

Adams, Frances G

From: Teufel, Hugo [Hugo.Teufel@dhs.gov]
Sent: Friday, December 08, 2006 1:31 PM
To: Rosenzweig, Paul; Levy, Andrew; Coldebella, Gus; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R. (b) (6); Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; (b) (6); Ahern, Jayson P; Richards, Rebecca
Cc: (b) (6); Klundt, Kelly R
Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM
Importance: High

The transcript of the DPIAC June 2005 morning meeting has a quote from Paul talking about automated targeting, as had been briefed to the committee the day earlier. It was in the morning session, and can be found here:

http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_trans_am.pdf

Paul asks the question and Robert Jacksta responds. See pages 26 and 27. Paul first:

I guess I'm going to take the Chairman's privilege of the first question, and screen Mr. Jacksta. We learned yesterday about the automated tracking, targeting center, and in particular, we learned that it was operating under a legacy, privacy impact statement since it initiated before the Privacy Act came into existence even. It seemed to me, from the way it was described, it changed its function quite a bit, post 9/11, as it should, to reflect the terrorists, the changing terrorist's flight.

So I was wondering if you were planning on going through the process of developing another privacy impact assessment, statement for it, if not, why not, and if so, when?

The response from Jacksta is:

MR. JACKSTA: I think the best way to answer that question is, obviously, it's something that we need to continue to look at, and if there's a need to make sure that we're in compliance with the Privacy Act and the Privacy Impact Statements, then we'll do that and work very closely with the Privacy Office to make sure that we accomplish that.

I think what is important to note was that the systems that you saw running yesterday were systems that were in place well before 2001. They weren't defined as they are today and obviously we have better rules, we have a better system, but before 2001, we were receiving a APIS information, we were using passenger name record information. we were using an automated targeting system that allowed us to bring all that information together. Over the years, over the last three or four years we have made improvements on that to allow us to, first of all, process additional information quicker and faster and get better results back to the officer in easier format for them to read.

The legacy systems that we have brought together that are now being worked --to establish the right connectivity to the officers are legacy systems that were out there for our officers before, whether they were immigration or customs, so I'll bring that question back. I can't specifically answer if we need to

have a new privacy impact statement, but I do know that we work very closely with the Privacy Office, with our counsel to make sure that we're in compliance, that's extremely important to us.

Hugo Teufel III
Chief Privacy Officer
U.S. Department of Homeland Security
Washington, DC 20528
571.227.3813

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 this message. Thank you.

From: Rosenzweig, Paul
Sent: Friday, December 08, 2006 1:05 PM
To: Levy, Andrew; Coldebella, Gus; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b) (6) Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; (b) (6)
A: Ahern, Jayson P
Cc: (b) (6) Klundt, Kelly R; Teufel, Hugo
Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Someone needs to get with the Privacy office ... back when I was chair of the Data Privacy Advisory Committee (a public body) in June 2005, CBP took the members on a tour of the Boston targeting unit and all of this was very clear. Jacksta testified before us the next day and his testimony was also clear, though a bit more guarded.

But I think "ATS was briefed to DPIAC in June 2005" is accurate and worth saying ...

P

From: Levy, Andrew [mailto:Andrew.Levy@dhs.gov]
Sent: Fri 12/8/2006 12:30 PM
To: Coldebella, Gus; Levy, Andrew; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b) (6) Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; Atkiss, Steve
A: Ahern, Jayson P
Cc: (b) (6) Klundt, Kelly R
Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Not from 1999, but strong language from Jacksta on June 22, 2006 to Senate Commerce, Science and Transportation Trade, Tourism and Economic Development:

"At the center of our targeting efforts is CBP's National Targeting Center (NTC), where CBP personnel use the Automated Targeting System (ATS) to analyze advance information about passengers before they arrive in the United States. The NTC employs sophisticated risk assessment rules and algorithms based upon strategic intelligence about terrorist threat, and

1/18/2007

000196

incorporates data from numerous national intelligence and law enforcement databases, to screen all passengers traveling to the United States for potential terrorist connections or terrorist risk factors.”

Andrew J. Puglia Levy
Associate General Counsel (Legal Counsel)
U.S. Department of Homeland Security

(b) (6) (work)
(b) (6) (cell)
(b) (6) (fax)

andrew.levy@hq.dhs.gov

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

From: Coldebella, Gus [mailto:Gus.Coldebella@dhs.gov]

Sent: Friday, December 08, 2006 12:29 PM

To: Levy, Andrew; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b) (6)

(b) (6) Coldebella, Gus; Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville,

Michael; (b) (6) Ahern, Jayson P

Cc: (b) (6) Klundt, Kelly R

Subject: Re: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Testimony from 1999 -- when I understand ATS P to have begun -- would be helpful. Andrew and I are checking LEXIS.

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

From: Levy, Andrew <Andrew.Levy@dhs.gov>

To: Sales, Nathan <Nathan.Sales@dhs.gov>; Kraninger, Kathleen <Kathleen.Kraninger@dhs.gov>;

AGEN, JARROD <JARROD.Agen@dhs.gov>; Knocke, William R <William.R.Knocke@dhs.gov>;

(b) (6); (b) (6); Coldebella, Gus <Gus.Coldebella@dhs.gov>; Perry,

Phil <Phil.Perry@dhs.gov>; Levy, Andrew <Andrew.Levy@dhs.gov>; Isles, Adam

<Adam.Isles@dhs.gov>; Baker, Stewart <Stewart.Baker@dhs.gov>; Rosenzweig, Paul

<Paul.Rosenzweig@dhs.gov>; Scardaville, Michael <Mike.Scardaville@dhs.gov>; (b) (6)

Ahern, Jayson P

Cc: (b) (6) Klundt, Kelly R

Sent: Fri Dec 08 12:15:55 2006

Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

The legal points appear to be pulled from an earlier version of our talking points. I've attached the revised version, which we should pull from instead. Below are some of the points that we should try to include:

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Andrew J. Puglia Levy

Associate General Counsel (Legal Counsel)

U.S. Department of Homeland Security

(b) (6) (work)
(cell)
(fax)

andrew.levy@hq.dhs.gov

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

From: Sales, Nathan [mailto:Nathan.Sales@dhs.gov]
Sent: Friday, December 08, 2006 12:11 PM
To: Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b) (6) Coldebella, Gus;
Perry, Phil; Levy, Andrew; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Sales, Nathan; Scardaville,
Michael; (b) (6) Ahern, Jayson P
Cc: (b) (6) Klundt, Kelly R
Subject: Re: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING
SYSTEM

Agree. Can we add some statements from when the system was administered by Treasury?

Sent from my BlackBerry Wireless Handheld

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

From: Kraninger, Kathleen <Kathleen.Kraninger@dhs.gov>
To: Agen, Jarrod <JARROD.Agen@dhs.gov>; Knocke, William R <William.R.Knocke@dhs.gov>;
(b) (6) (b) (6) Coldebella, Gus <Gus.Coldebella@dhs.gov>; Perry,
Phil <Phil.Perry@dhs.gov>; Levy, Andrew <Andrew.Levy@dhs.gov>; Isles, Adam
<Adam.Isles@dhs.gov>; Baker, Stewart <Stewart.Baker@dhs.gov>; Rosenzweig, Paul
<Paul.Rosenzweig@dhs.gov>; Sales, Nathan <Nathan.Sales@dhs.gov>; Scardaville, Michael
<Mike.Scardaville@dhs.gov>; Kraninger, Kathleen <Kathleen.Kraninger@dhs.gov>; (b) (6)
Ahern, Jayson P
Cc: (b) (6) Klundt, Kelly R

Sent: Fri Dec 08 12:07:48 2006

Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING
SYSTEM

Testimony on ATS goes back farther. I think we should make it clear that this Administration has been talking about it since 2001 - can't speak for Customs before that but maybe CBP wants to? Thanks.

From: Agen, Jarrod [mailto:JARROD.Agen@dhs.gov]

Sent: Fri 12/8/2006 12:04 PM

1/18/2007

000199

To: Knocke, William R; (b) (6) Coldebella, Gus; Perry, Phil; Levy, Andrew; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Sales, Nathan; Scardaville, Michael; Kraninger, Kathleen; Atkiss, Steve A; Ahern, Jayson P

Cc: (b) (6) Klundt, Kelly R

Subject: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Please review this JUST THE FACTS response to AP article. Let me know if there are any errors or changes to be made. We will push it out in an about an hour.

Press Office

U.S. Department of Homeland Security

Just The Facts

Dec 8, 2006

ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

* DHS Deputy Secretary Michael P. Jackson, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee (April 5, 2006): "ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry."

* CBP Assistant Commissioner Jayson Ahern, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (March 28, 2006): "The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

* CBP Assistant Commissioner Jayson Ahern, Written Testimony, Senate Committee on Judiciary, Subcommittee on Terrorism, Technology, and Homeland Security (September 7, 2006): "Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information - Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate bona fide travelers so it can focus its resources on areas of highest risk."

* Former CBP Commissioner Robert Bonner, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 25, 2004): "The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what cargo is "high risk," and therefore will be scrutinized at the port of entry or, in some cases, overseas.

* CBP Executive Director, Traveler Security and Facilitation, Robert Jacksta, Written Testimony, Hearing before House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations (July 13, 2004): The Automated Targeting System-Passenger (ATS-P) is CBP's premier targeting tool in the passenger environment, and is available to CBP personnel at U.S. ports of entry nationwide. This system utilizes information from the National crime Information center (NCIC), the Treasury Enforcement Communications System (TECS), the Consular Lookout and Support System (CLASS) and other law enforcement databases to provide automated risk assessments on arriving international passengers.

Adams, Frances G

From: Baker, Stewart
Sent: Friday, December 15, 2006 5:27 PM
To: Isles, Adam; Coldebella, Gus; (b) (6)
Cc: Levy, Andrew; Barth, Richard; Sales, Nathan
Subject: RE: ATS-P -- some possible shifting tactics by the ACLU et al

Very helpful. We're getting the same signals from Hill staff. My view is that this is just the beginning of a psychological retreat. If we keep pushing, I think even the USC issue will go away, for the reasons given by Brian.

At the same time, if there's a consensus that we aren't worried about the privacy of foreigners, perhaps Congress will authorize us to compel production of travel records from, say, Waziristan to Indonesia.

From: Isles, Adam
Sent: Friday, December 15, 2006 2:52 PM
To: Coldebella, Gus; Baker, Stewart; (b) (6)
Cc: Levy, Andrew; Barth, Richard; Sales, Nathan
Subject: FW: ATS-P -- some possible shifting tactics by the ACLU et al

Some further thoughts on ATS from Brian Goebel, who advised Commissioner Bonner on targeting.

I might add an additional point to Brian's note below on rationale for putting USCs through ATS: we may not be able to exclude USC entry into the country, but we can keep their contraband luggage (weapons, etc.) from coming in, and we need tools to help us make these assessments.

Adam Isles
Counselor to the Secretary
U.S. Department of Homeland Security
202-282-8335 - tel

From: Brian Goebel [mailto:(b) (6)]
Sent: Friday, December 15, 2006 7:00 AM
To: 'Isles, Adam'
Cc: 'Josh Kussman'
Subject: ATS-P -- some possible shifting tactics by the ACLU et al

Adam,

I was invited to speak to the attorneys at Gibson Dunn yesterday. Not surprisingly, the issue of ATS-P came up. I ended up in a very spirited exchange with one of the more liberal members of the firm, and someone who may be piped into the ACLU. The interesting point in the exchange was this: he ultimately agreed that the government could perform risk assessments and store data on non-US citizens. He also seemed to recognize that the government could perform risk assessments on US citizens (although he didn't fully accept the need for this, suggesting that USCs weren't going to commit attacks in the U.S.). But he thought that the government should not be allowed to store data on USCs or use the risk assessment on USCs for any other purpose.

I raise this dialogue because I think it may help you prepare for the issues that are going to come up in the Congress and it may give some insight into where much the ATS-P debate is going to be fought - what to do about USCs. And, my debate really identified two separate issues: (1) what is the legal authority/what are the legal prohibitions on collecting and using information on USCs; and (2) what are the policy arguments that would support collecting and using this data on USCs. I think the legal arguments are pretty strong. Border search authority (the general authority) and ATSA (the specific authority) do not distinguish in CBP's ability to search

1/18/2007

000212

(i.e., obtain information from) USC's and non-USC's, although I have not researched the case law to confirm that view. I would encourage you to have the Department prepare a pocket brief on that point, if you haven't already done so. Second, what are the policy arguments for risk-assessing USC's and storing data on USC's (even if they are assessed as no risk)? I pointed out that there have been plenty of USC's involved in terrorism, although I couldn't remember all the names. And, I pointed out that just because a person is judged as no threat in 2006 doesn't mean he or she won't be a threat in 2015, and therefore maintaining some relatively innocuous travel history information on people is justifiable. This, ultimately, may be where the ACLU (and Members of Congress) are going to argue most strongly against ATS-P. Some people believe this is Hoover's FBI all over again.

