



Homeland Security

Privacy Office, Mail Stop 0550

February 1, 2007

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

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

Dear Mr. Sobel:

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

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the redress that is available to individuals who believe that the ATS contains or utilizes inaccurate, incomplete or outdated information about them.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

- b. Whether the underlying error rate of the government and private databases that will be used in the ATS to assign a risk level to an individual will not produce a large number of false positives that will result in a significant number of individuals being treated mistakenly or security resources being diverted;
- c. Whether the agency has stress-tested and demonstrated the efficacy and accuracy of all search tools in the ATS and has demonstrated that the ATS can make an accurate predictive assessment of those individuals who may constitute a threat;
- d. Whether the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which the ATS is being developed and prepared;
- e. Whether the agency has built in sufficient operational safeguards to reduce the opportunities for abuse;
- f. Whether substantial security measures are in place to protect the ATS from unauthorized access by hackers or other intruders;
- g. Whether the agency has adopted policies establishing effective oversight of the use and operation of the system;
- h. Whether there are no specific privacy concerns with the technological architecture of the system;
- i. Whether the agency has, pursuant to the requirements of section 44903(i)(2)(A) of Title 49, United States Code, modified the ATS with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger a high risk status; and
- j. Whether appropriate life-cycle estimates, expenditure and program plans exist.

Our November 7, 2007 letter summarized our processing of your request. Our searches directed to the DHS Office of the Executive Secretariat (ES), DHS Office of Policy (PLCY), DHS Privacy Office (PRIV), DHS Office of General Counsel (OGC), the Transportation Security Administration (TSA), and the U.S. Customs and Border Protection (CBP) have thus far produced a combined total of 1,295 pages. Out of those 1,295 pages, we provided you with a combined total of 843 pages with certain information withheld pursuant to the FOIA. We have continued to process your request within CBP.

A search directed to CBP has produced an additional 369 pages of records responsive to your request. We have determined that 162 pages are releasable to you in their entirety, 92 pages are releasable to you with certain information withheld pursuant to Exemptions 2, 5 and 6 of the FOIA, and 115 pages are withheld in their entirety pursuant to Exemptions 5 and 6 of the FOIA.

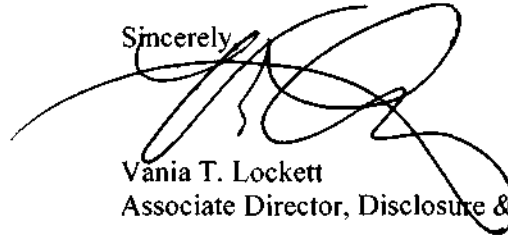
We further notified you in previous correspondence that while processing FOIA request number DHS/OS/PRIV 07-90/Hofmann request, documents originating with PLCY were found to be responsive to this request. We have partially completed our consultation with other offices concerning the additional supplemental PLCY documents and 40 pages are releasable to you with certain information withheld pursuant to Exemptions 2(high), 6, and 7E of the FOIA. We are continuing our consultations regarding several more supplemental PLCY documents and will respond to you once those consultations are complete.

Enclosed are 294 pages of releasable information. The withheld information, consists of names, telephone numbers, email addresses, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, and 7E of the FOIA, 5 U.S.C. §§ 552 (b)(2), (b)(5), (b)(6), and (b)(7)(E). Exemption 2(high) protects information applicable to internal administrative matters to the extent that disclosure would risk circumvention of an agency regulation or statute, impede the effectiveness of an agency's activities, or reveal sensitive information that may put the security and safety of an agency activity or employee at risk. Included within such information may be operating rules, guidelines, manuals of procedures for examiners or adjudicators, and homeland security information. Exemption 5 protects the integrity of the deliberative or policy-making processes within the

agency by exempting from mandatory disclosure opinion, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Exemption 7E protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

We are continuing to process your request as it pertains to additional supplemental PLCY documents, and the CBP Offices of the Chief Council and Information Technology. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-160/Sobel request**. This office can be reached at 866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely

A handwritten signature in black ink, appearing to read 'V. Lockett', with a large, stylized flourish extending to the right.

Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 294 pages

6/1/06
10:00 AM

Threshold Successes - Sample Cases

1. On () () arrived at Atlanta Hartsfield airport ()
() Both travelers are citizens of () who originally embarked in ()
() Based on API, PNR data for the current flight and previous travel patterns,
both were referred by ATS-P as Threshold Targeting hits.

Upon questioning by Atlanta's CTR team, both were referred to secondary for
inspection. Further questioning revealed () was a legal permanent resident who
was out of the US for 15 months. ()
() was placed in deportation proceedings. ()
was determined to be inadmissible to the US.

2. On May () 2006, () () a citizen of ()
arrived at Atlanta Hartsfield airport () Based on
API, PNR data for the current flight and previous travel patterns, () was referred
by ATS-P as a Threshold Targeting hit.

During initial questioning, CBP determined () visa was issued one week prior
to 9/11/01, yet had never traveled to the US. () profession was listed in his
() passport as "flight instructor." () intended purpose for travel to the
US was to () and to "see a man in New York for two days."
()
determined to be inadmissible to the US.

001666

204

~~For Official Use Only~~

1. Aviation & Border Security

- 5/15/05
2005/11/11
C/S
- On () a suspect was identified as traveling from () to () via () Upon pulling his PNR, another traveler was identified as traveling on the same reservation. DHS had no previous derogatory records on the second passenger. The () was removed from the United States and second subject was allowed to withdraw his application for admission. Similar cases have been found from () and ()
 - A series of PNR's generated by () in March 2005 identified linkages ()
 - On () CBP used PNR to identify linkages between () on the No-Fly list and a traveler ()
 - On March 11, 2005 CBP arrested two individuals for smuggling drugs from London to Chicago. Upon analyzing their PNR the use of a common credit card was found. Further analysis of this credit card's reservation history found a 3rd traveler had used the same card and listed a second credit card. Analysis of this new credit card number identified 3 additional travelers. 3 of the 4 new travelers where arrested during subsequent travel with drugs.
 - On () CBP analysis of PNR for a flight from () to Chicago identified 3 passengers that may have been seeking to use fraudulent travel documents. CBP alerted the air carrier who performed a thorough review of all three travelers documents prior to boarding. One was denied boarding by the airline. The two remaining travelers were referred to CBP secondary upon arrival in the United States. Both subjects were determined to be part of a human smuggling organization and they were smuggling the first subject. Additionally, one subject was identified as a member of the Yazuka crime syndicate.
 - In January 2003, CBP Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling cocaine between Venezuela and Miami. In this instance a corrupt ticket counter agent would identify a low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami were scheduled to remove the added bags from circulation prior to inspection by CBP in Miami.

7
~~For Official Use Only~~

- CBP has used PNR to identify practices adopted by users of fraudulent documents to identify the operation of a human smuggling ring in C

Global
beginning
to
b/c

2. USE of Pattern Analysis to Dismantle a Human Smuggling Operation

ICE Field Intelligence used PNR information to uncover an alien smuggling operation involved in smuggling Dominicans into the U.S. through various Ports of Entry. This work eventually resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, the disruption of an organization responsible for successfully smuggling thirty-seven individuals, and the increased awareness by CBP officers of a simple and highly effective alien smuggling technique. Details of the case are below:

On March 13, 2004, a woman named C. G. was arrested at Newark International Airport for attempted alien smuggling. She was escorting a Dominican national posing as C.G.'s son, and using her son's valid Puerto Rican birth certificate as his travel document. Although the imposter was removed and C.G. admitted that this was not the first time she had smuggled aliens in this way, prosecution was declined. At this point, the NE FIU analyst initiated research on her prior travel.

