurate. Thanks very much.

Best,  
NAS

-----  
Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Agen, Jarrod  
To: Sales, Nathan  
Cc: Baker, Stewart; ( b2 ) ( c6 )  
( c2 ) Scardaville, Michael;  
Teufel, Hugo  
Sent: Fri Dec 01 07:37:58 2006  
Subject: RE: ATS Privacy Impact Assessment

Yes. We got several calls last night. This AP story stirred the interest. We had Ahearn and ( b2 ) speak to the reporter, but you can see the angle he took.

AP: Feds rate travelers for terrorism

By MICHAEL J. SNIFFEN Associated Press Writer

WASHINGTON - Without notifying the public, federal agents for the past four years have assigned millions of international travelers, including Americans, computer-generated scores rating the risk they pose of being terrorists or criminals.

The travelers are not allowed to see or directly challenge these risk assessments, which the government intends to keep on file for 40 years.

The scores are assigned to people entering and leaving the United States after computers assess their travel records, including where they are from, how they paid for tickets, their motor vehicle records, past one-way travel, seating preference and what kind of meal they ordered.

The program's existence was quietly disclosed earlier in November when the government put an announcement detailing the Automated Targeting System, or ATS, for the first time in the Federal Register, a fine-print compendium of federal rules. Privacy and civil

liberties lawyers, congressional aides and even law enforcement officers said they thought this system had been applied only to cargo.

The Homeland Security Department notice called its program "one of the most advanced targeting systems in the world." The department said the nation's ability to spot criminals and other security threats "would be critically impaired without access to this data."

Still, privacy advocates view ATS with alarm. "It's probably the most invasive system the government has yet deployed in terms of the number of people affected," David Sobel, a lawyer at the Electronic Frontier Foundation, a civil liberties group devoted to electronic data issues, said in an interview.

Government officials could not say whether ATS has apprehended any terrorists. Customs and Border Protection spokesman Bill Anthony said agents refuse entry to about 45 foreign criminals every day based on all the information they have. He could not say how many were spotted by ATS.

A similar Homeland Security data-mining project, for domestic air travelers \_ now known as Secure Flight \_ caused a furor two years ago in Congress. Lawmakers barred its implementation until it can pass 10 tests for accuracy and privacy protection.

In comments to the Homeland Security Department about ATS, Sobel said, "Some individuals will be denied the right to travel and many the right to travel free of unwarranted interference as a result of the maintenance of such material."

Sobel said in the interview the government notice also raises the possibility that faulty risk assessments could cost innocent people jobs in shipping or travel, government contracts, licenses or other benefits.

The government notice says ATS data may be shared with state, local and foreign governments for use in hiring decisions and in granting licenses, security clearances, contracts or other benefits. In some cases, the data may be shared with courts, Congress and even private contractors.

"Everybody else can see it, but you can't," Stephen Yale-Loeher, an immigration lawyer who teaches at Cornell Law school, said in an interview.

But Jayson P. Ahern, an assistant commissioner of Homeland Security's Customs and Border Protection agency, said the ATS ratings simply allow agents at the border to pick out people not previously identified by law enforcement as potential terrorists or criminals and send them for additional searches and interviews. "It does not replace the judgments of officers," Ahern said in an interview Thursday.

This targeting system goes beyond traditional border watch lists, Ahern said. Border agents compare arrival names with watch lists separately from the ATS analysis.

In a privacy impact assessment posted on its Web site this week, Homeland Security said ATS is aimed at discovering high-risk individuals who "may not have been previously associated with a law enforcement action or otherwise be noted as a person of concern to law enforcement."

Ahern said ATS does this by applying rules derived from the government's knowledge of terrorists and criminals to the passenger's travel patterns and records.

For security reasons, Ahern declined to disclose any of the rules, but a Homeland Security document on data-mining gave an innocuous example of a risk assessment rule: "If an individual sponsors more than one fiancée for immigration at the same time, there is likelihood of immigration fraud."

In the Federal Register, the department exempted ATS from many provisions of the Privacy Act designed to protect people from secret, possibly inaccurate government dossiers. As a result, it said travelers cannot learn whether the system has assessed them. Nor can they see the records "for the purpose of contesting the content."

Toby Levin, senior adviser in Homeland Security's Privacy Office, noted that the department pledged to review the exemptions over the next 90 days based on the public

comment received. As of Thursday, all 15 public comments received opposed the system outright or criticized its redress procedures.

The Homeland Security privacy impact statement added that "an individual might not be aware of the reason additional scrutiny is taking place, nor should he or she" because that might compromise the ATS' methods.

Nevertheless, Ahern said any traveler who objected to additional searches or interviews could ask to speak to a supervisor to complain. Homeland Security's privacy impact statement said that if asked, border agents would hand complaining passengers a one-page document that describes some, but not all, of the records that agents check and refers complaints to Custom and Border Protection's Customer Satisfaction Unit.

Homeland Security's statement said travelers can use this office to obtain corrections to the underlying data sources that the risk assessment is based on. "There is no procedure to correct the risk assessment and associated rules stored in ATS as the assessment ... will change when the data from the source system(s) is amended."

"I don't buy that at all," said Jim Malmberg, executive director of American Consumer Credit Education Support Services, a private credit education group. Malmberg noted how hard it has been for citizens, including members of Congress and even infants, to stop being misidentified as terrorists because their names match those on anti-terrorism watch lists.

Homeland Security, however, is nearing an announcement of a new effort to improve redress programs and the public's awareness of them, according to a department privacy official, who requested anonymity because the formal announcement has not been made.

The department says that 87 million people a year enter the country by air and 309 million enter by land or sea. The government gets advance passenger and crew lists for all flights and ships entering and leaving and all those names are entered into the system for an ATS analysis, Ahern said. He also said the names of vehicle drivers and passengers are entered when they cross the border and Amtrak is voluntarily supplying passenger data for trains to and from Canada.

Ahern said that border agents concentrate on arrivals more than on departures because their resources are limited.

"If this catches one potential terrorist, this is a success," Ahern said.