In any event, I wanted you to have this information as you continue to plot strategy on this issue. Good luck,

Brian

(b) (6)

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

Close hold. Is there anything more we can add? Anything incorrect?

From: Knocke, William R [mailto:William.R.Knocke@dhs.gov]
Sent: Friday, November 03, 2006 1:19 PM
To: Sweet, Chad; (b) (6) 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; (b) (6) Baker, Stewart; Teufel, Hugo; Perry, Phil; Coldebella, Gus; Rosenzweig, Paul
Cc: Agen, Jarrod; Gonzalez, Joanna
Subject: RE: JUST THE FACTS

Appreciate the rapid reaction.

CCS

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

O: (b) (6)
C: (b) (6)
E: chad.sweet@dhs.gov

From: Knocke, William R
Sent: Friday, November 03, 2006 12:21 PM
To: (b) (6) 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; (b) (6)
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)

000373

1/24/2007

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 REGULARLY 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)

(b) (6)

From: Richards, Rebecca (b) (6)
Sent: Friday, November 03, 2006 10:55 AM
To: Rosenzweig, Paul; (b) (6) Agen, Jarrod; Knocke, William R
Cc: Teufel, Hugo; Mortensen, Kenneth (b) (6)
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

- Under U.S. laws, all travelers and cargo entering the United States or leaving the country are subject to inspection and examination for compliance with customs, immigration and a multitude of other laws. No level of suspicion is required to conduct this basic screening at the border.
- Screening like this has been conducted and authorized for decades (and in the case of land and sea for centuries).
- On the merits, it makes no sense at all to treat all travelers the same. In a world of limited resources we need to target our examination at those people who present the highest risk

SORN UPDATE

- The ATS SORN is part of Department's effort to move from legacy system of records notices to DHS system of records notice. As part of that process, DHS is analyzing existing SORNs and updating them. The ATS SORN is a description of what DHS has been doing under TECS. The only addition with this SORN is two new routine uses, which will not go into effect until the SORN is final:
 - o Routine use for sharing in pandemic health situations and
 - o Testing of live data.
- *[ONLY IF ASKED: The Privacy Act has a provision for sharing personal information for health, and the individual must be notified of the sharing. In instances of analysis to determine pandemic health, it would only be appropriate to notify the individual if there was a risk, but DHS may need to share the information in order to conduct the analysis and make that determination.]*

RETENTION

- Not all information retained for the 40 years. The SORN specifically states that CBP will regularly remove information if determined to no longer be relevant and useful. The Privacy Office will conduct reviews of CBP's implementation.
- The Automated Targeting System leverages and fuses data from an array of sources to maximize risk assessment capabilities. ATS sources enforcement data from the Treasury Enforcement Communication System (TECS), which maintains data for up to 40 years. ATS leverages the TECS data available for this full period to ensure that derogatory information that might exist and help identify viable risks are effectively integrated into CBP's risk assessments. CBP enforces the borders, and criminals or terrorist suspects may operate for many years without crossing our borders; thus, necessitating the maintenance of enforcement data for this full period.

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

To: (b) (6) Agen, Jarrod
Cc: Richards, Rebecca
Subject: RE: Talking point on new ATS Fed Register Announcement

Suggest something along the following lines:

- Screening like this has been going on for dozens of years in the air and sea environment and also in the land environment for selected cases
- The ATS SORN does not announce any changes at all -- it merely formalizes in a single place existing screening systems and rules
- On the merits, it makes no sense at all to treat all travelers the same. In a world of limited resources we need to target our examination at those people who present the highest risk

Rebecca -- anything to add?

Paul Rosenzweig
(b) (6)
paul.rosenzweig@dhs.gov

From: (b) (6) (b) (6)
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.

(b) (6)

(b) (6)

Director for Canadian Affairs
DHS Policy
Office of International Affairs

(b) (6) (desk)
cell)

(b) (6)

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; A15

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.

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."

(b) (6)

From: Scardaville, Michael
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

Mike

(b) (6)

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

From: (b) (6)
Sent: Friday, December 15, 2006 2:08 PM
To: Sales, Nathan; Scardaville, Michael
Subject: ATS Standards
Importance: High

Mike, the following should assist in answering your questions:

1. ATS has been assigned a security categorization of HIGH according to:

Security categorization of information systems and the information processed, as mandated by the Federal Information Processing Standards FIPS PUB-199 Standards for Security Categorization of Federal Information and Information Systems.

2. ATS is tested and certified/accredited according to: National Institute of Standards and Technology SP 800-53, Recommended Security Controls for Federal Information System which defines the set of security controls required for ATS, based upon its security categorization which is HIGH.

3. Finally, ATS goes through yearly assessment in accordance with The Federal Information Security Management Act (FISMA) of 2002 which mandates that all federal organizations report annually on the status of their security programs. ATS Conducts an annual security self-assessment using the NIST SP 800-26, Self-Assessment Questionnaire which allows us to show compliance with standard security controls.

4. Other key documents that are part of the ATS C&A process include OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems and NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, which gives us guidelines for contingency planning/testing and disaster recovery.

(b) (6)

Adams, Frances G

From: Sales, Nathan

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

To: Rosenzweig, Paul; Baker, Stewart; (b) (6) White, Brian M; (b)(6)
(b)(6) Levy, Andrew

Subject: Re: Analysis: Dems slam border screening rules

Also on point 2. Dan Solove of GWU just published a piece in U Penn L Rev on the privacy implications of sharing lawfully-obtained information. Solove is pushing the law, and in a direction we may not like, but it may be a useful compendium of the key cases.

Sent from my BlackBerry Wireless Handheld

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

From: Rosenzweig, Paul

To: Sales, Nathan; Baker, Stewart; (b) (6) White, Brian M; 'Coldebella, Gus' (b) (6)
'Wheelbarger, Kathryn' (b) (6) Levy, Andrew

Sent: Wed Jan 03 10:42:39 2007

Subject: RE: Analysis: Dems slam border screening rules

There is a host of law on the second point. The one that comes closest to mind is Stanford Daily v. Zurcher (?). You might also check out all the law on traffic stops which hold, generally, that so long as the police officer has an objectively legitimate purpose for the stop, the information collected may be used for any other lawful purpose ...

P

Paul Rosenzweig

(b) (6)

(b)(6)

From: Sales, Nathan

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

To: Baker, Stewart; Rosenzweig, Paul; (b) (6) White, Brian M; 'Coldebella, Gus'; Wheelbarger, Kathryn; Levy, Andrew

Subject: RE: Analysis: Dems slam border screening rules

I'm not sure I understand Thompson's claim. Is he suggesting that the collection of passenger data offends the Fourth Amendment's warrant requirement? Or is he suggesting that the sharing of passenger data offends the warrant requirement?

The first claim is clearly wrong. A person has no reasonable expectation of privacy in records he has voluntarily handed over to third parties, such as passenger information (see, e.g., *United States v. Miller*, *Smith v. Maryland*, etc.). The second one sounds intuitively wrong, too, though I haven't looked at the cases. It can't be the case that the Fourth Amendment requires the government to get a warrant any time it wants to share information it has collected lawfully.

Gus, Andrew, and Katie, we think the new Democratic Congress is going to take a close look at the ATS program, and it would help to have a clearer sense of the law in this area. Would it be possible for OGC to put together a three-to-five-page memo on the Fourth Amendment constraints on collecting and sharing business-records information? 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

(b) (6)

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

And I think we should go along to the extent we can. These comments really could have been worse. He's endorsed the basic thrust of the program.

From: Rosenzweig, Paul
Sent: Tuesday, January 02, 2007 12:08 PM
To: Baker, Stewart; (b) (6)
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: (b) (6)
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 (b)(6)
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

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.

(b) (6)

From: Scardaville, Michael (b) (6)
Sent: Friday, December 01, 2006 5:05 PM
To: Richards, Rebecca
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

(b) (6)

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

From: Sales, Nathan
Sent: Friday, December 01, 2006 5:03 PM
To: Scardaville, Michael; Agen, Jarrod
Cc: Baker, Stewart; 'richard.barth@dhs.gov'; 'paul.rosenzweig@dhs.gov'; White, Brian M; Teufel, Hugo
Subject: RE: ATS Privacy Impact Assessment

Okay, here's the new version with my edits.

(b) (5)

(b) (5)

Best,
NAS

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

(b) (6)

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

From: Sales, Nathan
Sent: Friday, December 01, 2006 3:18 PM
To: Scardaville, Michael; Agen, Jarrod
Cc: Baker, Stewart; (b) (6); 'paul.rosenzweig@dhs.gov'; White, Brian M; 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

(b) (6)

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

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

To: Sales, Nathan; Agen, Jarrod
Cc: Baker, Stewart; (b) (6) 'paul.rosenzweig@dhs.gov'; White, Brian M; Teufel, Hugo
Subject: RE: ATS Privacy Impact Assessment

Nathan,

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

Mike
(b) (6)

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

From: Sales, Nathan
Sent: Friday, December 01, 2006 8:44 AM
To: Agen, Jarrod
Cc: Baker, Stewart; (b) (6) 'paul.rosenzweig@dhs.gov'; White, Brian M; 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. Seems to me we might want to ask the AP for a correction (or corrections).

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; (b) (6) 'paul.rosenzweig@dhs.gov' <paul.rosenzweig@dhs.gov>; White, Brian M; 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 Toby Levin 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; (b) (6) 'paul.rosenzweig@dhs.gov'; White, Brian M; Scardaville, Michael; Teufel, Hugo
Subject: ATS Privacy Impact Assessment

Jarrold, 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 (b) (6)
To: Sales, Nathan <Nathan.Sales@dhs.gov>
Sent: Fri Dec 01 07:13:09 2006
Subject: Re: "DHS Seizing / Downloading Laptops"

Me neither, but if I recall correctly the talkers are about 3 lines and mount to "we're CBP and we can search what ever we want.". While true perhaps, not very confidence inspiring for travelers and citizens. That said, in this case I don't know if there is anything more we can say w/o revealing sensitive info.

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 <Nathan.Sales@dhs.gov>
To: Scardaville, Michael (b) (6) (b) (6)
(b) (6) Rosenzweig, Paul <Paul.Rosenzweig@dhs.gov>
Cc: Sales, Nathan <Nathan.Sales@dhs.gov>
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 (b) (6)
To: (b) (6) Rosenzweig, Paul <Paul.Rosenzweig@dhs.gov>;
Scardaville, Michael (b) (6)
Cc: Sales, Nathan <Nathan.Sales@dhs.gov>
Sent: Fri Dec 01 06:20:21 2006
Subject: Re: "DHS Seizing / Downloading Laptops"

Thanks Mark,

I have CBP's talkers at the office and will send them once I get in. However, they don't say much and our Counsel asked to discuss before sharing. I'm hoping to get some more background for you out of that conversation. Unfortunately we've been plying phone tag.

Mike

Sent from my BlackBerry Wireless Handheld

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

From: Koumans, Mark (b) (6)
To: Rosenzweig, Paul <Paul.Rosenzweig@dhs.gov>; Scardaville, Michael (b) (6)
Cc: Sales, Nathan <Nathan.Sales@dhs.gov>
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 [mailto:Paul.Rosenzweig@dhs.gov]
Sent: Wednesday, November 29, 2006 01:00
To: Koumans, Mark ; 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

(b) (6)

paul.rosenzweig@dhs.gov

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


(b) (6)

Issue: APIS Retention Period


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

Current Status: It is believed that the CBP Office of Field Operations would require a retention period of (b)(5), High (b)(2), (b)(7)(E) for Advance Passenger Information data in order to adequately support CBP's Anti-Terrorism mission.


High (b)(2), (b)(7)(E)

A large black rectangular redaction box covering several lines of text.


High (b)(2), (b)(7)(E)

A large black rectangular redaction box covering several lines of text.

High (b)(2), (b)(7)(E)

A large black rectangular redaction box covering several lines of text.

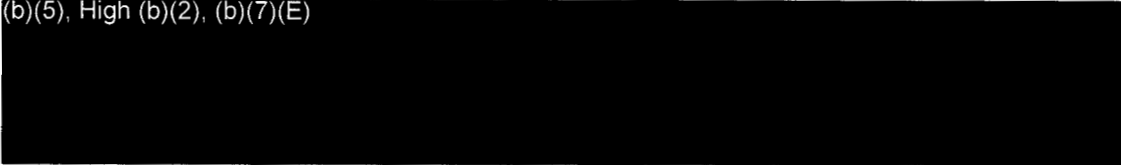
High (b)(2), (b)(7)(E)

A large black rectangular redaction box covering several lines of text.