PNR information from her two known arrivals revealed that, in each case, she had traveled alone on the outbound segments from the U.S. to the Dominican Republic, but returned on the inbound portion of her reservation accompanied by travelers posing as her children. The "children" presented round trip tickets that indicated they were returning to their point of departure, but the outbound segments of their reservations had never actually been used.

The analyst identified three associates of C.G. who had each traveled outbound several times with her to the Dominican Republic. Their PNRs revealed the same pattern: the three associates returned to the U.S. with persons identified as their children, but the children had not traveled outbound before "returning." When APIS reported that the three were scheduled to return to the U.S. on separate flights within 48 hours, the analyst ensured that the travelers were intercepted.

M. P. was arrested on April 29, 2004, at Miami International Airport (MIA). M.P. was attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.P. was indicted on alien smuggling charges and the three minors were removed. (She is currently awaiting sentencing.)

On April 30, 2004, M. T. arrived and was arrested at MIA after attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.T. was indicted on alien smuggling charges and the three minors were deported. (M.T. has since been sentenced to five years in prison)

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 1042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001668

~~For Official Use Only~~

on these charges.) After her two associates were arrested, the third woman changed her reservation. She had been scheduled to fly into MLA with three children who had not been with her on her outbound trip. Instead, she arrived at San Juan International Airport alone but she had three extra suitcases with her after a one-week trip, indicating a probable last minute change of plans.

The analyst described the scheme in an Intelligence Alert, identifying the steps that Customs and Border Protection (CBP) Officers could take to reveal similar alien smuggling techniques. CBP Officers in San Juan informed the analyst that the information in the intelligence alert was responsible for their discoveries of three more smugglers, again using PNR information:

- Q. C. was arrested at San Juan International Airport (SJU) on May 24, 2004, while attempting to smuggle a Dominican national minor with a valid Puerto Rican birth certificate. Q.C. was indicted by SAC San Juan on alien smuggling charges and the minor was deported.
- Y. S. was arrested at SJU On June 13, 2004, while attempting to smuggle two Dominicans with Puerto Rican birth certificates. Y.S. was indicted by SAC San Juan and one minor was deported. The second was found to be a previously deported adult and he was also arrested.
- On July 16, 2004, M. C. was arrested at SJU while attempting to smuggle a Dominican minor with a Puerto Rican birth certificate. M.C. was indicted on alien smuggling charges and the minor was deported.

On July 17, 2004, S. B. was detained at Boston's Logan International Airport. S.B. was traveling with two suspected Dominican national minors with valid New York State birth certificates. S.B. had been identified by the San Juan Passenger Analysis Unit (PAU) as an associate of M.C. and a possible alien smuggler, but they had not referenced the detailed NEFIU report in the subject record. As a result, CBP officers in Boston did not believe they had enough evidence to detain the travelers so S.B. and the minors were released. The information has subsequently been turned over to ICE agents in Boston for investigation.

3. Use of Telephone Number Data Fields to Solve Stalled Cases

The effectiveness of subscriber information as an important investigative tool has been seriously compromised in recent years as new cell phone companies abound that will accept subscribers using fictitious identities. Many investigations have reached dead ends because there is no way to identify the parties actually making and receiving the calls. ICE recently had several successes because the fictitious subscribers' phones were used to make airline reservations for real people. A search of saved PNRs for the phone numbers led to the break-throughs. In some cases, the phone subscriber was the traveler,

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11642.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001009

~~For Official Use Only~~

and thus fully identified; in other cases, the subscriber was making reservations for drug couriers who were then identified and apprehended.

4. Use of Telephone Numbers to Identify User Identities and Clear Innocents

During a nine month investigation into a Vietnamese / US/Canadian MDMA smuggling organization, PNR information was used to identify actual users of phones for which we had previously received false subscriber information from the phone company. The information obtained from the PNR, not only helped to identify criminal targets, but also helped to clear individuals whose names were used as fake subscribers, and were not part of the criminal conspiracy

5. Pattern Analysis to Identify Sexual Predators

ICE Investigators learned of a suspected child sex predator ("Mr.X") planning a trip to Bangkok and believed to be affiliated with a particular travel agency that specialized in "Sex Tourism". Although no arrests have yet been made in this case, PNR research led to the identification of many additional potential sexual predators and their methods of operation:

- A review of all reservations on Mr. X's flight and on all other flights to the same destination from the New York City area within a one-week period led to the identification of other men who had booked travel with the same travel agency. (The travel agency booked each traveler separately and on a variety of flights as a way of protecting themselves and the others on the tour in case one of the men was a law enforcement target.)
- When Mr. X changed his reservation to leave from a West Coast city, a second travel agency was cited in the record. Reservations from the second city, naming the second travel agency, revealed many more potential targets for investigation.
- Mr. X's PNR identified the hotel he would be visiting in Bangkok, facilitating surveillance.
- It was subsequently learned that some of the men on the trip made new reservations after they arrived in Bangkok, for a side trip to Cambodia. Because there was no direct nexus to the U.S. on those trips, the PNRs were unavailable for research. It is believed that those men who were specifically interested in sex with children traveled on the Cambodian trip.

6. Use of PNR to Bolster APIS Analysis and Identify a Coconspirator

Information was gleaned from a Title III wire tap that "Harry" would be arriving on that day into the U.S. from Venezuela with heroin. A search was conducted in APIS and

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001670

For Official Use Only

ADIS on all flights from Venezuela into all US ports. A possible "Harry" was identified, and his reservation was obtained from CBP. Another individual was identified as ~~traveling on the same reservation~~, and both Harry C. and J. C. were arrested for conspiracy to distribute narcotics. Timely acquisition of all information from the PNR resulted in the success of the case.

7. Use of PNR to Support Early Identification

On January 20, 2006, agents assigned to the New York Organized Crime Drug Enforcement Strike Force arrested a money launderer for the Hells Angels Motorcycle Gang and other international narcotics organizations. M.T. allegedly laundered \$1 billion his clients accumulated doing everything from stock fraud to peddling the "date-rape" drug GHB, used by sexual predators, and then wire-transferred it to accounts in Texas, the Bahamas and elsewhere.

M.T. also invested millions of dollars in illegal proceeds from cocaine and hydroponic marijuana trafficking, mail fraud and additional securities-fraud schemes, court papers show He had been sought for years, but spent very little time in the U.S. and no specific travel information was ever available until after he had already left the country. In this instance, it was known that he was planning a brief meeting in New York City while en-route between Nassau, the Bahamas, and Canada. A massive PNR search found his reservation and agents were able to begin surveillance when he arrived at a New York area airport. They followed him to his meeting in the lobby of the Mandarin Oriental Hotel in New York City where he was arrested.