-----Original Message-----

From: Sales, Nathan  
Sent: Friday, December 01, 2006 7:23 AM  
To: Agen, Jarrod  
Cc: Baker, Stewart; ( J2 ) ( hb )  
Scardaville, Michael; Teufel, Hugo  
Subject: ATS Privacy Impact Assessment

Jarrod, I imagine y'all know about this already, but please see the attached note from Mike Scardaville. Apparently ABC did a story on the ATS PIA. You can imagine their angle. Good thing we pulled together those talkers last week.

-----  
Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Scardaville, Michael ( )  
To: Sales, Nathan ( )  
Sent: Fri Dec 01 07:13:09 2006  
Subject: Re: "DHS Seizing / Downloading Laptops"

Me neither, but if I recall correctly the talkers ( [ hb ] )

On another note, ABC just had a short story about the ATS PIA/SORN expressing surprise that we're doing this.

-----  
Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Sales, Nathan ( )  
To: Scardaville, Michael ( )  
( ) Rosenzweig, Paul ( )  
Cc: Sales, Nathan ( )  
Sent: Fri Dec 01 07:02:08 2006  
Subject: Re: "DHS Seizing / Downloading Laptops"

Thanks, Mike. I'm not surprised that CBP is tight-lipped about this. Law enforcement agencies tend to keep quiet about investigations and methods.

-----  
Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Scardaville, Michael ( )  
To: ( ) Rosenzweig, Paul ( )  
Scardaville, Michael ( )  
Cc: Sales, Nathan ( )  
Sent: Fri Dec 01 06:20:21 2006  
Subject: Re: "DHS Seizing / Downloading Laptops"

Thanks ( )

I have CBP's talkers at the office and will send them once I get in. However, they don't say much ( ) Unfortunately we've been )  
( )  
plying phone tag.

Mike

-----  
Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Koumans, Mark <KoumansM@state.gov>  
To: Rosenzweig, Paul ( ) Scardaville, Michael  
( )  
Cc: Sales, Nathan ( )  
Sent: Fri Dec 01 06:09:51 2006  
Subject: RE: "DHS Seizing / Downloading Laptops"

Laptops give up their secrets to U.S. customs agents

By Joe Sharkey The New York Times

Published: October 24, 2006

NEW YORK A lot of business travelers are walking around with laptops that contain private corporate information that their employers really do not want outsiders to see.

Until recently, their biggest concern was that someone might steal the laptop. But now there's a new worry - that the laptop will be seized or its contents scrutinized at U.S.

customs and immigration checkpoints upon entering the United States from abroad.

Although much of the evidence for the confiscations remains anecdotal, it's a hot topic this week among more than a thousand corporate travel managers and travel industry officials meeting in Barcelona at a conference of the Association of Corporate Travel Executives.

Last week, an informal survey by the association, which has about 2,500 members worldwide, indicated that almost 90 percent of its members were not aware that customs officials have the authority to scrutinize the contents of travelers' laptops and even confiscate laptops for a period of time, without giving a reason.

"One member who responded to our survey said she has been waiting for a year to get her laptop and its contents back," said Susan Gurley, the group's executive director. "She said it was randomly seized. And since she hasn't been arrested, I assume she was just a regular business traveler, not a criminal."

Appeals are under way in some cases, but the law is clear. "They don't need probable cause to perform these searches under the current law," said Tim Kane, a Washington lawyer who is researching the matter for corporate clients. "They can do it without suspicion or without really revealing their motivations."

In some cases, random inspections of laptops have yielded evidence of possession of child pornography. Laptops may be scrutinized and subject to a "forensic analysis" under the so-called border search exemption, which allows searches of people entering the United States and their possessions "without probable cause, reasonable suspicion or a warrant," a federal court ruled in July. In that case, the hard drive of a man's laptop was found to contain images of child pornography.

No one is defending criminal possession of child pornography, or even suggesting that the government has nefarious intent in conducting random searches of a traveler's laptop, Gurley said.

"But it appears, from information we have, that agents have a lot of discretion in doing these searches, and that there's a whole spectrum of reasons for doing them," she added.

The association is asking the government for better guidelines so corporate policies on traveling with proprietary information can be re-evaluated. It is also asking whether corporations need to reduce the proprietary data that travelers carry.

"We need to be able to better inform our business travelers what the processes are if their laptops and data are seized - what happens to it, how do you get it back," Gurley said.

She added: "The issue is what happens to the proprietary business information that might be on a laptop. Is information copied? Is it returned? We understand that the U.S. government needs to protect its borders. But we want to have transparent information so business travelers know what to do. Should they leave business proprietary information at home?"

Besides the possibility for misuse of proprietary information, travel executives are also concerned that a seized computer, and the information it holds, becomes unavailable to its user for a time. One remedy some companies are considering is telling travelers returning to the United States with critical information on their laptop hard drives to encrypt the data and e-mail it to themselves, which at least preserves access to the information, although it does not guard its privacy.

In one recent case in California, a federal court went against the trend, ruling that laptop searches were a serious invasion of privacy.

"People keep all sorts of personal information on computers," the court ruling said, citing diaries, personal letters, financial records, lawyers' confidential client information and reporters' notes on confidential sources.

That court ruled, in that specific case, that "the correct standard requires that any border search of the information stored on a person's electronic storage device be based, at a minimum, on a reasonable suspicion."

In its informal survey last week, the association also found that 87 percent of its members would be less likely to carry confidential business or personal information on international trips now that they were aware of how easily laptop contents could be searched.

"We are telling our members that they should prepare for the eventuality that this could happen, and they have to think more about how they handle proprietary information," Gurley said. "Potentially, this is going to have a real effect on how international business is conducted."

---

From: Rosenzweig, Paul ( b2 )  
Sent: Wednesday, November 29, 2006 01:00  
To: ( b2 ) : Scardaville, Michael  
Cc: Sales, Nathan  
Subject: RE: "DHS Seizing / Downloading Laptops"

Did I respond to this already? It's a court case in California, not a policy.