Had DHS/CBP not had this historical data, the ability to tie these people, groups, and networks together would be nonexistent.

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


(b)(5), High (b)(2), (b)(7)(E)



(b)(5), High (b)(2), (b)(7)(E)




(b)(5), High (b)(2), (b)(7)(E)



Chief Counsel revision (10/25/06):

(b)(5), High (b)(2), (b)(7)(E)



**Guidelines for Use and Disclosure of Passenger Name Record (PNR) Data
By ICE and DHS Office of the Secretary**

I. Use of PNR Information¹

A) Permissible Purposes: Department of Homeland Security (DHS) personnel within ICE and the Office of the Secretary who are authorized to access Passenger Name Record (PNR) data through CBP's Automated Targeting System - Passenger (ATS-P) in connection with their official duties (personnel collectively referred to as, "Authorized DHS Users"), may do so in accordance with the following:

1) PNR derived from flights between the United States and European Union (EU): Authorized DHS Users may access this PNR through ATS-P strictly for purposes of preventing and combating:

- a) terrorism and related crimes;
- b) other serious crimes that are transnational in nature; and
- c) flight from warrants or custody for the crimes described in (1) and (2), above.

2) PNR derived from flights between the U.S. and foreign ports or places outside of the EU (except Switzerland and Iceland, to which DHS Authorized Personnel DO NOT have access): Authorized DHS Users may access this PNR for any lawful purpose in the performance of their official duties, and consistent with these PNR Guidelines and other applicable policies.

B) Available Data Elements

1) PNR derived from flights between the United States and European Union (EU): CBP's computer system is designed to provide access to Authorized DHS Users through ATS-P to 34 specific PNR data elements that may be available in an air carrier's reservation/departure control system related to flights between the U. S. and EU. A list of those specific data elements are set forth in Attachment "B." ATS-P is designed to provide

¹ These PNR Guidelines expressly exclude access by authorized personnel covered by these Guidelines to PNR derived from flights between the U.S. and Switzerland and the U.S. and Iceland. Such PNR is the subject of a separate arrangement with Switzerland and Iceland and is currently not available to Automated Targeting System - Passenger (ATS-P) users outside of Customs and Border Protection (CBP). Users subject to these Field Guidelines ARE PROHIBITED from requesting access to PNR data derived from flights between the U.S. and Switzerland and Iceland, or otherwise viewing such data, through ATS-P. Access to such data may be requested on a case-by-case basis from CBP pursuant to those applicable arrangements with Switzerland and Iceland.

000517

access to only those limited data elements (to the extent, and wherever, that data resides in a carrier's reservation/departure control system). Additional restrictions on this PNR data apply as follows:

- a) Other Service Information (OSI), Special Service Request (SSI/SSR): Although these fields are part of the 34 available data elements mentioned above, these fields will generally be "blocked" by CBP's system to prevent routine viewing by authorized users. In the event that an individual is identified as high risk or to be of particular concern, a supervisor may authorize the CBP system to make the OSI and SSI/SSR fields of the subject's PNR available to the reviewing Authorized DHS User. This authorization will be facilitated at the discretion of the Authorized DHS User's supervisor. (

[b2 high
b7E]

- b) "Sensitive" Data: Certain PNR codes and terms which may appear in a PNR have been identified as "sensitive" and are blocked by CBP's automated system to prevent routine viewing by authorized users. A list of the mutually agreed upon "sensitive" codes/terms is contained in Attachment "C." (

[b2 high
b7E]

2) PNR derived from flights between the U.S. and foreign ports or places outside of the EU (except Switzerland and Iceland): CBP's computer system is designed to provide full access to Authorized DHS Users through ATS-P to all PNR data elements that may be available in an air carrier's reservation/departure control system.

C) Timing of Access: Applicable to All PNRs derived from flights flying to and from the U.S.:

1) Routine Access: ATS-P will pull or have pushed PNR data from all air carriers, no earlier than 72 hours prior to departure of the flight.

- a) Pull: In the case where data is pulled by CBP's system, the system will automatically recheck for PNRs no more than three (3) times between an initial pull, the departure of the flight from a foreign port

000513

or place and the flight's arrival in the United States, or between the initial pull and the departure of the flight from the United States, as applicable. This will be done to identify any changes in the information under the pull method.

- b) **Push:** Some air carriers that utilize the push method will push PNR data at the time of creation; all data that has been changed since the initial push will be then be subsequently pushed shortly after the change occurs. This will enable CBP to have the most updated information available in real time. Other air carriers will push data at the same timed scheduled as mentioned above for pulls. Scheduled times may be changed to meet operational needs.

The PNR data from the automated pulls or pushes will be available within ATS-P. Any other pulls or pushes that deviates from the above will be considered *non-routine*.

- 1) **Non-Routine Access:** All manual pulls of PNR data performed from CBP's system are considered non-routine. (

b2 high
b7E

II. **Disclosure of PNR Information**

A) **PNR derived from flights between the United States and European Union (EU)**

- 1) **Disclosures to or within CBP, ICE or DHS Office of the Secretary:**
Disclosures consistent with the purposes outlined above in paragraph I(A)(1) may be made by Authorized DHS Users to persons within such offices/agencies who have a need for the record in the performance of their official duties, in accordance with normal policies and procedures for sharing of information within DHS.

- 2) **Disclosures to Other U.S. Government Authorities with Counterterrorism functions that are Certified for Facilitated Access:²**
Authorized DHS Users may disclose PNR to other U.S. government authorities with counterterrorism functions for purposes of preventing or combating terrorism or related crimes, where such authority has been certified by CBP to receive facilitated access to PNR (i.e., where Authorized DHS Users are working jointly with an agency which has facilitated access, but disclosure is to be through a means other than by that agency through ATS-P). All Authorized DHS Users should use the automated disclosure system for such disclosures. For each disclosure, a PNR Disclosure Form and CF 191 must be completed to document the release of information. This form is automated within ATS-P and can be generated before or after accessing the PNR. The system will generate the required forms and pre-populate some of the information.

(b)(2)(b)(7)(E)

- 3) **Disclosures to other government authorities (except as provided for under paragraphs II(A)(1) and (2) above):**
 - a) PNR information may be disclosed on a case-by-case basis to such authorities, including foreign government authorities, in the following circumstances and in accordance with the procedures set forth in paragraph II(A)(2)(b) below:

² Some U.S. government agencies, including DHS components not covered by this Field Guidance, that have a counterterrorism function will receive PNR data through a mechanism referred to as "facilitated access," for purposes of combating terrorism and related crimes only. Facilitated access will be covered by a separate policy document. To the extent PNR is requested by (or discretionary disclosures made to) such an agency for a purpose consistent with paragraph I(A)(1) that is outside the scope of their facilitated access authorization (i.e., for combating a serious transnational crime with no nexus to terrorism), such a request should be treated consistent with paragraph II(A)(3).

- i) To another government authority that has law enforcement or counter-terrorism functions, where the disclosure is consistent with a purposes identified above in paragraph I(A)(1). Disclosures to such government authorities should only be made if it is determined that:
 - the receiving government authority is responsible for preventing, investigating or prosecuting violations of, or enforcing or implementing, a statute or regulations related to the purpose of the request; and
 - Authorized DHS Users are aware of an indication of a violation or potential violation of law.
 - ii) To relevant government authority(s), where disclosure of the PNR data is necessary to protect the vital interests of the subject of the PNR or of other persons (for example, in the case of significant health emergencies or epidemics).
- b) Disclosure Procedures and Conditions:
- i) Written Request: If another government authority is requesting information that would include PNR data, a written request from that government authority must explain the specific information requested and the reason(s) for the request. This written request may be submitted via e-mail by the requesting government authority and must be submitted prior to the disclosure of any PNR information. Only under exigent circumstances may PNR information be disclosed based on a verbal request. If this occurs, a written request must be submitted as soon as possible following the disclosure of the PNR information based on verbal representations.
 - ii) Review of Purpose: Review the request to insure that the purpose for obtaining the data relates to the purposes for which that government authority is permitted to receive PNR data (see paragraph I(A)(1) above).
 - iii) Record of Disclosure: All disclosures (regardless of the citizenship or residence of the data subject) must be recorded in accordance with the following procedures:
 - A PNR Disclosure Form and CF 191 must be completed to document the release of information. This form is automated within ATS-P and can be generated before or after accessing the PNR. The system will generate the required forms and pre-populate some of the information.

000521

[b2 high
b7E]

- Upon completion of the disclosure form, a cover letter will be automatically generated by the system. This letter must be included with the transfer of the PNR data to the other government authority.
- Authorized DHS Users shall maintain a copy of all written requests for disclosures for audit purposes.

iv) Marking of Transmitted PNR Data: Copies of PNR data (including any portion of any PNR) furnished to another government authority in accordance with this guidance must contain the following statements:

"Property of the U.S. Department of Homeland Security"

"This document is provided to your agency for its official use only and remains the PROPERTY OF THE DEPARTMENT OF HOMELAND SECURITY."

This document contains confidential personal information of the data subject ("Official Use Only") and confidential commercial information and may not be disclosed to any third party without the express prior written authorization of DHS."

B) **PNR derived from flights between the U.S. and foreign ports or places outside of the EU (except Switzerland and Iceland):** Such data may be disclosed to persons who have a need for the record in the performance of their official duties, in accordance with normal policies and procedures for sharing of information within and outside DHS and as otherwise authorized by law. See the Privacy Act System of Records Notice (SORN) for the Automated Targeting System (ATS)) (71 Federal Register 212 (November 2, 2006)). For each disclosure, a PNR Disclosure Form and CF 191 must be completed to document the release of information. This form is automated within ATS-P and can be generated before or after accessing the PNR. The system will generate the required forms and pre-populate some of the information.

[b2 high, b7E]

C) **Mandatory Disclosures of PNR**

006522

- 1) Subpoenas or other legally mandated disclosures (other than under the Freedom of Information Act or Privacy Act): All Authorized DHS Users should immediately contact the Office of General Counsel or their local counsel's office for guidance in responding. In responding to such demands, reasonable efforts should be taken to protect the confidentiality of such data, as permitted.
- 2) Freedom of Information Act (FOIA) Requests (5 U.S.C. 552) and Privacy Act Requests (5 U.S.C. 552a): Any FOIA or Privacy Act requests involving PNR data should be promptly referred to the Customer Satisfaction Unit (CSU) for a determination regarding whether PNR data should be released to the requestor.

*U.S. Customs and Border Protection
Customer Satisfaction Unit
1300 Pennsylvania Avenue NW
Washington, D.C. 20229*

III. Corrections and Complaints Regarding PNR Data:

- A) Requests for corrections or complaints regarding the accuracy of PNR data should be forwarded to the CSU at the address noted in paragraph II(C)(2) above. The CSU will forward the request to the designated personnel from the National Targeting and Security office within CBP to determine if information contained in a PNR is inaccurate (whether independently identified by the DHS Authorized User or upon the request of the data subject or his legal representative (e.g., EU Data Protection Authority). If appropriate, a note will be linked to the PNR record within ATS-P to document that the data was determined to be inaccurate and will provide the correct information. Authorized DHS Users may access any corrected information by clicking on the icon that resembles a note at the top of the PNR page within ATS-P.
- B) Any complaints regarding a specific agency's handling or use of PNR data will be handled by that agency. The agency should promptly provide CBP's Customer Satisfaction Unit with a copy of such complaints and the agency's response.

IV. Data Security

- A) CBP considers all data obtained from airline reservation/departure control systems to be law enforcement sensitive, confidential personal information of the data subject ("Official Use Only" Administrative Classification) and confidential commercial information. Details regarding access to PNR information in ATS-P (such as who, where, when (date and time)) are automatically recorded and routinely audited by the Office of Information and Technology to prevent unauthorized use of the ATS-P system.

000523

- B) ICE and the DHS Office of the Secretary have implemented policies which comport with those of CBP's with regard to the treatment and handling of PNR data by their users (including these PNR Field Guidelines). Unauthorized access by any personnel to air carrier reservation systems or ATS-P (in which PNR data is stored) is subject to strict disciplinary action (which may include termination of employment) and may result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030).
- C) ICE and the DHS Office of the Secretary policies (consistent with CBP applicable policy and regulations) also provide for stringent disciplinary action (which may include termination of employment) to be taken against any employee who discloses PNR data without official authorization (title 19, Code of Federal Regulations, section 103.34). Criminal penalties (including fines, imprisonment of up to one year, or both) may be assessed against any officer or employee of the United States for disclosing PNR data obtained in the course of his/her employment, where such disclosure is not authorized by law (see title 18, United States Code, sections 841, 1030, 1905).