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD N042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001671

Global
b2 High
b7E

~~For Official Use Only~~

1. Aviation & Border Security

- > On () (), a suspect () was identified as traveling from () to () via () . Upon pulling his PNR, another traveler was identified as traveling on the same reservation. DHS had no previous derogatory records on the second passenger. The () was removed from the United States and second subject was allowed to withdraw his application for admission. Similar cases have been found from () and ()
- > A series of PNR's generated by () in March 2005 identified linkages ()
- > ()
- > On () CBP used PNR to identify linkages between () on the No-Fly list and a traveler ()
- > On March 11, 2005 CBP arrested two individuals for smuggling drugs from London to Chicago. Upon analyzing their PNR the use of a common credit card was found. Further analysis of this credit card's reservation history found a 3rd traveler had used the same card and listed a second credit card. Analysis of this new credit card number identified 3 additional travelers. 3 of the 4 new travelers were arrested during subsequent travel with drugs.
- > On () , CBP analysis of PNR for a flight from () to Chicago identified 3 passengers that may have been seeking to use fraudulent travel documents. CBP alerted the air carrier who performed a thorough review of all three travelers documents prior to boarding. One was denied boarding by the airline. The two remaining travelers were referred to CBP secondary upon arrival in the United States. Both subjects were determined to be part of a human smuggling organization and they were smuggling the first subject. Additionally, one subject was identified as a member of the Yazuka crime syndicate.
- > In January 2003, CBP Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling cocaine between Venezuela and Miami. In this instance a corrupt ticket counter agent would identify a low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami were scheduled to remove the added bags from circulation prior to inspection by CBP in Miami.

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001072

206

~~For Official Use Only~~

- 66661
b.2
b7E
- CBP has used PNR to identify practices adopted by users of fraudulent documents to identify the operation of a human smuggling ring in ()

2. USE of Pattern Analysis to Dismantle a Human Smuggling Operation

ICE Field Intelligence used PNR information to uncover an alien smuggling operation involved in smuggling Dominicans into the U.S. through various Ports of Entry. This work eventually resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, the disruption of an organization responsible for successfully smuggling thirty-seven individuals, and the increased awareness by CBP officers of a simple and highly effective alien smuggling technique. Details of the case are below:

On March 13, 2004, a woman named C. G. was arrested at Newark International Airport for attempted alien smuggling. She was escorting a Dominican national posing as C.G.'s son, and using her son's valid Puerto Rican birth certificate as his travel document. Although the imposter was removed and C.G. admitted that this was not the first time she had smuggled aliens in this way, prosecution was declined. At this point, the NE FIU analyst initiated research on her prior travel.

PNR information from her two known arrivals revealed that, in each case, she had traveled alone on the outbound segments from the U.S. to the Dominican Republic, but returned on the inbound portion of her reservation accompanied by travelers posing as her children. The "children" presented round trip tickets that indicated they were returning to their point of departure, but the outbound segments of their reservations had never actually been used.

The analyst identified three associates of C.G. who had each traveled outbound several times with her to the Dominican Republic. Their PNRs revealed the same pattern: the three associates returned to the U.S. with persons identified as their children, but the children had not traveled outbound before "returning." When APIS reported that the three were scheduled to return to the U.S. on separate flights within 48 hours, the analyst ensured that the travelers were intercepted.

M. P. was arrested on April 29, 2004, at Miami International Airport (MIA). M.P. was attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.P. was indicted on alien smuggling charges and the three minors were removed. (She is currently awaiting sentencing.)

On April 30, 2004, M. T. arrived and was arrested at MIA after attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.T. was indicted on alien smuggling charges and the three minors were deported. (M.T. has since been sentenced to five years in prison)

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001673

~~For Official Use Only~~

on these charges.) After her two associates were arrested, the third woman changed her reservation. She had been scheduled to fly into MIA with three children who had not been with her on her outbound trip. Instead, she arrived at San Juan International Airport alone but she had three extra suitcases with her after a one-week trip, indicating a probable last minute change of plans.

The analyst described the scheme in an Intelligence Alert, identifying the steps that Customs and Border Protection (CBP) Officers could take to reveal similar alien smuggling techniques. CBP Officers in San Juan informed the analyst that the information in the intelligence alert was responsible for their discoveries of three more smugglers, again using PNR information:

- Q. C. was arrested at San Juan International Airport (SJU) on May 24, 2004, while attempting to smuggle a Dominican national minor with a valid Puerto Rican birth certificate. Q.C. was indicted by SAC San Juan on alien smuggling charges and the minor was deported.
- Y. S. was arrested at SJU On June 13, 2004, while attempting to smuggle two Dominicans with Puerto Rican birth certificates. Y.S. was indicted by SAC San Juan and one minor was deported. The second was found to be a previously deported adult and he was also arrested.
- On July 16, 2004, M. C. was arrested at SJU while attempting to smuggle a Dominican minor with a Puerto Rican birth certificate. M.C. was indicted on alien smuggling charges and the minor was deported.

On July 17, 2004, S. B. was detained at Boston's Logan International Airport. S.B. was traveling with two suspected Dominican national minors with valid New York State birth certificates. S.B. had been identified by the San Juan Passenger Analysis Unit (PAU) as an associate of M.C. and a possible alien smuggler, but they had not referenced the detailed NEFIU report in the subject record. As a result, CBP officers in Boston did not believe they had enough evidence to detain the travelers so S.B. and the minors were released. The information has subsequently been turned over to ICE agents in Boston for investigation.

3. Use of Telephone Number Data Fields to Solve Stalled Cases

The effectiveness of subscriber information as an important investigative tool has been seriously compromised in recent years as new cell phone companies abound that will accept subscribers using fictitious identities. Many investigations have reached dead ends because there is no way to identify the parties actually making and receiving the calls. ICE recently had several successes because the fictitious subscribers' phones were used to make airline reservations for real people. A search of saved PNRs for the phone numbers led to the break-throughs. In some cases, the phone subscriber was the traveler,

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001674

~~For Official Use Only~~

and thus fully identified; in other cases, the subscriber was making reservations for drug couriers who were then identified and apprehended.

4. Use of Telephone Numbers to Identify User Identities and Clear Innocents

During a nine month investigation into a Vietnamese / US/Canadian MDMA smuggling organization, PNR information was used to identify actual users of phones for which we had previously received false subscriber information from the phone company. The information obtained from the PNR, not only helped to identify criminal targets, but also helped to clear individuals whose names were used as fake subscribers, and were not part of the criminal conspiracy

5. Pattern Analysis to Identify Sexual Predators

ICE Investigators learned of a suspected child sex predator ("Mr.X") planning a trip to Bangkok and believed to be affiliated with a particular travel agency that specialized in "Sex Tourism". Although no arrests have yet been made in this case, PNR research led to the identification of many additional potential sexual predators and their methods of operation:

- A review of all reservations on Mr. X's flight and on all other flights to the same destination from the New York City area within a one-week period led to the identification of other men who had booked travel with the same travel agency. (The travel agency booked each traveler separately and on a variety of flights as a way of protecting themselves and the others on the tour in case one of the men was a law enforcement target.)
- When Mr. X changed his reservation to leave from a West Coast city, a second travel agency was cited in the record. Reservations from the second city, naming the second travel agency, revealed many more potential targets for investigation.
- Mr. X's PNR identified the hotel he would be visiting in Bangkok, facilitating surveillance.
- It was subsequently learned that some of the men on the trip made new reservations after they arrived in Bangkok, for a side trip to Cambodia. Because there was no direct nexus to the U.S. on those trips, the PNRs were unavailable for research. It is believed that those men who were specifically interested in sex with children traveled on the Cambodian trip.

6. Use of PNR to Bolster APIS Analysis and Identify a Coconspirator

Information was gleaned from a Title III wire tap that "Harry" would be arriving on that day into the U.S. from Venezuela with heroin. A search was conducted in APIS and

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1 relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001875

~~For Official Use Only~~

ADIS on all flights from Venezuela into all US ports. A possible "Harry" was identified, and his reservation was obtained from CBP. Another individual was identified as traveling on the same reservation, and both Harry C. and J. C. were arrested for conspiracy to distribute narcotics. Timely acquisition of all information from the PNR resulted in the success of the case.