If you need more info, my colleague Nathan Sales can provide

P

Paul Rosenzweig

( b2 )  
( b2 )

---

From: Koumans, Mark [mailto:KoumansM@state.gov]  
Sent: Wednesday, November 22, 2006 11:08 AM  
To: Scardaville, Michael  
Cc: Rosenzweig, Paul  
Subject: "DHS Seizing / Downloading Laptops"

Mike -

Do you have anything official - press guidance, testimony - that addresses these bizarre allegations in the press about CBP seizing / downloading from people's laptops at the port of entry? There have been some stories in international media, and like those stories about travelers getting the 3rd degree, they may be taking a life of their own.

The German business community, not unexpectedly, sees this as a commercial espionage issue. They also saw the SWIFT imbroglio as a USG commercial espionage attempt to learn about the prices European companies (e.g., Airbus) charge their customers.



Would welcome anything you can give me on the subject. The German business community has a way of getting to the Economic Minister very quickly. Then he calls the Ambassador.

Mark

Mark Koumans  
First Secretary for Counterterrorism, Homeland Security and Legal  
Affairs  
U.S. Embassy Berlin  
( 02 )



## ARTICLE 29 Data Protection Working Party

### Automated Targeting System (ATS)

Version 21/03/2007

PNR subgroup

#### **New ATS (state of play on March 21, 2007)**

Nov. 2, 2006: DHS Chief Privacy Officer publishes the new automated targeting system (ATS) in the US Federal Register

Nov. 30, 2006: PNR subgroup sends comments and questions on ATS to the DHS Chief Privacy Officer

Dec. 30, 2006: comment period expires

Jan. 12, 2007: EU Commission informs PNR subgroup about a DHS letter saying that the proposed "System of Record Notice (SORN) and the Privacy impact Assessment (PIA) recently released by DHS describe the general operation of ATS. They in no way supersede or otherwise alter the PNR Agreement...DHS continues to govern its access to and use of PNR from European flights consistent with the October 2006 Agreement, the Undertakings and my October 2006 letter... This includes the storage and processing of data in ATS"

February 7, 2007: The DHS Chief Privacy Officer informs the PNR subgroup that he is still reviewing several hundred comments and that after this review a new ATS will be published in the Federal Register.

**The proposed new ATS has not yet become effective nor is it clear when a final decision will be taken and how the final version will look like.**

**Problems arising from the current version of the proposed ATS:**

The proposed ATS raises several questions and seems in some points not in line with the PNR Agreement and in particular the Undertakings given in 2004 by the US Government.

- The ATS is an analytical tool to screen all passengers entering or leaving the US and not only those on watch lists. Although it does not profile on race, ethnicity or arbitrary assumptions it is not clear in how far the system can be used for general profiling purposes and analysing behavioural patterns.
- The list of data elements goes beyond the 34 elements mentioned in the annex of the PNR Agreement: 1.) Identifiers for free tickets, 2.) number of bags, 3.) number of bags on each segment, 4.) voluntary and involuntary upgrades. In addition to that the restrictions regarding frequent flyer information (data element 11: data related to miles flown and addresses) are missing.
- Unrestricted onward transfer to wide ranging recipients would considerably violate the Undertakings in particular Undertaking 29
- storage period (up to 40 years) would violate Undertaking 15 restricting the storage period to 3.5 years.

The ATS as published in the Federal Register does not mention the PNR Agreement and so it is ambiguous whether it also covers PNR data derived from European data

bases. For that reason DHS' letter of January 2007 was helpful to the extent that it makes clear that it is not interfering with the current PNR Interim Agreement.

However, even in case the current ATS proposal adopted in its present version would not interfere with the PNR Agreement serious concerns remain:

The US has already unilaterally given notice to the EU amending the data elements in the Undertakings, raising concerns about the continued expansion in the direction of the wider extent of the ATS. The increase in data elements without effective consultation is a significant concern.

In order to respect the EU PNR Agreement and the Undertakings the US would need two PNR regimes due to the fact that the ATS contains less stringent data protection rules than the PNR Agreement: One PNR regime would cover PNR data stemming from European data bases and one for PNR data derived from other regions.

Among others the following aspects of such a situation need to be addressed:

How, for example, will data be separated if passengers enter the US once from Europe and once from a non-EU country? Will their record created from the EU PNR and their other record that would be subject to the wider ATS provisions be kept separately, or merged?

What about data of passengers flying to the US that are stored in non-European Reservation systems and transferred to DHS?

How many data elements are stored if a passenger enters the US via a third country using a non-European airline given the fact that the proposed ATS foresees to store more data elements than the current PNR Agreement?

If there are not two separate regimes what about the storage period, right of access and rectification if some PNR data fall under the PNR Agreement others, however, under the ATS?

How are passengers going to be informed that their data may be subject to different data protection regimes given the fact that European carriers are only obliged to inform about the details of the current PNR Agreement?

**These issues require further attention by all stakeholders and should be raised During the ongoing negotiations between the EU and the US in order to clarify them prior to the conclusion of the follow-up agreement.**

**Issue: PNR Retention Period**

b5, b7E

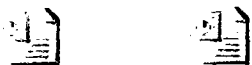
b7E

b5, b7E

[ b6 ]

From: ( b6 )  
Sent: Tuesday, October 24, 2006 2:11 PM  
To: ( b6 )  
Subject: Fw: OMB meeting - ATS data flow chart

Attachments: ATS Flowchart - OMB 10-24-2006 (cc comments 10-24-06) - dd edits.ppt; ATS Flowchart - OMB 10-24-2006.ppt



ATS Flowchart - OMB 10-24-2006...  
ATS Flowchart - OMB 10-24-2006...

Any comments? I will ask them to send to CPO in the meantime.

( b6 )  
Office of Chief Counsel  
U.S. Customs and Border Protection

[ b2, b6 ]

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

----- Forwarded by KRISTIN L DUBELIER/NE/USCS on 10/24/2006 02:10 PM -----

( b2, b6 )  
( b2, b6 )  
10/24/2006 02:03 PM  
chart

To: ( b2, b6 )  
cc: ( b2, b6 )  
Subject: Re: OMB meeting - ATS data flow  
(Document link: ( b6 )

( b6 )

Some answers:

[ b5 ]

(See attached file: ATS Flowchart - OMB 10-24-2006 (cc comments 10-24-06) - (b6)edits.ppt)

( b6 )  
Office of Field Operations  
Customs and Border Protection  
[ b2 ]

( b2, b6 )  
chart  
[ b6 ]  
10/24/2006 10:35  
AM

To: ( b2, b6 )  
CC: ( b2, b6 )  
Subject: Re: OMB meeting - ATS data flow  
(Document link: ( b6 )

Couple comments/questions:

[ b5 ]

Can you clean up the slides as necessary and resend them to me to share with Ellen?