V. Process for Access to CBP's System

- A) ICE and the Office of the Secretary have established a single point of contact (liaison) for their agency through which to forward PNR access requests. In cases of system misuse or abuse or system inactivity, the agency point of contact will be notified by CBP.
- B) All new requests for access to PNR data from the ATS-P database must be approved by each requestor's supervisor before being forwarded to the agency/office's PNR point of contact. Once approved then the request will be forwarded to (b2, b6) at (b2, b6) Operations (OFO).
- C) Request for access to CBP's system is to be forwarded by email from the agency/office's PNR point of contact to the ATS-P Program Manager, OFO at CBP Headquarters (currently David Dodson at David.Dodson@dhs.gov).
- D) An invitation letter, a Request Letter template, and a CBP Form 7300 will be forwarded to the requestor's agency point of contact, along with the pertinent policies and documents for PNR use and ATS-P access.
- E) Once the Request Letter and CBP Form 7300 is received by OFO and access is approved by CBP's system security and OFO, accounts and passwords will

000521

be established for new users. OFO will then forward an approval letter to the pertinent agencies.

- F) If the U.S. government employee no longer requires PNR access to perform their duties (e.g., change of work assignment or separation from the agency), then the point of contact is required to immediately notify the ATS-P Program Manager of CBP's Office of Field Operations.
- G) Due to the sensitive nature of the data and the requirement that only those personnel with a need to know can access PNR data, employees who have failed to log in to ATS-P within a 90-day period will lose access to that system. If an employee requests to be reinstated, the employee's supervisor is responsible for verifying and notifying OFO of the employee's need to retain access to ATS-P.

VI. Training

- A) A CBP subject matter expert will provide Train-the-Trainer sessions for nominated representatives of the pertinent agencies. The training will include hands-on and verbal instructions, as well as distribution of written policies.

VII. No Private Right Created

These Field Guidelines are intended for internal DHS use only and they do not create or confer any right or benefit on any person or party, private or public.

000525

Attachment "A"

List of European Union (EU) Countries (as of 11/02/06):

Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
The Netherlands
United Kingdom

Joining effective January, 2007: Bulgaria and Romania

000520

Attachment "B"

**List of PNR Data Elements DHS Authorized Users May Access In
Connection with Flights between the United States and the European
Union Countries**

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address (es))*
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/Divided PNR information
17. Email address
18. Ticketing field information
19. General remarks
20. Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information
27. SSI/SSR information
28. Received from information
29. All historical changes to the PNR
30. Number of travelers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS information
34. ATFQ fields

* CBP's system will also automatically access any of the other 34 data elements to the extent they may exist within the frequent flyer record.

000527

b2 high
b7E

000523

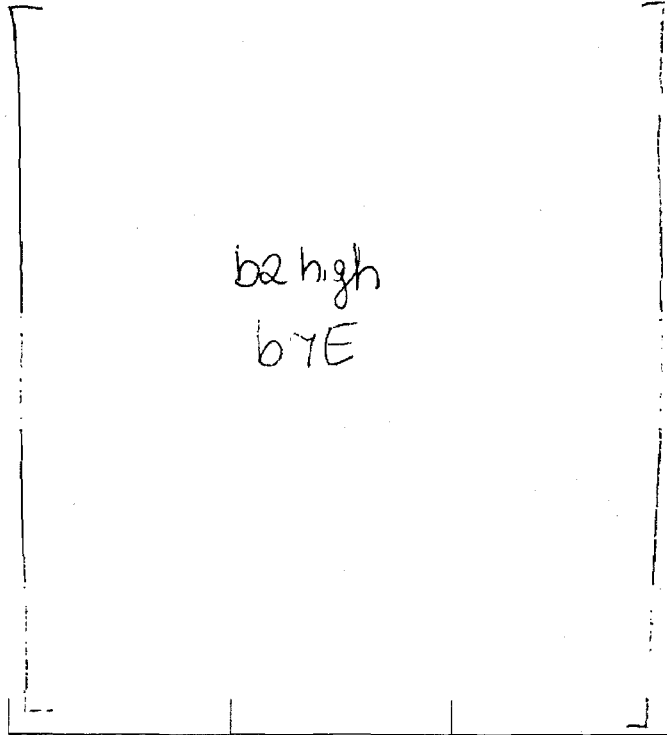
b2 high

b7E

000529

b2h.gh
b7E

000530



00531

6⁷ release
M.L. Vaughn # 98
Bates 540-543

U.S. Department of Homeland Security
Washington, DC 20229



U.S. Customs and
Border Protection

MEMORANDUM FOR: DIRECTORS, FIELD OPERATIONS
DIRECTOR, PRECLEARANCE OPERATIONS
FROM: Acting Director, Border Targeting and Analysis (b6)
SUBJECT: Standardization of ATS Access Requests for ATS Modules

This memorandum is provided to Directors of Field Operations in order to create uniformity in new user access requests for Automated Targeting System (ATS) modules.

The Automated Targeting System (ATS) is a decision support tool used to enhance and improve CBP targeting efforts. ATS is used for assessing travelers and cargo shipments for risks that may be related to terrorism and as a tool to combat or prevent other types of transnational crimes. Access to the ATS system is controlled and is available only to Customs and Border Protection (CBP) personnel and government employees of other agencies with a need-to-know in connection with their official duties. Access to ATS is contingent upon the employee's obtaining access to CBP mainframe applications (TECS for all modules, ACS for ATS cargo modules), which in turn requires a current CBP adjudicated background investigation.

Access to all ATS applications is granted pending completion of the following:

- The prospective user's supervisor must submit a properly completed access request form to the designated OFO/NTS manager identified for the specified ATS module. RESMON access requires the access request form be submitted by the designated OFO/DFO.
- The following access request fields are required in order to ensure uniformity among field locations. Please note that commas, dashes and periods should not be used when completing the form.

[b2]

*Access Request format in Excel shown here. Definitions are shown below.

- o **User First Name** – Requestor's first name
- o **User Last Name** – Requestor's last name
- o **User Mid Name** – Requestor's middle name
- o **User SSN Nbr** – New user's social security number
- o **User Hash ID Nbr** – New user's hash identification number
- o **SUPVR HASH Nbr** – New user's supervisor's hash ID
- o **SUPBR SSN Nbr** – New user's supervisor's SSN
- o **Govt employee Y/N** – Specify if requestor is a government employee
- o **USER WRK PHN NBR** – New user's work phone number
- o **User Email Address** – New user's work email address
- o **Agency CD** – Agency Code
- o **User CBP ORG Code** – New User's 13 character organization code
- o **User Assigned Port Code** – Port Code new user is assigned to
- o **User Job Title** – Title of new user (Targeter, Supervisor, etc.)
- o **Requested System** – Each ATS sub-system requested (ATS-N, ATS-AT, ATS-L, TAP2K, ATS4, ATS-P, ATS-PDA, RESMON) must be listed

ATS Modules are comprised of the following:

- **ATS-N (Inbound)** access is provided to CBP personnel assigned in the air and sea cargo environments, Express Courier Hubs, CSI locations, select ICE agents and personnel assigned at the NTCC for cargo targeting and analysis. ATS-N provides enforcement information from TECS, transactional data from ACS as well as exterior data sources, and ensures relevant data is available to ATS-N in time for CBP to effectively evaluate and investigate inbound shipments prior to arrival. Requests for access must be provided in the prescribed format to the appropriate managers, (b7) at (a2, b7) or (b7) (a7) at (a2, b7) .
- **ATS-AT (Anti-terrorism / Outbound)** access is provided to CBP personnel assigned to outbound cargo environments and NTC personnel. ATS-AT provides an efficient means of identifying high-risk export shipments among the millions of recorded shipments and incorporates the enforcement of other government agency laws to include Treasury Office of Foreign Asset and Control lists; targeting for materials defined by the Nuclear Regulatory Commission (NRC) as weapons of mass destruction components; and ensures adherence to the State Department's Office of Defense Trade Controls (ODTC) Regulations. Requests for access must be provided in the prescribed format to the appropriate OFO/NTS managers, (b7) ; at (b2, b7) ; or (b7) (a7) at (a2, b7)
- **ATS-L (Land)** access is provided to CBP personnel assigned to Land Border crossing locations. ATS-L capabilities include the automatic crosschecks of information, (b2 h, gh, b7E)]

lookout for terrorism, smuggling, etc. Requests for access must be provided in the prescribed format to the appropriate OFO/NTS manager (b) (6) at (b) (6)

- The Trend Analysis and Analytical Selectivity Program (TAP2K) supports field users and ATS. TAP is an analytical profile tool that aggregates data (b)(2)high (b)(7)(E)
 - This information is utilized by ATS, field personnel and other disciplines to review historical trends and trade patterns (b)(2)high (b)(7)(E)
 - Requests for access must be provided in the prescribed format to the appropriate OFO/NTS managers (b) (6) a (b) (6) or (b) (6) (b) (6)
- ATS4 is in the testing phase in conjunction with the Cargo Enforcement Reporting and Tracking System (CERTS). Requests for access to ATS4 are limited to those ports identified in the Phase I and Phase II testing cycle. Requests for access to ATS4 applications must be provided in the prescribed format to the appropriate OFO/NTS manager (b) (6) at (b) (6)
- ATS-P (Passenger) utilizes information from a diverse set of databases to allow CBP officers to conduct research queries of international travelers to assist in the inspectional decision-making process. ATS-P contains data such as border crossings, I-94 and visa data, as well as modules for reviewing airline reservation data (PNR), and passenger arrival statistics (ATS-PDA.) Due to an agreement between DHS and the European Union, access to PNR data is limited based on the user roles described below.
 - Basic User Role access is typically provided to (b)(2)high (b)(7)(E) whose duties do not require access to PNR data.
 - CTR User Role access is given to (b)(2)high (b)(7)(E) whose duties require viewing PNR data no older than seven (7) days after a flight's arrival to, or departure from, the U.S.
 - PAU User Role access is given to (b)(2)high (b)(7)(E) and permits viewing of PNR data older than seven (7) days, but no older than 3.5 years, unless the PNR is linked to an enforcement record.

- o The PAU Supervisor User Role access is provided to (b2, b7E)
(b2 high, b7E) This user role allows viewing of PNR data with the same conditions as the PAU User Role. Recipients can grant permission to view restricted PNR fields to officers with PNR access.

All requests for ATS-P access, including the Resmon and ATS-PDA modules, must be provided in the prescribed format to the appropriate OFO/NTS managers, (b6) at (b3, b6) and (b6) at (b2, b6).

Once the approving OFO/NTS manager receives a request in the proper format, the manager evaluates the request and forwards the request to ATS Security. ATS Security reviews the new user request, verifies the user's background investigation status and ensures the new user has access to mainframe applications. ATS Security then notifies the new user of the access and provides the new user with a temporary password. This process normally requires 3-5 working days.

Requestors should not contact the approving OFO/NTS manager directly to inquire about the status of their pending access requests. Problems encountered attempting to access the ATS modules should be directed to the ATS Hotline at (b2) (b2)

Periodic ATS audits and reviews are conducted to ensure inactive accounts and users no longer requiring access are deleted from the system.

If you have any questions, please direct them via email to (b6)
(b2, b6) or telephonically (b2) or (b6) at
(b2, b6) or telephonically

(b) (6)

From: (b) (6)
Sent: Friday, November 03, 2006 10:49 AM
To: Richards, Rebecca
Cc: (b) (6); Teufel, Hugo; Mortensen, Kenneth; (b) (6); (b) (6)
Richards, Rebecca; (b) (6)
Subject: RE: Talking points on ATS NEED INPUT

Becky,

Here is another:

The Automated Targeting System leverages and fuses data from an array of sources to maximize risk assessment capabilities. ATS sources enforcement data from the Treasury Enforcement Communication System (TECS), which maintains data for up to 40 years. ATS leverages the TECS data available for this full period to ensure that derogatory information that might exist and help identify viable risks are effectively integrated into CBP's risk assessments. CBP enforces the borders, and criminals or terrorist suspects may operate for many years without crossing our borders; thus, necessitating the maintenance of enforcement data for this full period.

(b) (6)
Office of Field Operations
Customs and Border Protection

(b) (6) fax

"Richards,
Rebecca"
(b) (6) "Richards, Rebecca"
(b) (6) <Rebecca.Richards
(b) (6) (b) (6)
(b) (6) @dhs.gov>
(b) (6)

To: (b) (6)
(b) (6) (b) (6)
(b) (6) (b) (6)
(b) (6)
cc: "Mortensen, Kenneth"
<Hugo.Teufel@dhs.gov>
Subject: RE: Talking points on ATS NEED

11/03/2006 10:42
<Kenneth.Mortensen@dhs.gov>, "Teufel, Hugo"
AM

INPUT

They are talking to the press in about 15 minutes. Any changes need to come in the next five. Sorry for the short turn around. We have already been on the phone talking with OPA.