7. Use of PNR to Support Early Identification

On January 20, 2006, agents assigned to the New York Organized Crime Drug Enforcement Strike Force arrested a money launderer for the Hells Angels Motorcycle Gang and other international narcotics organizations. M.T. allegedly laundered \$1 billion his clients accumulated doing everything from stock fraud to peddling the "date-rape" drug GHB, used by sexual predators, and then wire-transferred it to accounts in Texas, the Bahamas and elsewhere.

M.T. also invested millions of dollars in illegal proceeds from cocaine and hydroponic marijuana trafficking, mail fraud and additional securities-fraud schemes, court papers show. He had been sought for years, but spent very little time in the U.S. and no specific travel information was ever available until after he had already left the country. In this instance, it was known that he was planning a brief meeting in New York City while en-route between Nassau, the Bahamas, and Canada. A massive PNR search found his reservation and agents were able to begin surveillance when he arrived at a New York area airport. They followed him to his meeting in the lobby of the Mandarin Oriental Hotel in New York City where he was arrested.

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 1042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001876

~~For Official Use Only~~

Aviation & Border Security Applications

(Note: The following examples have not been cleared by CBP for public release)

- 3500
CO
OK
- On () () arrived at Atlanta Hartsfield airport. Both travelers are citizens of () who originally embarked in (). Based on API, PNR data for the current flight and previous travel patterns, both were referred by ATS-P as (). Further questioning revealed () was a legal permanent resident who was out of the US for 15 months. () was placed in deportation proceedings.
 - On May () 2006, () a citizen of Pakistan, arrived at Atlanta Hartsfield airport on (). Based on API, PNR data for the current flight and previous travel patterns, () was referred by ATS-P as a Threshold Targeting hit. CBP determined () visa was issued one week prior to 9/11/01, yet had never traveled to the US. () profession was listed in his () passport as "flight instructor." () intended purpose for travel to the US was to () and to "see a man in New York for two days." () was placed in deportation proceedings.
 - On () subjects - () traveled () into Atlanta-Hartsfield Airport and applied for admission ()

- On () Minneapolis apprehended an F1 student from (). The student was identified as () was targeted by the PAU during ATS queries. ()

() FBI Agents and an FBI interpreter examined the computer and drives. A file on the computer contained a

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001577

~~For Official Use Only~~

b2
b7E

video on ([redacted]) The file also contained images of [redacted] .
[redacted]) The file also contained photos of [redacted] .
[redacted] Other thumbnail drives were found to contain images [redacted] .
[redacted] The JTTF summoned a special team from FBI Headquarters in
Washington DC to interview [redacted]) US Attorney's office charged
[redacted]) with making false statements. As of 12/06/2006, [redacted])

- CBP Officers at Minneapolis St. Paul apprehended [redacted]) JTTF and FBI responded with Agents and a computer specialist team. Passenger [redacted])

[redacted]) During CBP interview and research, it was determined that [redacted])
[redacted]) admitted to being arrested and convicted on terrorist related charges at the age of 19. [redacted]) originally claimed credible fear but recanted and he was expeditiously removed from the U.S.

- The subject arrived unaccompanied from [redacted])

[redacted]) The subject was determined inadmissible as an immigrant without an immigrant visa.

- On [redacted]) at approximately 2100 hours subjects [redacted]) and applied for admission as Visa Waiver applicants. Both subjects were ATS-P lookouts. During secondary one subject stated that he was traveling to the U.S. on business [redacted])

Both subjects were refused admission under 212(a)(7)(A)(i)(I) Immigrant not in possession of valid travel document since they not able to prove that they were bonafide applicants.

Global
B-2
b7E

~~For Official Use Only~~

- > In [redacted] as a result of ATS Miami PAU targeted numerous passengers that required additional scrutiny prior to boarding an aircraft from [redacted] to Miami. Ultimately, [redacted] diverted the aircraft to the Dominican Republic and identified 11 undocumented Cubans aboard the aircraft. [redacted] returned to [redacted] and removed the undocumented Cubans.
- > On [redacted] During the examination of the subject's luggage, \$144,895 was discovered within pairs of jeans in the subject's luggage.
- > On [redacted] a suspect [redacted] was identified as traveling from [redacted] to [redacted] via [redacted]. Upon pulling his PNR, another traveler was identified as traveling on the same reservation. DHS had no previous derogatory records on the second passenger. The [redacted] was removed from the United States and second subject was allowed to withdraw his application for admission. Similar cases have been found from [redacted] and [redacted].
- > A series of PNR's generated by a [redacted] in March 2005 identified linkages [redacted]
- > [redacted]
- > On [redacted] CBP used PNR to identify linkages between an [redacted] on the No-Fly list and a traveler [redacted].
- > On March 11, 2005 CBP arrested two individuals for smuggling drugs from London to Chicago. Upon analyzing their PNR the use of a common credit card was found. Further analysis of this credit card's reservation history found a 3rd traveler had used the same card and listed a second credit card. Analysis of this new credit card number identified 3 additional travelers. 3 of the 4 new travelers were arrested during subsequent travel with drugs.
- > On [redacted] CBP analysis of PNR for a flight from [redacted] Chicago identified 3 passengers that may have been seeking to use fraudulent travel documents. CBP alerted the air carrier who performed a thorough review of all three travelers documents prior to boarding. One was denied boarding by the airline. The two remaining travelers were referred to CBP secondary upon arrival in the United States. Both subjects were determined to be part of a human smuggling organization and they were smuggling the first subject. Additionally, one subject was identified as a member of the Yazuka crime syndicate.

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001879

~~For Official Use Only~~

- 6/10/01
b2
b7E
- In January 2003, CBP Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling cocaine between Venezuela and Miami. In this instance a corrupt ticket counter agent would identify a low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami were scheduled to remove the added bags from circulation prior to inspection by CBP in Miami.
 - CBP has used PNR to identify practices adopted by users of fraudulent documents to identify the operation of a human smuggling ring in ()

Investigatory Applications

(Note: The following examples have been cleared by CBP for public release)

1. USE of Pattern Analysis to Dismantle a Human Smuggling Operation

ICE Field Intelligence used PNR information to uncover an alien smuggling operation involved in smuggling Dominicans into the U.S. through various Ports of Entry. This work eventually resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, the disruption of an organization responsible for successfully smuggling thirty-seven individuals, and the increased awareness by CBP officers of a simple and highly effective alien smuggling technique. Details of the case are below:

On March 13, 2004, a woman named C. G. was arrested at Newark International Airport for attempted alien smuggling. She was escorting a Dominican national posing as C.G.'s son, and using her son's valid Puerto Rican birth certificate as his travel document. Although the imposter was removed and C.G. admitted that this was not the first time she had smuggled aliens in this way, prosecution was declined. At this point, the NE FIU analyst initiated research on her prior travel.

PNR information from her two known arrivals revealed that, in each case, she had traveled alone on the outbound segments from the U.S. to the Dominican Republic, but returned on the inbound portion of her reservation accompanied by travelers posing as her children. The "children" presented round trip tickets that indicated they were returning to their point of departure, but the outbound segments of their reservations had never actually been used.

The analyst identified three associates of C.G. who had each traveled outbound several times with her to the Dominican Republic. Their PNRs revealed the same pattern: the three associates returned to the U.S. with persons identified as their children, but the children had not traveled outbound before "returning." When APIS reported that the three were

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001880

For Official Use Only

scheduled to return to the U.S. on separate flights within 48 hours, the analyst ensured that the travelers were intercepted.