( b6 )  
Office of Chief Counsel  
U.S. Customs and Border Protection  
[ b2, b6 ]

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

( b2, b6 )  
( b2, b6 )  
10/24/2006 10:18  
AM

To: ( b2, b6 )  
CC: ( b2, b6 )  
Subject: OMB meeting - ATS data flow chart

( b6 )

Here's the powerpoint (basic slides on ATS data flow) for tomorrow's meeting with OMB.

(See attached file: ATS Flowchart - OMB 10-24-2006.ppt)

Thanks,

[ b6 ]

Office of Field Operations  
Customs and Border Protection

[ b2 ]

( b6 )

**From:** ( b2, b6 )  
**Sent:** Thursday, November 02, 2006 4:03 PM  
**To:** ( b6 )  
**Subject:** FW: PNR

( b6 )  
Senior Counsel  
Department of Homeland Security  
Office of the General Counsel  
NAC-4, Washington, D.C. 20528

[ b2 ]

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete the message. Thank you.

**From:** ( b6 )  
**Sent:** Thursday, November 02, 2006 3:58 PM  
**To:** Coldebella, Gus  
**Subject:** RE: PNR

Gus – I have partial answers on the 2 questions that can be answered unclassified:

100% of PNR is screened according to rules that result in a risk assessment for each traveler.

PNR is screened against the ATS-P database, which contains the following:

- Advance Passenger Information System (APIS)
- Border Crossing, TECS
- Land Border Crossing, TECS
- I94, TECS<sup>[1]</sup>
- Personal Search, TECS
- Secondary Referrals, TECS
- Secondary Referrals/Land, TECS
- Secondary Referrals/CBP/ICE, TECS
- Seized Property, TECS
- Seized Vehicle, TECS
- USVISIT, TECS<sup>[2]</sup>
- NCIC III, TECS
- Air Craft Arrivals, ACS
- PNR (Approximately 100 airlines), Airline Reservations Systems



- Visa, TECS
- Enforcement Subjects: Person, TECS
- Enforcement Subjects: Business, TECS
- Enforcement Subjects: Address, TECS

## PNR Data Elements

Original 39 Data Elements	EU Negotiated 34 Data Elements
<ol style="list-style-type: none"> <li>1. PNR record locator code</li> <li>2. Date of reservation</li> <li>3. Date(s) of intended travel</li> <li>4. Name</li> <li>5. Other names on PNR</li> </ol>	<ol style="list-style-type: none"> <li>1. PNR record locator code</li> <li>2. Date of reservation</li> <li>3. Date(s) of intended travel</li> <li>4. Name</li> <li>5. Other names on PNR</li> </ol>
<ol style="list-style-type: none"> <li>6. Number of travelers on PNR</li> <li>7. Seat information</li> <li>8. Address</li> <li>9. All forms of payment information</li> <li>10. Billing address</li> <li>11. Contact telephone numbers</li> <li>12. All travel itinerary for specific PNR</li> <li>13. Frequent flyer information (limited to miles flown and address(es))</li> <li>14. Travel agency</li> <li>15. Travel agent</li> <li>16. Code share PNR information</li> <li>17. Travel status of passenger</li> <li>18. Split/Divided PNR information</li> <li>19. Identifiers for free tickets</li> <li>20. One-way tickets</li> <li>21. Email address</li> <li>22. Ticketing field information</li> <li>23. ATFQ fields</li> <li>24. General remarks</li> <li>25. Ticket number</li> <li>26. Seat number</li> <li>27. Date of ticket issuance</li> <li>28. Any collected APIS information</li> <li>29. No show history</li> <li>30. Number of bags</li> <li>31. Bag tag numbers</li> <li>32. Go show information</li> <li>33. Number of bags on each segment</li> <li>34. OSI information</li> <li>35. SSI information</li> <li>36. SSR information</li> <li>37. Voluntary/involuntary upgrades</li> <li>38. Received from information</li> <li>39. All historical changes to the PNR</li> </ol>	<ol style="list-style-type: none"> <li>6. Address</li> <li>7. All forms of payment information</li> <li>8. Billing address</li> <li>9. Contact telephone numbers</li> <li>10. All travel itinerary for specific PNR</li> <li>11. Frequent flyer information (limited to miles flown and address(es))</li> <li>12. Travel agency</li> <li>13. Travel agent</li> <li>14. Code share PNR information</li> <li>15. Travel status of passenger</li> <li>16. Split/Divided PNR information</li> <li>17. Email address</li> <li>18. Ticketing field information</li> <li>19. General remarks</li> <li>20. Ticket number</li> <li>21. Seat number</li> <li>22. Date of ticket issuance</li> <li>23. No show history</li> <li>24. Bag tag numbers</li> <li>25. Go show information</li> <li>26. OSI information</li> <li>27. SSI/SSR information</li> <li>28. Received from information</li> <li>29. All historical changes to the PNR</li> <li>30. Number of travelers on PNR</li> <li>31. Seat information</li> <li>32. One-way tickets</li> <li>33. Any collected APIS information</li> <li>34. ATFQ fields</li> </ol>

It's my understanding that your 4 questions are specifically answered in a memo from CBP to I&A. It is classified such that I could not get it remotely from CBP, but ( b6 ) working to get you a copy from I&A. Please let me know if you want me to come by to discuss further ( b6 )

( b6 )  
Senior Counsel  
Department of Homeland Security  
Office of the General Counsel  
NAC-4, Washington, D.C. 20528

[ b2 ]

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete the message. Thank you.

**From:** Coldebella, Gus  
**Sent:** Wednesday, November 01, 2006 6:52 PM  
**To:** ( b6 )  
**Subject:** PNR

Can you brief me and provide some talkers on the following points tomorrow?