Becky

- Screening like this has been going on for dozens of years in the air and sea environment and also in the land environment for selected cases
- On the merits, it makes no sense at all to treat all travelers the same. In a world of limited resources we need to target our examination at those people who present the highest risk
- The ATS SORN is part of Department's effort to move from legacy system of records notices to DHS system of records notice. As

part of that process, DHS is analyzing existing SORNs and updating them. The ATS SORN is a description of what DHS has been doing under TECS. The only addition with this SORN is two new routine uses, which will not go into effect until the SORN is final:

- o Routine use for sharing in pandemic health situations and
- o Testing of live data.

The Privacy Act has a provision for sharing personal information for health, and the individual must be notified of the sharing. In instances of analysis to determine pandemic health, it would only be appropriate to notify the individual if there was a risk, but DHS may need to share the information in order to conduct the analysis and make that determination.

From: Rosenzweig, Paul
Sent: Friday, November 03, 2006 9:46 AM
To: (b) (6); Agen, Jarrod
Cc: Richards, Rebecca
Subject: RE: Talking point on new ATS Fed Register Announcement

Suggest something along the following lines:

- o Screening like this has been going on for dozens of years in the air and sea environment and also in the land environment for selected cases
- o The ATS SORN does not announce any changes at all - it merely formalizes in a single place existing screening systems and rules
- o On the merits, it makes no sense at all to treat all travelers the same. In a world of limited resources we need to target our examination at those people who present the highest risk

From: McClain, Ellen (mailto:(b) (6))
Sent: Friday, November 03, 2006 10:28 AM
To: Richards, Rebecca; (b) (6)
Cc: Mortensen, Kenneth; Teufel, Hugo
Subject: RE: Talking points on ATS NEED INPUT

Becky,

I don't have any bullets but would appreciate an opportunity to review anything you put together. I read the article and was concerned about all the substantive legal inaccuracies about our legal authority at the border. While you are drafting yours I will try and put together a bullet or two from the legal border authority perspective. Thanks E

(b) (6)

Deputy Associate General Counsel (Enforcement) Department of Homeland Security

O: (b) (6)
Fax: (b) (6)

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 this message. Thank you.

From: Richards, Rebecca (b) (6)
Sent: Friday, November 03, 2006 9:50 AM

To: (b) (6)
Cc: Mortensen, Kenneth; Teufel, Hugo
Subject: Talking points on ATS NEED INPUT

All:

I am drafting TPS re the POST article. Particularly as it relates to the 40 years.
Anyone have something already written? Otherwise I am cribbing from what we have stated to OMB.

Becky

Rebecca J. Richards
Director Privacy Compliance
Privacy Office
Department of Homeland Security
Tel. (b) (6)
Email (b) (6)
See: www.dhs.gov/privacy

Adams, Frances G

From: Dinucci, Richard F
Sent: Thursday, December 07, 2006 5:04 PM
To: (b) (6)
Cc: Lovejoy, Michaeljohn; Ahern, Jayson P; Anthony, William A; Levy, Andrew; Isles, Adam
Subject: Re: Fw: ATS vis a vis DHS Appropriations Act prohibition
Importance: High
Attachments: ipatsapp.doc

(b) (6) please see attached.

RD
(See attached file: ipatsapp.doc)

(b) (6)

To

12/07/2006 04:48 PM

(b) (6)

Subject
Fw: ATS vis a vis DHS
Appropriations Act prohibition

need someone to review and respond asap to russ knocke (dhs pao) and bill anthony (cbp pao). ac and adam isles to be copied. thanks. marcy

----- Forwarded by (b) (6) on 12/07/2006 04:46 PM -----

"Ahern, Jayson P"

(b) (6)

To

12.07.2006 04:44 PM

(b) (6)

Subject
Fw: ATS vis a vis DHS
Appropriations Act prohibition

Sent from my BlackBerry Handheld.

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

From: "Knocke, William R" [William.R.Knocke@dhs.gov]
Sent: 12/07/2006 04:35 PM
To: "Isles, Adam" <Adam.Isles@dhs.gov>; "Ahern, Jayson P"
(b) (6) "Rosenzweig, Paul" (b) (6)
"Kraninger, Kathleen" (b) (6)
Cc: "Levy, Andrew" <Andrew.Levy@dhs.gov>; "Coldebella, Gus"
<Gus.Coldebella@dhs.gov>; "Scardaville, Michael"
(b) (6) "Baker, Stewart" (b) (6)
(b) (6)) (6) (b) (6)
(b) (6) (b) (6) (b) (6)
Subject: Re: ATS vis a vis DHS Appropriations Act prohibition

OGC is crashing on a statement but this is going to hit the wire soon. so
I'll take any and all bullets (does not have to be pretty or wordy)... just
need facts to push back with ASAP

Sent from my BlackBerry Wireless Handheld

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

From: Isles, Adam
To: Knocke, William R; Ahern, Jayson P; 'Rosenzweig, Paul'
(b) (6) Kraninger, Kathleen
Cc: 'Levy, Andrew' <Andrew.Levy@dhs.gov>; 'Coldebella, Gus'
<Gus.Coldebella@dhs.gov>; Scardaville, Michael; Baker, Stewart; (b) (6)
(b) (6)
Sent: Thu Dec 07 16:33:52 2006
Subject: RE: ATS vis a vis DHS Appropriations Act prohibition

This is just factually wrong ... do you have WHAT you need FROM OGC to try to
quash this, OR CAN WE HELP IN SOME ADDITIONAL WAY?

Adam Isles

Counselor to the Secretary

U.S. Department of Homeland Security

1/18/2007

000567

(b) (6) tel

From: Knocke, William R
Sent: Thursday, December 07, 2006 4:29 PM
To: Ahern, Jayson P; Isles, Adam; 'Rosenzweig, Paul'
Cc: 'Levy, Andrew'
Subject: FW: ATS vis a vis DHS Appropriations Act prohibition

FYI - AP is moving this story and the ACLU is pushing it hard right now. OGC is helping with a statement.

From: Sniffen, Michael [mailto:MSniffen@ap.org]
Sent: Thursday, December 07, 2006 3:23 PM
To: Knocke, William R
Subject: RE: ATS vis a vis DHS Appropriations Act prohibition

Russ.

Left you voicemails at your office and cell phones. We're going ahead today with piece in which some raise this possibility of a violation. Would very much like DHS' response in the story from the get-go. Writing the piece now.

Mike Sniffen

AP/Washington

776-9468

From: Knocke, William R [mailto:William.R.Knocke@dhs.gov]
Sent: Wednesday, December 06, 2006 7:56 PM
To: Sniffen, Michael
Subject: RE: ATS vis a vis DHS Appropriations Act prohibition

Let's talk tomorrow.

From: Sniffen, Michael [mailto:MSniffen@ap.org]
Sent: Wednesday, December 06, 2006 4:18 PM
To: Knocke, William R; (b) (6)

Re: Fw: ATS vis a vis DHS Appropriations Act prohibition

Page 4 of 6

Subject: ATS vis a vis DHS Appropriations Act prohibition

Russ, Bill--

Doesn't the ATS as used by CBP violate the DHS Appropriations Act and the Anti-Deficiency Act (which carries criminal penalties)?

Asst. Commissioner Ahern told me ATS was separate from checking names on watchlists and was designed to go beyond watchlists and target suspicious people who hadn't already come to law enforcement attention.

This is confirmed on page 9 of the DHS privacy impact assessment, which says:

"The ATS rules and resulting risk assessments are designed to signal to CBP officers that

further inspection of a person, shipment or conveyance may be warranted, even though an

individual may not have been previously associated with a law enforcement action or otherwise be

noted as a person of concern to law enforcement." (emphasis added)

-0-

The DHS Appropriations Act has contained the following section in 2005, 2006 and 2007 I understand. See particularly sec. 514(e) which is not limited by any reference to either TSA or Secure Flight like section 514(a) is. (I understand the 2004 appropriation had a limitation confined to TSA and CAPPS II).

Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441)

TITLE V: GENERAL PROVISIONS

SEC. 514. (a) None of the funds provided by this or previous appropriations Acts

may be obligated for deployment or implementation, on other than a test basis, of the

Secure Flight program or any other follow on or successor passenger prescreening

program, until the Secretary of Homeland Security certifies, and the Government

Accountability Office reports, to the Committees on Appropriations of the

1/18/2007

000569

Senate and

the House of Representatives, that all ten of the conditions contained in paragraphs (1)

through (10) of section 522(a) of Public Law 108-334 (118 Stat. 1319) have been

successfully met.

(b) The report required by subsection (a) shall be submitted within 90 days after

the Secretary provides the requisite certification, and periodically thereafter, if

necessary, until the Government Accountability Office confirms that all ten conditions

have been successfully met.

(c) Within 90 days of enactment of this Act, the Secretary shall submit to the

Committees on Appropriations of the Senate and the House of Representatives a detailed

plan that describes: (1) the dates for achieving key milestones, including the date or time

frames that the Secretary will certify the program under subsection (a); and (2) the

methodology to be followed to support the Secretary's certification, as required under

subsection (a).

(d) During the testing phase permitted by subsection (a), no information gathered

from passengers, foreign or domestic air carriers, or reservation systems may be used to

screen aviation passengers, or delay or deny boarding to such passengers, except in

instances where passenger names are matched to a Government watch list.

(e) None of the funds provided in this or previous appropriations Acts may be

utilized to develop or test algorithms assigning risk to passengers whose names are not

on Government watch lists.

(f) None of the funds provided in this or previous appropriations Acts may be

utilized for data or a database that is obtained from or remains under the

control of a

non-Federal entity: Provided, That this restriction shall not apply to
Passenger Name

Record data obtained from air carriers.

###

The information contained in this communication is intended for the use of the designated recipients named above. If the reader of this communication is not the intended recipient, you are hereby notified that you have received this communication in error, and that any review, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify The Associated Press immediately by telephone at +1-212-621-1898 and delete this email. Thank you.
[IP_US_DISC]

The information contained in this communication is intended for the use of the designated recipients named above. If the reader of this communication is not the intended recipient, you are hereby notified that you have received this communication in error, and that any review, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify The Associated Press immediately by telephone at +1-212-621-1898 and delete this email. Thank you.
[IP_US_DISC]

(b) (6)

From: Mortensen, Kenneth [Kenneth.Mortensen@dhs.gov]
Sent: Wednesday, November 29, 2006 7:03 PM
To: Levin, Toby M; Richards, Rebecca; Mortensen, Kenneth
Subject: Re: AP interview re ATS PIA

>I should share the reporter's questions which indicate that the PIA
>could have been more clear -- Is the list of data sources complete or
>does include mean there are other sources?

This is a good question and one we probably need to make sure we understand the answer for when we address the NPRM for the exemptions.

>So when does a traveler learn about the redress option? Does CBP have
>to give each traveler the IBIS notice or is it optional?

The answer for this actual came from CBP at a One-Stop Redress Communications WG that I attended. The IBIS notice is provided as a tearsheet or in some takeaway form for folks that go to secondary. In addition, the new redress process PLOR (Primary Lookout Override Record) is meant to be initiated by the CBP officer when someone clears secondary an identity mismatch.

>How can a person ask for redress if he doesn't know it is a right and
>can't ask for the data used to make the decision?

This is definitely something we must address in the exemption NPRM.

>Given that decisions are made about individuals, how can their access
>be exempt? This violates the Privacy Act.

Not necessarily. If an agency promulgates a rule to claim an exemption under (k) are absolutely correct. This section specifically provides that access must be to the individual if denied "any right, privilege, or benefit that he would other entitled by Federal law...."

But, if an agency promulgates a rule to claim exemptions under (j)(2), there is no such right for the individual. The qualifier for (j)(2) is that law enforcement must be the primary function of the agency (or component thereof). In our situation, CBP qualifies for the (j)(2) exemption.

Oh, and under (k)(5), the other (k) we usually see exemptions for, this is for the narrow purpose of security clearances.

HTH... Ken

Kenneth P. Mortensen
Acting Chief of Staff
Privacy Office
U.S. Department of Homeland Security

Sent from my BlackBerry and typed with my thumbs, so please make allowances for curtness and typos.