M. P. was arrested on April 29, 2004, at Miami International Airport (MIA). M.P. was attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.P. was indicted on alien smuggling charges and the three minors were removed. (She is currently awaiting sentencing.)

On April 30, 2004, M. T. arrived and was arrested at MIA after attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.T. was indicted on alien smuggling charges and the three minors were deported. (M.T. has since been sentenced to five years in prison on these charges.) After her two associates were arrested, the third woman changed her reservation. She had been scheduled to fly into MIA with three children who had not been with her on her outbound trip. Instead, she arrived at San Juan International Airport alone but she had three extra suitcases with her after a one-week trip, indicating a probable last minute change of plans.

The analyst described the scheme in an Intelligence Alert, identifying the steps that Customs and Border Protection (CBP) Officers could take to reveal similar alien smuggling techniques. CBP Officers in San Juan informed the analyst that the information in the intelligence alert was responsible for their discoveries of three more smugglers, again using PNR information:

- Q. C. was arrested at San Juan International Airport (SJU) on May 24, 2004, while attempting to smuggle a Dominican national minor with a valid Puerto Rican birth certificate. Q.C. was indicted by SAC San Juan on alien smuggling charges and the minor was deported.
- Y. S. was arrested at SJU On June 13, 2004, while attempting to smuggle two Dominicans with Puerto Rican birth certificates. Y.S. was indicted by SAC San Juan and one minor was deported. The second was found to be a previously deported adult and he was also arrested.
- On July 16, 2004, M. C. was arrested at SJU while attempting to smuggle a Dominican minor with a Puerto Rican birth certificate. M.C. was indicted on alien smuggling charges and the minor was deported.

On July 17, 2004, S. B. was detained at Boston's Logan International Airport. S.B. was traveling with two suspected Dominican national minors with valid New York State birth certificates. S.B. had been identified by the San Juan Passenger Analysis Unit (PAU) as an associate of M.C. and a possible alien smuggler, but they had not referenced the detailed NEFIU report in the subject record. As a result, CBP officers in Boston did not believe

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001861

For Official Use Only

they had enough evidence to detain the travelers so S.B. and the minors were released. The information has subsequently been turned over to ICE agents in Boston for investigation.

2. Use of Telephone Number Data Fields to Solve Stalled Cases

The effectiveness of subscriber information as an important investigative tool has been seriously compromised in recent years as new cell phone companies abound that will accept subscribers using fictitious identities. Many investigations have reached dead ends because there is no way to identify the parties actually making and receiving the calls. ICE recently had several successes because the fictitious subscribers' phones were used to make airline reservations for real people. A search of saved PNRs for the phone numbers led to the break-throughs. In some cases, the phone subscriber was the traveler, and thus fully identified; in other cases, the subscriber was making reservations for drug couriers who were then identified and apprehended.

3. Use of Telephone Numbers to Identify User Identities and Clear Innocents

During a nine month investigation into a Vietnamese / US/Canadian MDMA smuggling organization, PNR information was used to identify actual users of phones for which we had previously received false subscriber information from the phone company. The information obtained from the PNR, not only helped to identify criminal targets, but also helped to clear individuals whose names were used as fake subscribers, and were not part of the criminal conspiracy

4. Pattern Analysis to Identify Sexual Predators

ICE Investigators learned of a suspected child sex predator ("Mr.X") planning a trip to Bangkok and believed to be affiliated with a particular travel agency that specialized in "Sex Tourism". Although no arrests have yet been made in this case, PNR research led to the identification of many additional potential sexual predators and their methods of operation:

- A review of all reservations on Mr. X's flight and on all other flights to the same destination from the New York City area within a one-week period led to the identification of other men who had booked travel with the same travel agency. (The travel agency booked each traveler separately and on a variety of flights as a way of protecting themselves and the others on the tour in case one of the men was a law enforcement target.)
- When Mr. X changed his reservation to leave from a West Coast city, a second travel agency was cited in the record. Reservations from the second city, naming the second travel agency, revealed many more potential targets for investigation.

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001682

For Official Use Only

- Mr. X's PNR identified the hotel he would be visiting in Bangkok, facilitating surveillance.

- It was subsequently learned that some of the men on the trip made new reservations after they arrived in Bangkok, for a side trip to Cambodia. Because there was no direct nexus to the U.S. on those trips, the PNRs were unavailable for research. It is believed that those men who were specifically interested in sex with children traveled on the Cambodian trip.

5. Use of PNR to Bolster APIS Analysis and Identify a Coconspirator

Information was gleaned from a Title III wire tap that "Harry" would be arriving on that day into the U.S. from Venezuela with heroin. A search was conducted in APIS and ADIS on all flights from Venezuela into all US ports. A possible "Harry" was identified, and his reservation was obtained from CBP. Another individual was identified as traveling on the same reservation, and both Harry C. and J. C. were arrested for conspiracy to distribute narcotics. Timely acquisition of all information from the PNR resulted in the success of the case.

6. Use of PNR to Support Early Identification

On January 20, 2006, agents assigned to the New York Organized Crime Drug Enforcement Strike Force arrested a money launderer for the Hells Angels Motorcycle Gang and other international narcotics organizations. M.T. allegedly laundered \$1 billion his clients accumulated doing everything from stock fraud to peddling the "date-rape" drug GHB, used by sexual predators, and then wire-transferred it to accounts in Texas, the Bahamas and elsewhere.

M.T. also invested millions of dollars in illegal proceeds from cocaine and hydroponic marijuana trafficking, mail fraud and additional securities-fraud schemes, court papers show He had been sought for years, but spent very little time in the U.S. and no specific travel information was ever available until after he had already left the country. In this instance, it was known that he was planning a brief meeting in New York City while en-route between Nassau, the Bahamas, and Canada. A massive PNR search found his reservation and agents were able to begin surveillance when he arrived at a New York area airport. They followed him to his meeting in the lobby of the Mandarin Oriental Hotel in New York City where he was arrested.

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001883

b2
b7c

~~For Official Use Only~~

Aviation & Border Security Applications

(Note: The following examples have not been cleared by CBP for public release)

- On () (b6) and (b6) arrived at Atlanta Hartsfield airport () Both travelers are citizens of () who originally embarked in () Based on API, PNR data for the current flight and previous travel patterns, both were referred by ATS-P as () Further questioning revealed (b6) was a legal permanent resident who was out of the US for 15 months. (b6) () was placed in deportation proceedings.
- On May () 2006, () citizen of () arrived at Atlanta Hartsfield airport on () Based on API, PNR data for the current flight and previous travel patterns, (b6) was referred by ATS-P as a Threshold Targeting hit. CBP determined (b6) visa was issued one week prior to 9/11/01, yet had never traveled to the US. (b6) profession was listed in his () passport as "flight instructor." (b6) intended purpose for travel to the US was to (b6) and to "see a man in New York for two days." () was placed in deportation proceedings.
- On () subjects - (b6) () into Atlanta-Hartsfield Airport and applied for admission () ()
- On () Minneapolis apprehended an F1 student from () The student was identified as () was targeted by the PAU during ATS queries. (b6) ()

() FBI Agents and an FBI interpreter examined the computer and drives. A file on the computer contained a video on () The file also contained images of (b6) ()

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001084

~~For Official Use Only~~

b2
b7c

() The file also contained photos ()
() Other thumbnail drives were found to contain images ()
() The JTTF summoned a special team from FBI Headquarters in Washington DC to interview (b6) US Attorney's office charged (b6) with making false statements. As of 12/06/2006, (b6)

> CBP Officers at Minneapolis St. Paul apprehended ()
() JTTF and FBI responded with Agents and a computer specialist team. Passenger (b6)

() During CBP interview and research, it was determined that (b6)
(b6) admitted to being arrested and convicted on terrorist related charges at the age of 19. (b6)
(b6) originally claimed credible fear but recanted and he was expeditiously removed from the U.S.