1. Against which databases is it screened?
2. How is it screened (100% of the data, random selections, targeting algorithms, etc?) 3. ( b7E )
4. [ b7E ]

Gus P. Coldebella  
Deputy General Counsel  
Office of the General Counsel  
U.S. Department of Homeland Security  
[ b2 ] (office)  
(mobile)

- (1) ATS receives I94 data via TECS. TECS receives I94 data directly from the source ICE system.
- (2) ATS receives USVISIT data via TECS. TECS receives US VISIT data directly from USVISIT

( b2 )

**Issue: APIS Retention Period**

**Background:** Currently under the TECS SORN there is no definitive retention period for API data.

[ b5, b7E ]

b7E

Long-term retention period statement for the PIA (10/24/06):

[ b5 ]

Chief Counsel revision (10/25/06):

[ b5 ]

“Before 9/11 no agency of the U.S. government systematically analyzed terrorists’ travel strategies. Had they done so, they could have discovered the ways in which the terrorist predecessors to al Qaeda had been systematically but detectably exploiting weaknesses in our border security since the early 1990s. “

See 9-11 Commission Report at p. 384

<http://www.gpoaccess.gov/911/pdf/sec12.pdf>

---

**“Recommendation: Targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.**

Since 9/11, significant improvements have been made to create an integrated watchlist that makes terrorist name information available to border and law enforcement authorities. However, in the already difficult process of merging border agencies in the new Department of Homeland Security—“changing the engine while flying” as one official put it<sup>34</sup>—new insights into terrorist travel have not yet been integrated into the front lines of border security.

The small terrorist travel intelligence collection and analysis program currently in place has produced disproportionately useful results. It should be expanded. [THIS IS ATS-P] Since officials at the borders encounter travelers and their documents first and investigate travel facilitators, they must work closely with intelligence officials.

Internationally and in the United States, constraining terrorist travel should become a vital part of counterterrorism strategy. Better technology and training to detect terrorist travel documents are the most important immediate steps to reduce America’s vulnerability to clandestine entry. Every stage of our border and immigration system should have as a part of its operations the detection of terrorist indicators on travel documents. Information systems able to authenticate travel documents and detect potential terrorist indicators should be used at consulates, at primary border inspection lines, in immigration services offices, and in intelligence and enforcement units. [THIS IS ALSO ATS-P] All frontline personnel should receive some training. Dedicated specialists and ongoing linkages with the intelligence community are also required. The Homeland Security Department’s Directorate of Information Analysis and Infrastructure Protection should receive more resources to accomplish its mission as the bridge between the frontline border agencies and the rest of the government counterterrorism community.”

See 9-11 Commission Report at p. 385

<http://www.gpoaccess.gov/911/pdf/sec12.pdf>

---

**“Recommendation: The U.S. border security system should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with systemwide goals in mind. Extending those standards among other governments could dramatically strengthen America and the world’s collective ability to intercept individuals who pose catastrophic threats.**

We advocate a system for screening, not categorical profiling. A screening system looks for particular identifiable suspects or indicators of risk. It does not involve guesswork about who might be dangerous. It requires frontline border officials who have the tools and resources to establish that people are who they say they are, intercept identifiable suspects, and disrupt terrorist operations. “ [THIS IS ATS-P]

See 9-11 Commission Report at p. 387  
<http://www.gpoaccess.gov/911/pdf/sec12.pdf>

---

**“A modern border and immigration system should combine a biometric entry-exit system with accessible files on visitors and immigrants, along with intelligence on indicators of terrorist travel.” [This is ATS-P]**

See 9-11 Commission Report at p. 389  
<http://www.gpoaccess.gov/911/pdf/sec12.pdf>

---

[Additionally, we know that the 9-11 Commission Staff knew about ATS-P because they extensively interviewed senior CBP officials, among many others, and were told about ATS-P. Moreover, the 9-11 Commission Staff Report on Terrorist Travel

**“And the National Targeting Center, assisted by the new Terrorist Screening Center, provides information support to inspectors at ports of entry so that they can make more informed decisions about potential terrorists and harmful cargo attempting to enter the United States.”**

See  
9-11 Commission Staff Report on Terrorist Travel at p. 164  
[http://www.9-11commission.gov/staff\\_statements/911\\_TerrTrav\\_Monograph.pdf](http://www.9-11commission.gov/staff_statements/911_TerrTrav_Monograph.pdf)

Office of Inspector General  
Office of Investigations

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



Homeland  
Security

January 25, 2007

MEMORANDUM FOR: Traci Lembke, Director  
Office of Professional Responsibility  
U.S. Immigration and Customs Enforcement

FROM: Elizabeth M. Redman *[Signature]*  
Assistant Inspector General for Investigations

SUBJECT: *Referral of* *OIG Complaint Number: R07-CBP-ATL-04238*

This matter is being referred to you for appropriate action and disposition in accordance with your organization's applicable rules, regulations, policies, and procedures. You are not required to include this matter in your monthly report to the Office of Inspector General (OIG), nor are you required to provide the OIG with a copy of your findings and/or final action concerning this matter.

If you have any questions concerning this matter, you may contact me at (202) 254-4100, or Gerald L. Coffman, Deputy Assistant Inspector General for Investigations, Headquarters Operations, at ( b2 )



Office of Inspector General  
Office of Investigations

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



Homeland  
Security

January 08, 2007

[ b6  
b7(C) ]

Re: OIG Complaint Number: 0704238

Dear ( b6 )

This is to acknowledge receipt of the information you provided to the Department of Homeland Security (DHS) Office of Inspector General (OIG), on January 8, 2007 . It is the policy of the DHS OIG to thoroughly review all complaints forwarded to this office. Accordingly, DHS OIG officials will review the information you provided to determine the appropriate course of action.

We appreciate you bringing this to the attention of the Office of Inspector General.