Levin, Toby

From: Richards, Rebecca (b) (6)
Sent: Thursday, October 12, 2006 4:49 PM
To: (b) (6) Richards, Rebecca; (b) (6)
Cc: Mortensen, Kenneth; (b) (6) Levin, Toby
Subject: RE: L Routine Use Justification

Attachments: Justification for Routine Use (L) (10-12-06) (PRIV kpm).doc



Justification for
Routine Use ...

While we are waiting for (b) (6) on exemptions, Ken and I reworked (b) (6) Routine Use L rebuttal. Redline is attached - clean is below. It isn't perfect, but

Justification for Routine Use (L)

OMB has objected to this routine use based on the fact that exemption (b) (8) of the Privacy Act appears to accomplish the same purpose and the fact that CBP may not exempt itself from the notice requirement simply by issuing a routine use under (b) (3). CBP proposed this new type of disclosure through a routine use statement to facilitate the disclosure of data from the ATS system to health officials (e.g., HHS, CDC, etc.) for use particularly in the context of significant threats to public health (pandemics, etc.). While prior health and safety threats for a specific individual involved the sharing of an individual's data between CBP with CDC pursuant to (b) (8), this proposed disclosure looks to understand health concerns on a broader context based on the expectations of the Administration in implementing its National Strategy for Pandemic Influenza by providing broader access to that data by health officials, which includes direct access for targeting of persons likely to be of high risk for the illness and analysis of exposure patterns. Under this information sharing environment, health officials access the ATS system to conduct a health risk analysis and assessment. The health official will need to review the underlying data to determine whether or not an actual significant health threat exists. As such, a notice to the individual based on the initial information sharing for health purposes could lead to wide spread panic and/or disruption, even though no actual health threat existed.

Additionally, to the extent a health official determines concretely that an individual is at risk for infection, it is expected that the individual would be contacted by the appropriate health officials (as opposed to CBP) to advise them of the situation and provide appropriate medical and health assistance; however, an individual whose records are accessed in connection with an outbreak investigation and enforcement of the quarantine laws, but who are ultimately determined not to be at risk, will not likely receive such notice from health officials, since that individual does not require contact and to do otherwise may not be appropriate. Contact tracing is one of the primary purposes for accessing data in ATS, which this proposed routine use would facilitate. Therefore, it is CBP's position that, as the facilitator, it should not be required to provide notice under the Privacy Act in making routine disclosures to health officials under these circumstances.

It should be noted that HHS has issued an NPRM to require carriers to provide HHS with data necessary for contract tracing, much of which it currently (and expects in the future to) obtain from CBP. The air carriers, in particular, have repeatedly objected to largely duplicative regulatory requirements which impose significant burden on the carriers. By providing HHS and related health officials with access to data already collected by CBP that is contained in ATS (and other CBP systems), the burden on the airlines is dramatically reduced. In addition, centralized access would permit appropriate controls for access to the data further enhancing privacy protections instead of operating multiple data streams that would provide inconsistent access.

It should be further noted that this routine use is entirely compatible with the purposes of collection. CBP is responsible for enforcing over 400 laws on behalf of over 40 different agencies, including the quarantine laws, pursuant to 42 USC 268(b).

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

From: (b) (6) (b) (6)
Sent: Thursday, October 12, 2006 4:42 PM
To: Richards, Rebecca; (b) (6)
Cc: Mortensen, Kenneth; (b) (6) Levin, Toby
Subject: RE: L Routine Use Justification

Becky,

When this revised version cobbled by committee is in a form such that you are about to send it to OMB can we please take one last quick look to see how all the pieces fit together? Thanks E

(b) (6)

Deputy Associate General Counsel (Enforcement) Department of Homeland Security

O: (b) (6)
Fax: (b) (6)

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 this message. Thank you.

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

From: Richards, Rebecca (b) (6)
Sent: Thursday, October 12, 2006 4:24 PM
To: (b) (6) Richards, Rebecca
Cc: (b) (6) Mortensen, Kenneth; (b) (6) Levin, Toby
Subject: RE: L Routine Use Justification

I added a few words to better more accurately capture - are you okay with this?

To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for purposes of ASSISTING SUCH AGENCIES IN preventing exposure to or transmission of a communicable or quarantinable disease or for combatting other significant public health threats.

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

From: (b) (6)
Sent: Thursday, October 12, 2006 4:05 PM
To: Richards, Rebecca
Cc: (b) (6) Mortensen, Kenneth; (b) (6)
Richards, Rebecca
Subject: RE: L Routine Use Justification

To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for purposes of preventing exposure to or transmission of a communicable or quarantinable disease or for combatting other significant public health threats.

(b) (6)

Office of Chief Counsel
U.S. Customs and Border Protection
Phone: (b) (6)
Fax: (b) (6)

Email: (b) (6)

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.

"Richards,

Rebecca"

To: (b) (6)

(b) (6)

"<Rebecca.Richards

(b) (6) "Richards, Rebecca"

@dhs.gov>

(b) (6) "Mortensen, Kenneth"

<Kenneth.Mortensen@dhs.gov>

10/12/2006 03:49

cc: (b) (6)

(b) (6)

PM

(b) (6)

(b) (6)

Subject: RE: L Routine

Use Justification

Don't forget to send me the specific changes to the language for L so that it doesn't track (b) (8).

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

From: (b) (6)

Sent: Thursday, October 12, 2006 3:05 PM

To: Richards, Rebecca; Mortensen, Kenneth

Cc: (b) (6)

Subject: L Routine Use Justification

(See attached file: Justification for Routine Use (L) (10-12-06).doc)

(b) (6)

Office of Chief Counsel

U.S. Customs and Border Protection

Phone: (b) (6)

Fax: (b) (6)

Email: (b) (6)

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.

Justification for Routine Use (L)

OMB has objected to this routine use based on the fact that exemption (b)(8) of the Privacy Act appears to accomplish the same purpose and the fact that CBP may not exempt itself from the notice requirement simply by issuing a routine use under (b)(3). CBP proposed this new type of disclosure through a routine use statement to facilitate the disclosure of data from the ATS system to health officials (e.g., HHS, CDC, etc.) for use particularly in the context of significant threats to public health (pandemics, etc.). While prior health and safety threats for a specific individual involved the sharing of an individual's data between CBP with CDC pursuant to (b)(8), this proposed disclosure looks to understand health concerns on a broader context based on the expectations of the Administration in implementing its National Strategy for Pandemic Influenza by providing broader access to that data by health officials, which includes direct access for targeting of persons likely to be of high risk for the illness and analysis of exposure patterns. Under this information sharing environment, health officials access the ATS system to conduct a health risk analysis and assessment. The health official will need to review the underlying data to determine whether or not an actual significant health threat exists. As such, a notice to the individual based on the initial information sharing for health purposes could lead to wide spread panic and/or disruption, even though no actual health threat existed.

Additionally, to the extent a health official determines concretely that an individual is at risk for infection, it is expected that the individual would be contacted by the appropriate health officials (as opposed to CBP) to advise them of the situation and provide appropriate medical and health assistance; however, an individual whose records are accessed in connection with an outbreak investigation and enforcement of the quarantine laws, but who are ultimately determined not to be at risk, will not likely receive such notice from health officials, since that individual does not require contact and to do otherwise may not be appropriate. Contact tracing is one of the primary purposes for accessing data in ATS, which this proposed routine use would facilitate. Therefore, it is CBP's position that, as the facilitator, it should not be required to provide notice under the Privacy Act in making routine disclosures to health officials under these circumstances.

It should be noted that HHS has issued an NPRM to require carriers to provide HHS with data necessary for contract tracing, much of which it currently (and expects in the future to) obtain from CBP. The air carriers, in particular, have repeatedly objected to largely duplicative regulatory requirements which impose significant burden on the carriers. By providing HHS and related health officials with access to data already collected by CBP that is contained in ATS (and other CBP systems), the burden on the airlines is dramatically reduced. In addition, centralized access would permit appropriate controls for access to the data further enhancing privacy protections instead of operating multiple data streams that would provide inconsistent access.

Deleted: .

Deleted: , has widespread

Deleted: a

Deleted: person's

Deleted: .

Deleted: is envisioned, including

(b)(5)

It should be further noted that this routine use is entirely compatible with the purposes of collection. CBP is responsible for enforcing over 400 laws on behalf of over 40 different agencies, including the quarantine laws, pursuant to 42 USC 268(b).

Deleted: If

03/22/2005 04:38

(b) (6)

PM

(b) (6)

(b) (6)

ATS-PIA, last revision, questions, and
12/28/2004 (Document link: (b) (6))

cc: (b) (6) /NE/USCS, LORRAINE

(b) (6) (b) (6)

(b) (6)

Subject: RE: Requested Documents regarding
responses --- RE: Revised ATS PIA

Becky,

Please find attached a revised version of the ATS-Maintenance PIA. We were able to address almost all of your questions and comments regarding the 3-1-2005 version. Based on our discussion today and review of our responses, there were four "outstanding" items that are detailed below. The first and second items are addressed in the revised version, however, you indicated that item 2 requires higher level DHS / CBP input for final resolution. Items 3 and 4 require input from outside of OIT that we are following up on. Any assistance in that area is appreciated (i.e., if you can forward the data access procedures, or come across the AES SORN).

(See attached file: CBP ATS PIA 03-22-2005 AZ.doc)

1) I was able to determine that the text about the CBP officer at the booth or in the inspection lanes communicating problems with ChoicePoint data should be removed at this time.

1.5. How will the information be checked for accuracy?

No further verification for accuracy will be conducted. No further verification for completeness will be conducted. ATS relies on the verifications for accuracy and completeness provided by the source systems of record.

(b)(2)high (b)(5) (b)(7)(E)

Question: Will you notify the driver if there appears to be a problem or will you give out the IBIS fact sheet?

(b)(2)high (b)(5) (b)(7)(E)

Added the following:
Upon request, CBP Officers will provide the IBIS fact sheet that provides information on appropriate redress.

Regarding the other outstanding items:

2) Higher level question about data retention period.

1.6. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

Yes. ATS builds a risk-based score for cargo and passengers based on criteria and rules developed by CBP. ATS maintains the risk score together with a record of which rules were used to develop the risk score. This score and related rules history associated with developing a risk-based score for an individual are maintained for up to fifty years to support ongoing targeting requirements. COMMENT: Need to provide a reason why we need to keep this data so long. I know it follows TECS, but since this getting its own SORN need to give a reason. We propose that you only maintain the risk score for those that are a high risk and delete the risk for all others crossing the border or archive the information so it is not readily accessible.

(b)(2)high (b)(5) (b)(7)(E)

- 3) We are still working on getting a copy of the January 31, 2005 data access procedures. 3.2. How will access to the data by a user be determined?

User data access is determined by the criteria, procedures, and controls documented in (b)(2)high (b)(7)(E)

This document thoroughly documents the ATS Security Desk procedures that define the quality control process to ensure and document checks and balances implemented to safeguard user access. Comment: this should be updated to the January 31, 2005 procedures.

- What are the January 28, 2005 procedures? (Review with Becky)
- ENF-1-FO-NTS ETS
- Issued by Charlie Bartoldus. Ask (b)(6) for them.

- 4) We are continuing to follow up on efforts to obtain the SORN for AES, but have not received it yet.

What is the SORN for the AES or the SEDs?

Please let us know if you have any follow-up questions. Also, if your comments and concerns have been addressed, can you please let us know if we can finalize the ATS-M PIA at this point and update it for the next budget submission once we are able to address outstanding items 3 and 4.

Thanks,

(b)(6)

(b)(6)

Sr. Financial Analyst
Department of Homeland Security
Bureau of Customs and Border Protection

(b)(6)

"Richards,
Rebecca"

(b) (6)

<Rebecca.Richards

(b) (6)

(b) (6)

(b) (6) "Elizabeth Withnell"

03/02/2005 04:43

(b) (6)

PM

ATS-PIA, last revision, questions, and

12/28/2004

To:

(b) (6)

(b) (6)

(b) (6)

cc:

(b) (6)

<Elizabeth.Withnell@dhs.gov>, (b) (6)

Subject: RE: Requested Documents regarding
responses --- RE: Revised ATS PIA

(b) (6)

I am attaching an updated version of the ATS-PIA. Please review and provide me with your thoughts. (b) (6) was going to seek a copy of the contract with Choicepoint to ensure that appropriate controls are in place and that CBP/DHS is aware of the contractual obligations related to the use of the DMV data.

An outstanding question for me, is whether the primary inspector at the land border will have access to the risk score, or will certain risk scores lead to specific statements within TECS. With ATS-P, you have at trained individual delving more into the reasons for the score, but not sure how you plan to implement this important step when you are at the land border and do not have the time you with most flights and ships.