> The subject arrived unaccompanied from ()
(b6)

() The subject was determined inadmissible as an immigrant without an immigrant visa.

> On () at approximately 2100 hours subjects (b6)

() and applied for admission as Visa Waiver applicants. Both subjects were ATS-P lookouts. During secondary one subject stated that he was traveling to the U.S. on business ()

() Both subjects were refused admission under 212(a)(7)(A)(i)(I) Immigrant not in possession of valid travel document since they not able to prove that they were bonafide applicants.

> In () as a result of ATS Miami PAU targeted numerous passengers that required additional scrutiny prior to boarding an aircraft from () to Miami. Ultimately, () diverted the aircraft to the Dominican Republic and

WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 110421, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

001885

Global
b2
b7E

~~For Official Use Only~~

corrupt ticket counter agent would identify a low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami were scheduled to remove the added bags from circulation prior to inspection by CBP in Miami.

- CBP has used PNR to identify practices adopted by users of fraudulent documents to identify the operation of a human smuggling ring in (

- b2 high, b7E)

Investigatory Applications

(Note: The following examples have been cleared for public release)

1. USE of Pattern Analysis to Dismantle a Human Smuggling Operation

ICE Field Intelligence used PNR information to uncover an alien smuggling operation involved in smuggling Dominicans into the U.S. through various Ports of Entry. This work eventually resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, the disruption of an organization responsible for successfully smuggling thirty-seven individuals, and the increased awareness by CBP officers of a simple and highly effective alien smuggling technique. Details of the case are below:

On March 13, 2004, a woman named C. G. was arrested at Newark International Airport for attempted alien smuggling. She was escorting a Dominican national posing as C.G.'s son, and using her son's valid Puerto Rican birth certificate as his travel document. Although the imposter was removed and C.G. admitted that this was not the first time she had smuggled aliens in this way, prosecution was declined. At this point, the NE FIU analyst initiated research on her prior travel.

PNR information from her two known arrivals revealed that, in each case, she had traveled alone on the outbound segments from the U.S. to the Dominican Republic, but returned on the inbound portion of her reservation accompanied by travelers posing as her children. The "children" presented round trip tickets that indicated they were returning to their point of departure, but the outbound segments of their reservations had never actually been used.

The analyst identified three associates of C.G. who had each traveled outbound several times with her to the Dominican Republic. Their PNRs revealed the same pattern: the three associates returned to the U.S. with persons identified as their children, but the children had not traveled outbound before "returning." When APIS reported that the three were scheduled to return to the U.S. on separate flights within 48 hours, the analyst ensured that the travelers were intercepted.

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001087

~~For Official Use Only~~

M. P. was arrested on April 29, 2004, at Miami International Airport (MIA). M.P. was attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.P. was indicted on alien smuggling charges and the three minors were removed. (She is currently awaiting sentencing.)

On April 30, 2004, M. T. arrived and was arrested at MIA after attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.T. was indicted on alien smuggling charges and the three minors were deported. (M.T. has since been sentenced to five years in prison on these charges.) After her two associates were arrested, the third woman changed her reservation. She had been scheduled to fly into MIA with three children who had not been with her on her outbound trip. Instead, she arrived at San Juan International Airport alone but she had three extra suitcases with her after a one-week trip, indicating a probable last minute change of plans.

The analyst described the scheme in an Intelligence Alert, identifying the steps that Customs and Border Protection (CBP) Officers could take to reveal similar alien smuggling techniques. CBP Officers in San Juan informed the analyst that the information in the intelligence alert was responsible for their discoveries of three more smugglers, again using PNR information:

- Q. C. was arrested at San Juan International Airport (SJU) on May 24, 2004, while attempting to smuggle a Dominican national minor with a valid Puerto Rican birth certificate. Q.C. was indicted by SAC San Juan on alien smuggling charges and the minor was deported.
- Y. S. was arrested at SJU On June 13, 2004, while attempting to smuggle two Dominicans with Puerto Rican birth certificates. Y.S. was indicted by SAC San Juan and one minor was deported. The second was found to be a previously deported adult and he was also arrested.
- On July 16, 2004, M. C. was arrested at SJU while attempting to smuggle a Dominican minor with a Puerto Rican birth certificate. M.C. was indicted on alien smuggling charges and the minor was deported.

On July 17, 2004, S. B. was detained at Boston's Logan International Airport. S.B. was traveling with two suspected Dominican national minors with valid New York State birth certificates. S.B. had been identified by the San Juan Passenger Analysis Unit (PAU) as an associate of M.C. and a possible alien smuggler, but they had not referenced the detailed NEFTU report in the subject record. As a result, CBP officers in Boston did not believe they had enough evidence to detain the travelers so S.B. and the minors were released. The information has subsequently been turned over to ICE agents in Boston for investigation.

~~WARNING: This document is UNCLASSIFIED/FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD-1042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001088

~~For Official Use Only~~

2. Use of Telephone Number Data Fields to Solve Stalled Cases

The effectiveness of subscriber information as an important investigative tool has been seriously compromised in recent years as new cell phone companies abound that will accept subscribers using fictitious identities. Many investigations have reached dead ends because there is no way to identify the parties actually making and receiving the calls. ICE recently had several successes because the fictitious subscribers' phones were used to make airline reservations for real people. A search of saved PNRs for the phone numbers led to the break-throughs. In some cases, the phone subscriber was the traveler, and thus fully identified; in other cases, the subscriber was making reservations for drug couriers who were then identified and apprehended.

3. Use of Telephone Numbers to Identify User Identities and Clear Innocents

During a nine month investigation into a Vietnamese / US/Canadian MDMA smuggling organization, PNR information was used to identify actual users of phones for which we had previously received false subscriber information from the phone company. The information obtained from the PNR, not only helped to identify criminal targets, but also helped to clear individuals whose names were used as fake subscribers, and were not part of the criminal conspiracy

4. Pattern Analysis to Identify Sexual Predators

ICE Investigators learned of a suspected child sex predator ("Mr.X") planning a trip to Bangkok and believed to be affiliated with a particular travel agency that specialized in "Sex Tourism". Although no arrests have yet been made in this case, PNR research led to the identification of many additional potential sexual predators and their methods of operation:

- A review of all reservations on Mr. X's flight and on all other flights to the same destination from the New York City area within a one-week period led to the identification of other men who had booked travel with the same travel agency. (The travel agency booked each traveler separately and on a variety of flights as a way of protecting themselves and the others on the tour in case one of the men was a law enforcement target.)
- When Mr. X changed his reservation to leave from a West Coast city, a second travel agency was cited in the record. Reservations from the second city, naming the second travel agency, revealed many more potential targets for investigation.
- Mr. X's PNR identified the hotel he would be visiting in Bangkok, facilitating surveillance.

~~WARNING: This document is UNCLASSIFIED FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 110421, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

001089

~~For Official Use Only~~

It was subsequently learned that some of the men on the trip made new reservations after they arrived in Bangkok, for a side trip to Cambodia. Because there was no direct nexus to the U.S. on those trips, the PNRs were unavailable for research. It is believed that those men who were specifically interested in sex with children traveled on the Cambodian trip.