Sincerely,

[ b6 ]

**DEPARTMENT OF HOMELAND SECURITY  
OFFICE OF INSPECTOR GENERAL - OFFICE OF INVESTIGATIONS  
CASE RECORD**

COMPLAINT: R07-CBP-ATL-04238      STATUS:      CLOSE  
AGENT:      RECVD METHOD: MAIL      DATE RECEIVED: 01/08/07  
DATE ENTERED: 01/08/07      ENTERED BY: [ b6  
b7(C) ]      CROSS REFERENCE:  
DATE AGT ASSIGNED:      INVESTIGATION TYPE:      DHS Employee  
Misconduct - Official -  
Law enforcement  
intelligence  
DHS Agency: CBP      DISPOSITION DATE: 01/08/07

**DISPOSITION NOTIFICATION BOX: 1-Referred, no reply**

<b>SUBJECT 1</b>	Automated Targeting System	<b>TITLE</b>	<b>TYPE:</b> DHS component
DHS Agency:		DOB:	SSN:
ADDRESS(W):			
ADDRESS(H):			
CITY/STATE/ZIP	HPhone/WPhone:		

<b>SUBJECT 2</b>		<b>TITLE:</b>	<b>TYPE:</b>
DHS Agency:		DOB:	SSN:
ADDRESS(W):			
ADDRESS(H):			
CITY/STATE/ZIP	HPhone/WPhone		

**NARRATIVE OF THE ALLEGATION**

Complainant alleges that Automated Targeting System (ATS) violates several United States laws which constitutes an invasion of privacy.

<b>COMPLAINANT:</b> [ b6 b7C ]	<b>STATUS:</b>
ADDRESS:	
CITY/STATE/ZIP	
TELEPHONE      H:	W:

## CASE NOTES

**File Number:** R07-CBP-ATL-04238

**Note:** -In response to triple FOIA request from ACLU, Electronic Frontier Foundation and Associated Press Washing  
Bureau, copy of file given to O.C. Gramian today. by [ <sup>b6</sup>  
b7C ] on 01/25/2007

-Referral changed from TSA to CBP. by [ <sup>b6</sup>  
b7C ] on 01/25/2007

Enter new notes here

Update Notes

Close

b6  
b7C

December 20, 2006 .

The Honorable Richard L. Skinner  
Inspector General  
Department of Homeland Security  
Washington, DC 20528

In Re: Automated Targeting System

Dear Inspector General Skinner:

I am writing this letter out of deep concern for both the procedure utilized in belated disclosure of the Automated Targeting System; and for the continuing activity of the program that clearly appears to be in violation of several laws of the United States and which constitutes an invasion of the privacy of its citizens.

On November 2, 2006 the Department of Homeland Security (hereinafter DHS) provided notice in the Federal Register of its intent to implement a system of data collection, privacy intrusion, and information retention and distribution known as the Automated Targeting System (hereinafter ATS). The implementation of this program was stated to be December 4, 2006. The obvious intent of DHS was to provide "notice," but at the same time allow *inadequate* time for concerned citizens and groups to object or engage in debate.

The activities of ATS are first and foremost a violation of the Fourth Amendment to the Constitution of the United States. They also invade the privacy of every American that chooses to travel. Beyond those invasions, the formation and implementation of ATS is in clear violation of the laws of the United States.

b6

The Honorable Richard L. Skinner  
December 20, 2006  
Page 2

Title V. Sec. 514(a) and (c) of the 2007 DHS Appropriations law will be violated by ATS: subsection (a) of that section because there has been no procedural reporting, as required, to this already implemented program. Subsection (c) is violated because the targeting is of *all* citizens and is not being restricted to "watch lists."

Moreover, it clearly appears that the very formation of ATS is a violation of the Antideficiency Act, 31 U.S.C. 1341, which contain attendant criminal provisions (see, 31 U.S.C. Secs. 1350, 1519).

The DHS has also attempted improperly to exempt itself from the Privacy Act of 1974 in its formation of ATS.

I ask that your office institute and conduct an investigation immediately, and that appropriate measures be taken to cause the DHS to cease and desist in their illegal intrusions into the lives of American citizens.

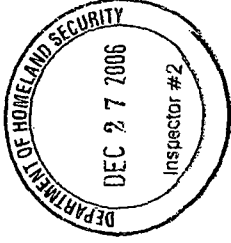
Please do not hesitate to contact me if I can be of further assistance. In the meantime, I remain,

very truly yours,

[  
bb  
b7c  
]



**SECURITY**



The Honorable Richard L. Skinner  
Inspector General  
Department of Homeland Security  
Washington, DC 20528

20528+0000

10/11/2006 10:00 AM

[ ]

b6  
b7c

[ ]

[ ]

b6  
b7c

[ ]



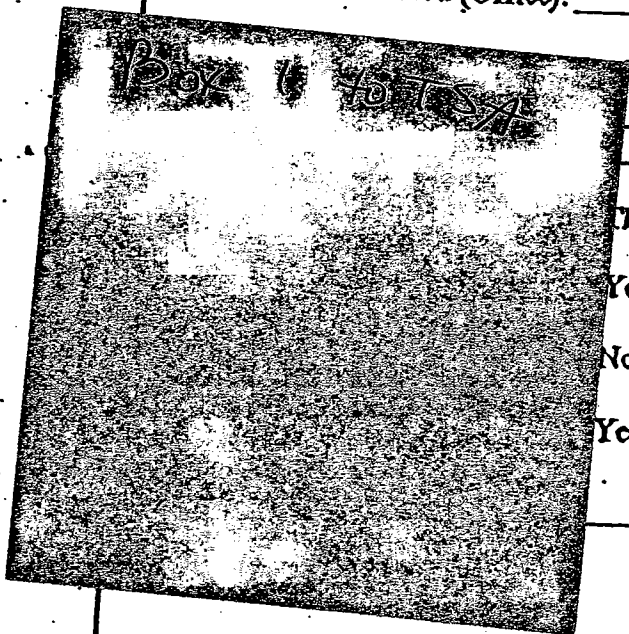
|||



Department of Homeland Security  
Office of Inspector General - Office of Investigations  
Complaint Processing Form

OIG CASE NUMBER: R07 04288

- Hotline (Mail/Email/Fax/Hotline Call/ETC..) Other # \_\_\_\_\_
- Referred by Agency Name and Xref# \_\_\_\_\_
- Field Generated (Office): \_\_\_\_\_



Yes  No

TE: \_\_\_\_\_

Yes Faxed to \_\_\_\_\_ Date \_\_\_\_\_

No \_\_\_\_\_

Yes  No  Date \_\_\_\_\_

Date Ref: \_\_\_\_\_

Classification: Box 1  Box 2  Box 3  Other

CONFIDENTIALITY ISSUE? (Yes)  (No)

COMPLAINANT DHS EMPLOYEE? (Yes)  (No)  (Unk)

Subject Name Queried (List Case Numbers): \_\_\_\_\_

Other Agency Number Queried?  Cross-referenced?