Finally, a question with regards to information on packages being mailed internationally has been brought to my attention. USPS is apparently going to start sending CBP data and I am guessing this data is going to go into the ATS data base and be used by ATS-AT, if this is the case, then we may want to address this in the same PIA or do a second one for this change to the ATS system.

The timing for both of these from my perspective is early/mid April - but you may have sooner deadlines for the piloting for ATS-L. If so, please advise because the SORN needs to be drafted and approved for this program.

Thanks,
Becky

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

From: (b) (6)

Sent: Monday, January 31, 2005 10:10 AM

To: Richards, Rebecca

Cc: (b) (6)

Subject: Requested Documents regarding ATS-PIA, last revision, questions, and responses ---
RE: Revised ATS PIA 12/28/2004

Becky,

As requested, this is the email with your response to the last version of the ATS-PIA we provided. Your questions regarding ATS-L and ATS-P are embedded in this email. The printed document I gave you during out meeting Friday contained our answers to these questions. I am attaching 1) the 12-28 version of the ATS-PIA along with 2) our responses to your questions for your convenience.

1) Last version of the ATS-PIA (the only thing changed since you saw it was the date on the cover page which was corrected from 12/14/2004 to 12/28/2004.

(See attached file: CBP ATS PIA 12-28-2004 revised for review.doc)

2) Document with your questions extracted from email below together with responses:

(See attached file: Response to ATS PIA Questions regarding draft PIA dated 12-28-2004.doc)

Based on a short conversation with (b) (6) my understanding is that we can move everything forward directly with you up until the point where you indicate that the ATS-PIA is ready for submission to OMB. At that time, we will need to provide the final version to (b) (6) in ORR. I am pleased that this method is available as it should facilitate moving to final product with the ATS-PIA and the NIPS-PIA. I do need to reach back and get input to update the NIPS-PIA and expect to be able to provide you an updated version shortly.

As we discussed Friday, we will look for an email from you showing what revisions are needed and will be acceptable to go to final product for the ATS-PIA.

Thanks again for your help in moving this forward.

(b) (6)

(b) (6)

Sr. Financial Analyst
Department of Homeland Security
Bureau of Customs and Border Protection

(b) (6)

"Richards,

Rebecca"

To:

(b) (6)

(b) (6)

<Rebecca.Richards

cc:

(b) (6)

(b) (6)

"Elizabeth Withnell"

@dhs.gov>

<Elizabeth.Withnell@dhs.gov>

Subject: RE: Revised ATS PIA 12/28/2004

12/30/2004 03:00

PM

(b) (6)

Works for me to go through you. I was just finishing my note to the broader group, but am going to send it to you. You had mentioned in our conversation that if I needed more specifics on the DMV information that I would need to talk with Phil and Joseph. I am more than happy to do so, but that is the area where I feel like there isn't a good description of what CBP is receiving, how it will be reviewed, and what is done with it.

(b) (6)

(b) (6) have done a good draft with the PIA for ATS. After reading this PIA, I have a few high level questions about ATS-P and then some about the implementation of ATS-L. It may make more sense to sit down and meet to go over these.

General ATS-P. In reading the PIA and from my understanding of the system, ATS has two different functionalities. The first is that it takes source data from different older systems and creates an easy to use GUI interface. ATS as a GUI interface can and is used by a larger group of individuals who are viewing source data from TECS.

The second functionality is the scoring portion of ATS. As I read the PIA it appears that only CBP staff has access to the scoring portion of the system.

If I have properly captured the above, then this should be included in the discussion of ATS, as the privacy concerns decrease if ATS is used more broadly as an interface tool but different agencies but the scoring portion is limited to smaller group of CBP employees working at the National Targeting Center or PAUs.

ATS-P Specific. In the PIA it states specifically that there are no access provisions and information may not be updated because the system is not collecting information. For the PNR data that is stored in ATS, if the information is inaccurate and leads to an individual having to go to Secondary screening and that inaccurate information is used at a later junction, is there no way to update or amend the PNR?

ATS-L. The sections relating to the new use of information need to be more robust. If you have a contract with Choice Point or whoever is providing this data, we would like to see a copy. For the PIA, we would like to see specifically what data you are pulling from the State DMV data, what provisions you put in place in terms of data quality.

I have a few picky comments as well, but would really like to get a better hold on the ATS-L information before I get into pickiness.

Thanks,
Becky

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

From: (b) (6)
Sent: Thursday, December 30, 2004 2:51 PM
To: Richards, Rebecca
Cc: (b) (6)
Subject: RE: Revised ATS PIA 12/28/2004

Becky,

If it works better for you to go directly to the business sponsors, that is great. If you would prefer to work through OIT instead, just let us know. In any case, there is a need to confer with individuals other than myself to answer questions about these PIAs. I will support whatever works best for you...

Happy New Year

(b) (6)

(b) (6)

Sr. Financial Analyst
Department of Homeland Security
Bureau of Customs and Border Protection

(b) (6)

"Richards,

Rebecca"

(b) (6)

<Rebecca.Richards

@dhs.gov>

To:

(b) (6)

cc:

Subject: RE: Revised ATS

PIA 12/28/2004

12/30/2004 01:28

PM

I am going to send my comments to the broader group based on our conversation earlier this week, you wanted to defer to others on my questions about ATS-L.

Overall, it is looking really good. Thanks for your hard work on this.

Happy New Year.
Becky

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

From: (b) (6)
Sent: Thursday, December 30, 2004 11:38 AM
To: Richards, Rebecca
Cc: (b) (6)
Subject: RE: Revised ATS PIA 12/28/2004

Becky,

No, but they will receive a copy today.

(b) (6)

(b) (6)
Sr. Financial Analyst
Department of Homeland Security
Bureau of Customs and Border Protection

(b) (6)

"Richards,

Rebecca"

(b) (6)

<Rebecca.Richards

@dhs.gov>

PIA 12/28/2004

To: (b) (6)

cc:

Subject: RE: Revised ATS

12/30/2004 10:46

AM

(b) (6)

Has this PIA been reviewed by the folks over in OFO like (b) (6)

Happy New Year,
Thanks,
Becky

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

From: (b) (6)
Sent: Tuesday, December 28, 2004 11:35 AM
To: Richards, Rebecca
Cc: Elizabeth Withnell; (b) (6)
Subject: Revised ATS PIA 12/28/2004

Becky,

Here is the revised ATS PIA. I believe we have responded to all of your comments and we appreciate your assistance. Please let me know if you have any additional questions or revisions that would be required.

(See attached file: CBP ATS PIA 12-28-2004 revised for review.doc)

Thanks,

(b) (6)

(b) (6)
Sr. Financial Analyst
Department of Homeland Security
Bureau of Customs and Border Protection

(b) (6)

(See attached file: CBP ATS PIA3-1-2005 RR.doc)

(b) (6)

From: Agen, Jarrod [JARROD.Agen@dhs.gov]
Sent: Friday, December 08, 2006 12:04 PM
To: Knocke, William R; (b) (6) Coldebella, Gus; Perry, Phil; Levy, Andrew; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Sales, Nathan; Scardaville, Michael; Kraninger, Kathleen; (b) (6) Ahern, Jayson P
Cc: (b) (6) Klundt, Kelly R
Subject: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Please review this JUST THE FACTS response to AP article. Let me know if there are any errors or changes to be made. We will push it out in an about an hour.

Press Office
U.S. Department of Homeland Security

Just The Facts

Dec 8, 2006

ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

AN ASSOCIATED PRESS STORY CLAIMS THAT THE AUTOMATED TAGERTING SYSTEM (ATS) MAY VIOLATE U.S. LAW: "The Homeland Security Department's newly revealed computerized risk assessments of international travelers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years." (*"Traveler Risk System May Violate Ban"*, Associated Press 12/7/06)

BUT IT IS CLEAR THAT CONGRESS DID NOT INTEND TO LIMIT THE ATS PROGRAM:

- The Aviation and Transportation Security Act of 2001 mandates that each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to Customs an electronic transmission of a passenger manifest and carriers shall make passenger name record information available to the Customs Service.

THE STORY CLAIMS A PROVISION BY CONGRESS PROHIBITS COMPUTERIZED RISK ASSESSMENTS: "But they said a separate section, covering the entire department, was added to prevent any use of computerized risk assessment of people who are not already on watch lists." (*"Traveler Risk System May Violate Ban"*, Associated Press 12/7/06)

BUT THE PROVISION IN QUESTION DOES NOT RELATE TO ATS, INSTEAD REFERS TO A SEPARATE PROGRAM CALLED SECURE FLIGHT:

- The provision (Section 514 of DHS Appropriations Bill) is concerned only with the Secure Flight program, not ATS. While Secure Flight's focus is on the screening of domestic travelers prior to boarding, ATS is screens international travelers bound for the US to determine additional screening before admissibility. The two programs derive authority from different laws, and are administered by different agencies (CBP operates ATS, while Secure

Flight is a TSA program.

- For one thing, ATS has been in existence since the late 1990's. Because ATS predates the Secure Flight program developed by TSA, it is neither a "follow-on" nor "successor" program to Secure Flight, as required by section 514(a). As a matter of statutory interpretation, Congress is presumed to be aware of programs in existence when it passes legislation.
- Furthermore, Congress expressly exempted Passenger Name Record data from section 514's restrictions. The provisions states "this restriction shall not apply to Passenger Name Record data obtained from air carriers." Passenger Name Record Data is the most integral source for data used by ATS, a fact that was well known by Congress.

THE STORY ALSO CLAIMS THAT THERE HAS BEEN LITTLE NOTICE OF ATS: "ATS has operated with little public notice or understanding until a description was published last month in the Federal Register, a fine print compendium of federal rules. (*"Traveler Risk System May Violate Ban"*, Associated Press 12/7/06)

BUT DEPARTMENT OFFICIALS HAVE TESTIMIFIED BEFORE CONGRESS SEVERAL TIMES AND HAVE PROVIDED NUMEROUS STAFF BRIEFINGS AND TOURS OF THE ATS AND THE OPERATIONS AT THE NATIONAL TARGETING CENTER.

Excerpts from the nearly 20 written testimony about ATS to Congress 19 times since May 2003 include:

DHS Deputy Secretary Michael P. Jackson, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee (April 5, 2006): "ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry."

CBP Assistant Commissioner Jayson Ahern, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (March 28, 2006): "The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

CBP Assistant Commissioner Jayson Ahern, Written Testimony, Senate Committee on Judiciary, Subcommittee on Terrorism, Technology, and Homeland Security (September 7, 2006): "Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS

compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate bona fide travelers so it can focus its resources on areas of highest risk."

- **Former CBP Commissioner Robert Bonner, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 25, 2004):** "The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what cargo is "high risk," and therefore will be scrutinized at the port of entry or, in some cases, overseas.

CBP Executive Director, Traveler Security and Facilitation, Robert Jacksta, Written Testimony, Hearing before House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations (July 13, 2004): The Automated Targeting System-Passenger (ATS-P) is CBP's premier targeting tool in the passenger environment, and is available to CBP personnel at U.S. ports of entry nationwide. This system utilizes information from the National crime Information center (NCIC), the Treasury Enforcement Communications System (TECS), the Consular Lookout and Support System (CLASS) and other law enforcement databases to provide automated risk assessments on arriving international passengers.

[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 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.

Deleted: direct access to

Access to ATS-P 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.

Deleted: PNR

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 ATS-P rights 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.

Deleted: access

If you have any questions, please contact (b) (6) at (b) (6)

Sincerely,

[Executive Director, National Targeting and Security]

Enclosure [Field Guidelines for Use and Disclosure of PNR]

6th release
Voyager # 117
Date # 605-606

WIF
105
Draft

Executive Director, National Targeting and Security
Office of Field Operations
U.S. Customs and Border Protection
1300 Pennsylvania Avenue NW
Washington, DC 20229

[Salutation]

The [agency name] requests access to the Automated Targeting System-Passenger (ATS-P), a U.S. Customs and Border Protection (CBP) system that maintains Passenger Name Record (PNR) data from air carriers operating flights to, and from, the United States.

[Agency Name] certifies that it has received and reviewed a copy of the *Undertakings of the Department of Homeland Security, Bureau of Customs and Border Protection* ("Undertakings") dated May 11, 2004 (including the October 6, 2006 letter from Assistant Secretary Stewart Baker to the European Commission and European Union Presidency re-interpreting certain provisions of those Undertakings) and that [Agency Name] will comply fully with the provisions of the Undertakings as interpreted with respect to its access to PNR through CBP systems. [Agency Name] further certifies that it exercises responsibilities that require access to PNR data for purposes of preventing or combating terrorism and other serious transnational crimes as set forth in Paragraph 3 of the Undertakings. The [agency name]'s mission or responsibilities are as follows:

[Agency to insert language on its counter-terrorism mission or law enforcement functions.]