5. Use of PNR to Bolster APIS Analysis and Identify a Coconspirator

Information was gleaned from a Title III wire tap that "Harry" would be arriving on that day into the U.S. from Venezuela with heroin. A search was conducted in APIS and ADIS on all flights from Venezuela into all US ports. A possible "Harry" was identified, and his reservation was obtained from CBP. Another individual was identified as traveling on the same reservation, and both Harry C. and J. C. were arrested for conspiracy to distribute narcotics. Timely acquisition of all information from the PNR resulted in the success of the case.

6. Use of PNR to Support Early Identification

On January 20, 2006, agents assigned to the New York Organized Crime Drug Enforcement Strike Force arrested a money launderer for the Hells Angels Motorcycle Gang and other international narcotics organizations. M.T. allegedly laundered \$1 billion his clients accumulated doing everything from stock fraud to peddling the "date-rape" drug GHB, used by sexual predators, and then wire-transferred it to accounts in Texas, the Bahamas and elsewhere.

M.T. also invested millions of dollars in illegal proceeds from cocaine and hydroponic marijuana trafficking, mail fraud and additional securities-fraud schemes, court papers show He had been sought for years, but spent very little time in the U.S. and no specific travel information was ever available until after he had already left the country. In this instance, it was known that he was planning a brief meeting in New York City while en-route between Nassau, the Bahamas, and Canada. A massive PNR search found his reservation and agents were able to begin surveillance when he arrived at a New York area airport. They followed him to his meeting in the lobby of the Mandarin Oriental Hotel in New York City where he was arrested.

~~WARNING: This document is UNCLASSIFIED FOR OFFICIAL USE ONLY (U/FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522.). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Policy, Management Directive MD 11042.1, relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

002090

The Northeast Field Intelligence Unit used PNR information to uncover an alien smuggling operation involved in smuggling Dominicans into the U.S. through various Ports of Entry. This work eventually resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, the disruption of an organization responsible for successfully smuggling thirty-seven individuals, and the increased awareness by CBP officers of a simple and highly effective alien smuggling technique.

On March 13, 2004, a woman named C(66)G. was arrested at Newark International Airport for attempted alien smuggling. She was escorting a Dominican national posing as C.G.'s son, and using her son's valid Puerto Rican birth certificate as his travel document. Although the imposter was removed and C.G. admitted that this was not the first time she had smuggled aliens in this way, prosecution was declined. At this point, the FIU analyst initiated research on her prior travel.

PNR information from her two known arrivals revealed that, in each case, she had traveled alone on the outbound segments from the U.S. to the Dominican Republic, but returned on the inbound portion of her reservation accompanied by travelers posing as her children. The "children" presented round trip tickets that indicated they were returning to their point of departure, but the outbound segments of their reservations had never actually been used.

The analyst identified three associates of C.G. who had each traveled outbound several times with her to the Dominican Republic. Their PNRs revealed the same pattern: the three associates returned to the U.S. with persons identified as their children, but the children had not traveled outbound before "returning." When APIS reported that the three were scheduled to return to the U.S. on separate flights within 48 hours, the analyst ensured that the travelers were intercepted. M(66)P. was arrested on April 29, 2004, at Miami International Airport (MIA). M.P. was attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.P. was indicted on alien smuggling charges and the three minors were removed. (She is currently awaiting sentencing.)

On April 30, 2004, M(66)T. arrived and was arrested at MIA after attempting to smuggle three Dominican national minors posing as her children. All three were in possession of valid Puerto Rican birth certificates. M.T. was indicted on alien smuggling charges and the three minors were deported. (M.T. has since been sentenced to five years in prison on these charges.) After her two associates were arrested, the third woman changed her reservation. She had been scheduled to fly into MIA with three children who had not been with her on her outbound trip. Instead, she arrived at San Juan International Airport alone but she had three extra suitcases with her after a one-week trip, indicating a probable last minute change of plans.

The analyst described the scheme in an Intelligence Alert, identifying the steps that Customs and Border Protection (CBP) Officers could take to reveal similar alien smuggling techniques. CBP Officers in San Juan informed the analyst that the information in the intelligence alert was responsible for their discoveries of three more smugglers, again using PNR information:

001691

- **Q(166) C. was arrested at San Juan International Airport (SJU) on May 24, 2004, while attempting to smuggle a Dominican national minor with a valid Puerto Rican birth certificate. Q.C. was indicted by SAC San Juan on alien smuggling charges and the minor was deported.**
- **Y(166) S. was arrested at SJU On June 13, 2004, while attempting to smuggle two Dominicans with Puerto Rican birth certificates. Y.S. was indicted by SAC San Juan and one minor was deported. The second was found to be a previously deported adult and he was also arrested.**
- **On July 16, 2004, M(166) C. was arrested at SJU while attempting to smuggle a Dominican minor with a Puerto Rican birth certificate. M.C. was indicted on alien smuggling charges and the minor was deported.**

On July 17, 2004, S(166) B. was detained at Boston's Logan International Airport. S.B. was traveling with two suspected Dominican national minors with valid New York State birth certificates. S.B. had been identified by the San Juan Passenger Analysis Unit (PAU) as an associate of M.C. and a possible alien smuggler, but they had not referenced the detailed NEFTU report in the subject record. As a result, CBP officers in Boston did not believe they had enough evidence to detain the travelers so S.B. and the minors were released. The information has subsequently been turned over to ICE agents in Boston for investigation.

1. The effectiveness of subscriber information as an important investigative tool has been seriously compromised in recent years as new cell phone companies abound that will accept subscribers using fictitious identities. Many investigations have reached dead ends because there is no way to identify the parties actually making and receiving the calls. ICE recently had several successes because the fictitious subscribers' phones were used to make airline reservations for real people. A search of saved PNRs for the phone numbers led to the break-throughs. In some cases, the phone subscriber was the traveler, and thus fully identified; in other cases, the subscriber was making reservations for drug couriers who were then identified and apprehended.

2. ICE Investigators learned of a suspected child sex predator ("Mr.X") planning a trip to Bangkok and believed to be affiliated with a particular travel agency that specialized in "Sex Tourism". Although no arrests have yet been made in this case, PNR research led to the identification of many additional potential sexual predators and their methods of operation:

- A review of all reservations on Mr. X's flight and on all other flights to the same destination from the New York City area within a one-week period led to the identification of other men who had booked travel with the same travel agency. (The travel agency booked each traveler separately and on a variety of flights as a way of protecting themselves and the others on the tour in case one of the men was a law enforcement target.)

- When Mr. X changed his reservation to leave from a West Coast city, a second travel agency was cited in the record. Reservations from the second city, naming the second travel agency, revealed many more potential targets for investigation.

- Mr. X's PNR identified the hotel he would be visiting in Bangkok, facilitating surveillance.

- It was subsequently learned that some of the men on the trip made new reservations after they arrived in Bangkok, for a side trip to Cambodia. Because there was no direct nexus to the U.S. on those trips, the PNRs were unavailable for research. It is believed that those men who were specifically interested in sex with children traveled on the Cambodian trip.

3. On January 20, 2006, agents assigned to the New York Organized Crime Drug Enforcement Strike Force arrested M | 4 | Γ., a money launderer for the Hells Angels Motorcycle Gang and other international narcotics organizations. M.T. allegedly laundered \$1 billion his clients accumulated doing everything from stock fraud to peddling the "date-rape" drug GHB, used by sexual predators, and then wire-transferred it to accounts in Texas, the Bahamas and elsewhere.