HOTLINE INVESTIGATOR'S INITIALS/DATE: [OK] 1-8-07

COMMENTS: 1/25/07 - Referral changed from TSA to CBP. [OK]

Office of Inspector General  
Office of Investigations

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



Homeland  
Security

January 08, 2007

MEMORANDUM FOR: K. David Holmes, Jr., Assistant Administrator  
Office of Inspection  
Transportation Security Administration

FROM: *for* Elizabeth M. Redman *[Signature]*  
Assistant Inspector General for Investigations

SUBJECT: *Referral of OIG Complaint Number: R07-TSA-ATL-04238*

This matter is being referred to you for appropriate action and disposition in accordance with your organization's applicable rules, regulations, policies, and procedures. You are not required to include this matter in your monthly report to the Office of Inspector General (OIG), nor are you required to provide the OIG with a copy of your findings and/or final action concerning this matter.

If you have any questions concerning this matter, you may contact me at (202) 254-4100, or Gerald L. Coffman, Deputy Assistant Inspector General for Investigations, Headquarters Operations, at ( *b2* )



**Review of CBP Actions Taken to Intercept  
Suspected Terrorists at U.S. Ports of Entry  
Findings and Recommendations**

**Finding: CBP is making progress towards pushing valuable information to Ports of Entry; this may allow supervisory CBP officers to make timely admissibility determinations.**

a.

[ b2 high  
b5  
b7E ]

- In addition, the TSDB displays several vulnerabilities in control over data validity and integrity, according to a recent DOJ OIG report, "Review of the Terrorist Screening Center."

[ b2 high  
b5  
b7E ]

- To assist the POEs in positively identifying incorrectly matched individuals in a timely manner, (

[ b2 high  
b5  
b7E ]

foreign nationals as they enter the country through the U.S. VISIT program. Encouraging travelers not normally subject to U.S. VISIT that are repeatedly referred to secondary, to submit to U.S. VISIT biometric collection, would also enhance the ability of POEs to positively identify incorrectly matched individuals.

Doc 102

*Recommendation: Establish a voluntary program whereby individuals not subject to U.S. VISIT requirements may submit to collection of biometric information to reduce repeated secondary screenings.*

b. Supervisory Discretion at Ports of Entry

- [ b2 high ]
- [ b5 ]
- [ b7 E ]

*Recommendation: Revise the Office of Anti-Terrorism directive to allow limited discretion for the POEs regarding clear incorrectly matched cases. (*

- [ b2 high ]
- [ b5 ]
- [ b7 E ]

**Finding: Increased counterterrorism efforts at ports of entry have negatively impacted traditional CBP missions such as narcotics interdiction and immigration fraud.**

- [ b2 high ]
- [ b5 ]
- [ b7 E ]

- A number of ports report that staffing is a serious problem. Many claim to have a significant number of vacancies with officers regularly working overtime.

*Recommendation: Port staffing needs to be reviewed to determine whether the work force is able to perform CBP's legacy missions along with increased challenges regarding the prevention of terrorism. Vacancies need to be filled.*

**Finding: Inconsistent reporting may be preventing valuable collected information from being processed and analyzed by CBP, DHS, and the Intelligence Community.**

a.

- [Redacted]
- [Redacted]
- [Redacted] b2 high
- [Redacted] b5
- [Redacted] b7E
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

*Recommendation: Develop a policy and procedure.* (

[ b2, 5, 7E ]

**b. Reporting to Intelligence Agencies**

- 
- 
- 
- 
- 

b2 high

b5

b7E

*Recommendation: Develop a clear reporting policy*

[ b2 high, b5, b7E ]

**Finding: An insufficient number** ( ba↑, b5, b7E ]

▪ [ ba high ]  
▪ [ b5 ]  
[ b7E ]

**Recommendation: Ensure that** ( ba high, b5, b7E ]

**Review of CBP Actions Taken to Intercept  
Suspected Terrorists at U.S. Ports of Entry  
Findings and Recommendations**

**Finding: CBP is making progress towards pushing valuable information to Ports of Entry; this may allow supervisory CBP officers to make timely admissibility determinations.**

- a.
  - [ b2 high  
b5  
b7E ]
  - In addition, the TSDB displays several vulnerabilities in control over data validity and integrity, according to a recent DOJ OIG report, "Review of the Terrorist Screening Center."

- [ b2 high  
b5  
b7E ]

- To assist the POEs in making this positive identification of an incorrectly matched individual in a timely manner. (

- [ b2 high  
b5  
b7E ]  
foreign nationals as they enter the country through the U.S. VISIT program. Encouraging travelers not normally subject to U.S. VISIT that are repeatedly referred to secondary, to submit to U.S. VISIT biometric collection, would also enhance the ability of POEs to positively identify incorrectly matched individuals.

*Recommendation: Establish a voluntary program whereby individuals not subject to U.S. VISIT requirements may submit to collection of biometric information to reduce repeated secondary screenings.*

- b. Supervisory Discretion at Ports of Entry

**Finding: Increased counterterrorism efforts at ports of entry have negatively impacted traditional CBP missions such as narcotics interdiction and immigration fraud.**

**Finding: Inconsistent reporting may be preventing valuable collecting information from being processed and analyzed by CBP, DHS, and the Intelligence Community.**

a.