[Agency Name] only requests access for the data in connection with their official duties. [Agency Name] ensures that its access request list contains the names and titles of government employees; [Agency Name] will not request access for contract employees. [Agency Name] acknowledges that it has received and reviewed CBP's PNR Field Guidance [insert date] and will ensure that the employees listed below adhere to CBP's policies as set forth in the Field Guidance regarding access to, use and disclosure of PNR data. [Agency Name] further certifies that it has reviewed its internal policies and confirms that it intends to address and discipline improper use or disclosure of PNR data or access to ATS-P by its employees in a manner consistent with CBP's policies and procedures (as set forth in the Undertakings and Field Guidance).

[Agency Name] will ensure that CBP's rules for transfer of PNR information, including use of ATS-P's electronic accounting mechanism for disclosures, are properly followed, regardless of whether the disclosure is written or verbal. [Agency Name] understands that all access to ATS-P by its employees will be subject to the same auditing procedures as are applicable to access by CBP personnel.

[Agency Name] designates [name of contact person] as the point of contact for [agency name]'s PNR access and use of the program; the point of contact will also coordinate the dates and locations of all necessary training sessions with CBP and notify CBP of any disciplinary actions related to the inappropriate use or disclosure of PNR. Any questions regarding this request can be directed to [Agency's point of contact] at [phone number and e-mail address].

In addition to the list below, [agency name] is attaching a completed CBP Form 7300 for each user requesting access. [Agency Name] acknowledges the form is necessary to expedite the adjudication of clearance sufficient for access to ATS-P. [Agency to insert names, SSN or hash ID, job titles, office/ branch/ division/ agency/ department, location of office, supervisor's name and SSN or hash ID.]

Thank you for your consideration [or similar closing].

[Agency signatory, at least Director level]

Enclosure(s) [agency to include completed CBP Form(s) 7300]

b¹ riles -
Vanguard # 118
Bates # 607-608

WIF
b5
draft

Executive Director, National Targeting and Security
Office of Field Operations
U.S. Customs and Border Protection
1300 Pennsylvania Avenue NW
Washington, DC 20229

[Salutation]

The [agency name] requests access to the Automated Targeting System-Passenger (ATS-P), a U.S. Customs and Border Protection (CBP) system that maintains Passenger Name Record (PNR) data from air carriers operating flights to, and from, the United States.

[Agency Name] certifies that it has received and reviewed a copy of the *Undertakings of the Department of Homeland Security, Bureau of Customs and Border Protection* ("Undertakings") dated May 11, 2004 (including the October 6, 2006 letter from Assistant Secretary Stewart Baker to the European Commission and European Union Presidency re-interpreting certain provisions of those Undertakings) and that [Agency Name] will comply fully with the provisions of the Undertakings as interpreted with respect to its access to PNR through CBP systems. [Agency Name] further certifies that it exercises responsibilities that require access to PNR data for purposes of preventing or combating terrorism and other serious transnational crimes as set forth in Paragraph 3 of the Undertakings. The [agency name]'s mission or responsibilities are as follows:

[Agency to insert language on its counter-terrorism mission or law enforcement functions.]

[Agency Name] only requests access for the data in connection with their official duties. [Agency Name] ensures that its access request list contains the names and titles of government employees; [Agency Name] will not request access for contract employees. [Agency Name] acknowledges that it has received and reviewed CBP's PNR Field Guidance [insert date] and will ensure that the employees listed below adhere to CBP's policies as set forth in the Field Guidance regarding access to, use and disclosure of PNR data. [Agency Name] further certifies that it has reviewed its internal policies and confirms that it intends to address and discipline improper use or disclosure of PNR data or access to ATS-P by its employees in a manner consistent with CBP's policies and procedures (as set forth in the Undertakings and Field Guidance).

[Agency Name] will ensure that CBP's rules for transfer of PNR information, including use of ATS-P's electronic accounting mechanism for disclosures, are properly followed, regardless of whether the disclosure is written or verbal. [Agency Name] understands that all access to ATS-P by its employees will be subject to the same auditing procedures as are applicable to access by CBP personnel.

[Agency Name] designates [name of contact person] as the point of contact for [agency name]'s PNR access and use of the program; the point of contact will also coordinate the dates and locations of all necessary training sessions with CBP and notify CBP of any disciplinary actions related to the inappropriate use or disclosure of PNR. Any questions regarding this request can be directed to [Agency's point of contact] at [phone number and e-mail address].

In addition to the list below, [agency name] is attaching a completed CBP Form 7300 for each user requesting access. [Agency Name] acknowledges the form is necessary to expedite the adjudication of clearance sufficient for access to ATS-P. [Agency to insert names, SSN or hash ID, job titles, office/ branch/ division/ agency/ department, location of office, supervisor's name and SSN or hash ID.]

Thank you for your consideration [or similar closing].

[Agency signatory, at least Director level]

Enclosure(s) [agency to include completed CBP Form(s) 7300]

Dec 8, 2006

ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

AN ASSOCIATED PRESS STORY CLAIMS THAT THE AUTOMATED TARGETING SYSTEM (ATS) MAY VIOLATE U.S. LAW: "The Homeland Security Department's newly revealed computerized risk assessments of international travelers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years." (*"Traveler Risk System May Violate Ban"*, Associated Press 12/7/06)

BUT IT IS CLEAR THAT CONGRESS DID NOT INTEND TO LIMIT THE ATS PROGRAM:

- The Aviation and Transportation Security Act of 2001 mandates that each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to Customs an electronic transmission of a passenger manifest and carriers shall make passenger name record information available to the Customs Service.

THE STORY CLAIMS A PROVISION BY CONGRESS PROHIBITS COMPUTERIZED RISK ASSESSMENTS: "But they said a separate section, covering the entire department, was added to prevent any use of computerized risk assessment of people who are not already on watch lists." (*"Traveler Risk System May Violate Ban"*, Associated Press 12/7/06)

BUT WHEN READ IN CONTEXT, IT IS CLEAR THAT THE PROVISION WHICH SOME HAVE SUGGESTED WAS ADDED TO REGULATE ATS (SECTION 514 OF THE DHS APPROPRIATIONS BILL), HAS NOTHING TO DO WITH ATS, NOR WAS IT INTENDED AS A CATCH-ALL PROVISION:

- The various sections of the law cannot be read in isolation. Section 514 is concerned only with aviation security generally and the Secure Flight program administered by TSA in particular. Congress did not intend section 514 to pertain to ATS, a program that has been funded by Congress since the late 1990's and has an entirely different mission from Secure Flight. Secure Flight is intended to screen domestic passengers attempting to board airplanes, while ATS relates to individuals seeking admission to the U.S. at ports of entry.
- ATS has been in existence since the late 1990's. Congress is presumed to be aware of programs in existence when it passes legislation. The fact that Congress makes no mention of ATS undermines the suggestion that it intended to regulate it in any way. Because ATS predates the Secure Flight program and fulfills CBP's border security mission (rather than being focused strictly on aviation security), it can be neither a

(b)(5), High (b)(2), (b)(7)(E),
Low (b)(2)

"follow-on" nor "successor" program to Secure Flight, as required by section 514(a).

- Furthermore, the provision prohibits the use of DHS funds "for data or a database that is obtained from or remains under the control of a non-Federal entity," except Passenger Name Record Data obtained from air carriers. This provision only makes sense if it is limited to testing activities for Secure Flight. Otherwise, by this language, Congress would have made illegal any use of non-Federal database material by the federal government, thereby shutting down numerous legitimate programs having nothing to do with aviation security.

THE STORY ALSO CLAIMS THAT THERE HAS BEEN LITTLE NOTICE OF ATS: "ATS has operated with little public notice or understanding until a description was published last month in the Federal Register, a fine print compendium of federal rules. (*Traveler Risk System May Violate Ban*", Associated Press 12/7/06)

BUT DEPARTMENT OFFICIALS HAVE TESTIFIED BEFORE CONGRESS SEVERAL TIMES AND HAVE PROVIDED NUMEROUS STAFF BRIEFINGS AND TOURS OF THE OPERATIONS AT THE NATIONAL TARGETING CENTER (INCLUDING THE OPERATIONAL APPLICATION OF ATS).

Deleted: THE ATS AND

- Excerpts from the nearly 20 written testimony about ATS to Congress since May 2003 include:
 - **DHS Deputy Secretary Michael P. Jackson, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee (April 5, 2006):** "ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry."
 - **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (March 28, 2006):** "The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk." and should be scrutinized at the port of entry, or in some cases, overseas."
 - **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Senate Committee on Judiciary, Subcommittee on Terrorism, Technology, and Homeland Security (September 7, 2006):** "Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of

Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate bona fide travelers so it can focus its resources on areas of highest risk."

- **Former CBP Commissioner Robert Bonner, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 25, 2004):** "The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what cargo is "high risk," and therefore will be scrutinized at the port of entry or, in some cases, overseas.
- **CBP Executive Director, Traveler Security and Facilitation, Robert Jacksta, Written Testimony, Hearing before House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations (July 13, 2004):** The Automated Targeting System-Passenger (ATS-P) is CBP's premier targeting tool in the passenger environment, and is available to CBP personnel at U.S. ports of entry nationwide. This system utilizes information from the National Crime Information Center (NCIC), the Treasury Enforcement Communications System (TECS), the Consular Lookout and Support System (CLASS) and other law enforcement databases to provide automated risk assessments on arriving international passengers.

(b) (6)

From: (b) (6)
Sent: Wednesday, March 23, 2005 1:46 PM
To: Richards, Rebecca
Subject: TECS Training Frequency to include in ----> RE: Requested Documents regarding ATS-PIA, last revision, questions, and responses --- RE: Revised ATS PIA 12/28/2004

Attachments: CBP ATS PIA 03-22-2005 AZ.doc; CBP ATS PIA3-1-2005 RR.doc



CBP ATS PIA 3-22-2005 AZ.doc .3-1-2005 RR.doc (1)

Becky,

Just wanted to let you know that the document I sent yesterday did not include the frequency of the TECS training requirement in section 4.6. Sorry for the omission. The text is inserted below for reference.

Please let us know what the next steps are.

Thanks,

(b) (6)

4.6. What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?

A number of management, technical, and operational security controls are used to mitigate the risk of unauthorized monitoring. (b)(2)high (b)(7)(F)

(b)(2)high (b)(7)(E) Comment: Can you provide a little more summary of the education and training that occurs for all CBP officers as it relates to this point.

All CBP Officers are provided initial training that reviews authorized use of CBP IT systems and protection of data covered under the Privacy Act. Ongoing training and refresher courses are required (every six months or annually) that review security awareness (required CBP wide), NCIC certification, and TECS security procedures and privacy awareness (every two years).

(b)(2)high (b)(7)(E)

(b) (6)

Sr. Financial Analyst
Department of Homeland Security
Bureau of Customs and Border Protection

(b) (6)

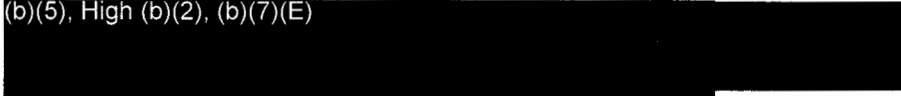
----- Forwarded by (b) (6) /NE/USCS on 03/23/2005 01:43 PM -----

(b) (6)

To: "Richards, Rebecca"

<Rebecca.Richards@dhs.gov>

Talking Points: FY07 Appropriations Act
Public Law 109-295
HR 5441

- CBP's Automated Targeting System has been in existence since the late 1990's. CBP has continuously worked to improve ATS and enhance our targeting processes to develop the most secure and efficient traveler entry and clearance process possible.
- ATS predates the Secure Flight program developed by TSA and is neither a "follow-on" nor a "successor" program to Secure Flight. While CBP continues to work with TSA to develop joint approaches to identify "No Fly" designees who attempt to board international flights, the ATS is specifically designed to meet the border security mission of CBP.
- ATS utilizes several name-matching algorithms to match potential high-risk travelers to established watch lists and government law enforcement databases. CBP regularly evaluates established rules to target previously unidentified high-risk travelers and refines them as appropriate based on current actionable intelligence and inspection results. CBP also develops new rules to enhance its targeting methodologies and address the intelligence threat stream.
- The rules evaluation and development process involves testing new or refined rules against pre-existing data to determine the effectiveness of the intelligence-based and other rules in isolating high-risk individuals, the potential impact on the traveling public, and the effects on CBP's inspectional resources at ports of entry.
- (b)(5), High (b)(2), (b)(7)(E)

Only after rules evaluations are completed and the results analyzed by subject matter experts are new rules introduced into the operational environment.