- 
- 
- 
- 
- 
- 
- 
- 

b2 high

b5

b7E

*Recommendation: Develop a policy and procedure (*

[ b2 high, b5, b7E ]

**b. Reporting to Intelligence Agencies**

- [ b2 high
- b5
- b7E
- 
- 
- 

*Recommendation: Develop a clear reporting policy (*

[ b2 high, b5 b7E ]



[  $b_2$  high,  $b_5$ ,  $\gamma E$  ]

**Finding: An insufficient number (**

[  $b_2$  high,  $b_5$ ,  $\gamma E$  ]

• [  $b_2$  high ]  
• [  $b_5$  ]  
• [  $b \gamma E$  ]

**Recommendation: Ensure that (**

[  $b_2$  high,  $b_5$ ,  $b \gamma E$  ]

**Review of CBP Actions Taken to Intercept  
Suspected Terrorists at U.S. Ports of Entry  
Findings and Recommendations**

**Finding: CBP is making progress towards pushing valuable information from central repositories to Ports of Entry; this may smooth the flow of arriving passengers and reduce the burden on POE secondary inspectors and the NTC staff.**

a.

▪

b2 high

▪

b5

▪

b7E

▪

▪

- To assist the POEs in positively identifying incorrectly matched individuals in a timely manner, (

▪

b2 high

b5

b7E

- ( b2 high, 5, 7E )  
foreign nationals as they enter the country through the U.S. VISIT program. Encouraging travelers not normally subject to U.S. VISIT that are repeatedly referred to secondary, to submit to U.S. VISIT biometric collection, would also enhance the ability of POEs to positively identify incorrectly matched individuals. [Comment - (

[ b2 high  
b5  
b7E ]

*Recommendation: Establish a voluntary program whereby individuals not subject to U.S. VISIT requirements may submit to collection of biometric information to reduce repeated secondary screenings.*

b. Supervisory Discretion at Ports of Entry

- [ b2 high
- [ b5
- [ b7E ]

*Recommendation: Revise the Office of Anti-Terrorism directive to allow limited discretion for the POEs regarding clear incorrectly matched cases. (*

[ b2 high  
b5  
b7E ]

**Finding: Increased counterterrorism efforts at ports of entry have negatively impacted traditional CBP missions such as narcotics interdiction and immigration fraud.**

- [ b2 high, 5, 7E ]

• [ b2 high  
• b5  
• b7E ]

*Recommendation: Port staffing needs to reviewed to determine whether the work force is able to perform CBP's legacy missions along with increased challenges regarding the prevention of terrorism. Vacancies need to be filled.*

**Finding: Inconsistent reporting of valuable collected information may be preventing it from being processed and analyzed by CBP, DHS, and the Intelligence Community.**

a [ b2 high  
• b5  
• b7E ]

• [ b2 high  
• b5  
• b7E ]

*Recommendation: Develop a policy and procedure*

[ b2 high, b5, b7E ]

**b. Reporting to Intelligence Agencies**

• [ b2 high  
• b5  
• b7E ]

• [ b2 high  
b5  
b7E ]

... one occasion, and has n

*Recommendation: Develop a clear reporting policy*

[ b2 high, 5, 7E ]

**Finding: An insufficient number**

• [ b2 high  
b5  
b7E ]

*Recommendation: Ensure that* [ b2 high, b5, b7E ]

**Memorandum of Conversation**

Date & Time: March 1, 2005 2:30 pm

Meeting held with: ( *de* )

Location: ( *b2 high* )

Inspections Staff: Randall L. Bibby, Philip Windust, Douglas Ellice, W. Preston Jacobs

Inspectors were given a general overview of CBP's history that detailed the background and training of employees. A detailed description of how CBP handles a watch-listed person was also given.

[ *b2 high*  
*b5*  
*b7E* ]

course in one week. Inspectors will follow up on her opinion of the course.

CBP receives information about who is on a plane within 15 minutes of its departure. Various databases of information provide CBP with information of who may be a threat. These include the Advance Passenger Information System (APIS), the Automated Targeting System (ATS), the Interagency Border Inspection System (IBIS), the National Criminal Information Center (NCIC), and the Treasury Enforcement Communications System (TECS). (

[ *b2 high*  
*b5*  
*b7E* ]

Many members of ( *b2 high, 5, 7E* )  
cited as an inconvenience because (

] This is

**Memorandum of Conversation**

Date & Time: February 28, 2005 2:00 pm

Meeting held with:

CBO Office of Anti-Terrorism

Location:

US Customs and Border Protection  
Ronald Reagan Building  
1300 Penn. Ave., NW. Washington, DC 20229

Inspections Staff: Randall L. Bibby, Douglas Ellice, Philip Windust, W. Preston Jacobs

CBO's Office of Anti-Terrorism (OAT) briefly clarified and reviewed various questions about the relationship between NTC, CBP, ICE and JTTF that may be asked in the field.

It was explained that ( <sup>b2 high, 5, 7E</sup>  
( <sup>b2 high, 5, 7E</sup> ) as well as the Automated Targeting  
System (ATS). ( <sup>b2 high, b5, b7E</sup>

[ <sup>b2 high</sup>  
<sup>b5</sup>  
<sup>b7E</sup> ]

OAT oversees policy. ( <sup>b2 high, 5, 7E</sup> ]

[ <sup>b2 high, 5, 7E</sup> ]



DATE: September 21, 2005, 1:00 p.m.

MEMO TO THE FILE: Summary of the September 21, 2005 meeting with (b6)  
( b6 ) CBP National Targeting  
Center

LOCATION: CBP National Targeting Center

OIG ATTENDEES: Doug Ellice, Preston Jacobs, Phil Windust

---

From the meeting we learned the following:

- [ b2 high  
b5 ]
- Discussion revolved around the issue of ( [ b2 high  
b5 ] )
- In addition, discussion centered around the idea of utilizing the U.S. VISIT program to assist in positively identifying repeat targeted travelers. ( b6 ) stated that [ b2 high, b5 ] ( ) U.S. VISIT. Therefore, a program could be initiated to allow individuals not subject to U.S. VISIT to voluntarily submit to the program (collection of biometric information) in order to expedite or even avoid repeat screenings.
- Access to databases was discussed. Ports have access to ATSP, TECS & [ b2 high, b5 ]
- An IT employee explained that progress is underway in ( [ b2 high  
b5 ] )

- When logs should and not be created was discussed. (

[

b2 high, b5

]

- When NTC should be called back was discussed. (

[

b2 high, b5

]

- 

[

b2 high  
b5

]

b2 high

b5