M.T. also invested millions of dollars in illegal proceeds from cocaine and hydroponic marijuana trafficking, mail fraud and additional securities-fraud schemes, court papers

002893

show He had been sought for years, but spent very little time in the U.S. and no specific travel information was ever available until after he had already left the country. In this instance, it was known that he was planning a brief meeting in New York City while en-route between Nassau, the Bahamas, and Canada. A massive PNR search found his reservation and agents were able to begin surveillance when he arrived at a New York area airport. They followed him to his meeting in the lobby of the Mandarin Oriental Hotel in New York City where he was arrested.

001894

b2
b7E

Some more war stories from someone in the SAC/NY very excited about the prospect of getting PNR access back :

Another recent [] success story that resulted from the use of RESMON was Case

b6

For Case (b2 b7E), information was gleaned from a Title III wire tap that "Harry" would be arriving on that day into the US from Venezuela with heroin. A search was conducted in APIS and ADIS on all flights from Venezuela into all US ports. A possible "Harry" was identified, and his reservation was obtained from CBP. Another individual was identified as traveling on the same reservation, and both Harry C. and J (W) C. were arrested for conspiracy to distribute narcotics. Timely acquisition of all information from the PNR resulted in the success of the case.

[] was a nine month investigation into a Vietnamese / US/Canadian [] smuggling organization. I used ATS PNR information on a few occasions to identify actual users of phones for which we had previously received false subscriber information from the phone company. The information obtained from the PNR, not only helped to identify criminal targets, but also helped to clear individuals whose names were used as bogus subscribers, and were not part of the criminal conspiracy.

001895

211

Use of Pattern Analysis to Dismantle a Human Smuggling Operation

ICE-Intelligence officers used PNR information to uncover an alien smuggling operation involved in smuggling Dominicans into the U.S. through various Ports of Entry. This work eventually resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, and the disruption of an organization responsible for successfully smuggling thirty-seven individuals.

In March, 2004, a woman named C. G. was arrested at Newark International Airport for attempted alien smuggling. She was escorting a Dominican national posing as C.G.'s son, and using her son's valid Puerto Rican birth certificate as his travel document. The imposter was removed and C.G. admitted that this was not the first time she had smuggled aliens in this way. Research on her prior travel revealed that, in each case, she had traveled alone on the outbound segments from the U.S. to the Dominican Republic, but returned on the inbound portion of her reservation accompanied by travelers posing as her children.

Analysis identified three associates who had each traveled outbound several times with C.G. to the Dominican Republic. Their PNRs revealed the same pattern: the three associates returned to the U.S. with persons identified as their children, but the children had not traveled outbound before "returning." When APIS reported that the three were scheduled to return to the U.S. on separate flights within 48 hours, the analyst ensured that the travelers were intercepted.

M. P. was arrested on April 29, 2004, at Miami International Airport (MIA). M.P. was attempting to smuggle three Dominican national minors posing as her children. M.P. was indicted on alien smuggling charges and the three minors were removed.

On April 30, 2004, M. T. arrived and was arrested at MIA after attempting to smuggle three Dominican national minors posing as her children. M.T. was indicted on alien smuggling charges and the three minors were deported. (M.T. has since been sentenced to five years in prison on these charges.) After her two associates were arrested, the third woman changed her reservation. She had been scheduled to fly into MIA with three children who had not been with her on her outbound trip. Instead, she arrived at San Juan International Airport alone but she had three extra suitcases with her after a one-week trip, indicating a probable last minute change of plans.

After the techniques used to uncover scheme were described to Customs and Border Protection (CBP) Officers, three more smugglers were detected in San Juan, Puerto Rico, and one in Boston.

002896

212

Global
b2
b7E

**Bullets for the Assistant Commissioner
Office of Field Operations**

Atlanta Hartsfield: Citizens of Pakistan

On () arrived at Atlanta Hartsfield airport () Both travelers are citizens of () who originally embarked in (). Based on API, PNR data for the current flight and previous travel patterns, both were referred by ATS-P as Threshold Targeting hits. Further questioning revealed () was a legal permanent resident who was out of the US for 15 months. () was placed in deportation proceedings.

Atlanta Hartsfield: Citizens of Pakistan

On May 23, 2006, () a citizen of (), arrived at Atlanta Hartsfield airport on (). Based on API, PNR data for the current flight and previous travel patterns, () was referred by ATS-P as a Threshold Targeting hit. CBP determined ()'s visa was issued one week prior to 9/11/01, yet had never traveled to the US. ()'s profession was listed in his () passport as "flight instructor." ()'s intended purpose for travel to the US was to () and to "see a man in New York for two days." () was placed in deportation proceedings.

Atlanta Hartsfield: Three Citizens () Refused Admission

On () subjects - () into Atlanta-Hartsfield Airport and applied for admission ()

Minneapolis-St Paul: F1 Student From ()

On () Minneapolis apprehended an F1 student from () The student was identified as () was targeted by the PAU during ATS queries. ()

b. FBI Agents and an FBI interpreter examined the computer and drives. A file on the computer contained a video on () The file also contained images of () The file

001097

b2
b7E

also contained photos () Other thumbnail drives were found to contain images () The JTTF summoned a special team from FBI Headquarters in Washington DC to interview (b6) US Attorney's office charged (b6) with making false statements. As of 12/06/2006, ()

Minneapolis-St Paul - Jordanian National - (b6)

CBP Officers at Minneapolis St. Paul apprehended () JTTF and FBI responded with Agents and a computer specialist team. Passenger (b6)

() During CBP interview and research, it was determined that (b6) admitted to being arrested and convicted on terrorist related charges at the age of 19. (b6) originally claimed credible fear but recanted and he was expeditiously removed from the U.S.

Los Angeles, CA - COC: () - Visa Waiver Refusal

The subject arrived unaccompanied from (b6) (b6)

() The subject was determined inadmissible as an immigrant without an immigrant visa.

Boston Logan Airport- Two Individuals refused admission with ties to () extremist group

On () at approximately 2100 hours subjects () and applied for admission as Visa Waiver applicants. Both subjects were ATS-P lookouts. During secondary one subject stated that he was traveling to the U.S. on business ()

Both subjects were refused admission under 212(a)(7)(A)(i)(I) Immigrant not in possession of valid travel document. since they not able to proof that they were bonafide applicants.

Miami, FI - PAU Targets Numerous Cubans Aboard () Airlines
In () as a result of ATS Miami PAU targeted numerous passengers that required additional scrutiny prior to boarding an aircraft from () to

001098

6/16/91
b2
b7E

Miami. Ultimately, () diverted the aircraft to the Dominican Republic and identified 11 undocumented Cubans aboard the aircraft. () , returned to () and removed the undocumented Cubans.

San Juan - \$144,895 in Currency Seized

On (_____), During the examination of the subject's luggage, \$144,895 was discovered within pairs of jeans in the subject's luggage. (_____)


The Honorable Bennie G. Thompson
Chairman-elect
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Representative Thompson:

(b)(6)




(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)



Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.


(b)(5) - Atty Client, (b)(5) - Delib



001700

Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

(b)(5) - Atty Client, (b)(5) - Delib




Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Del/b

(b)(5) - Atty Client, (b)(5) - Del/b, (b)(5)

Does the system contain mechanisms that allow Passenger Name Record Information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

(b)(5) - Atty Client, (b)(5) - Del/b

Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

(b)(5) - Atty Client, (b)(5) - Del/b

The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Atty Client, (b)(5) - Del/b

001702

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib



To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Atty Client, (b)(5) - Delib

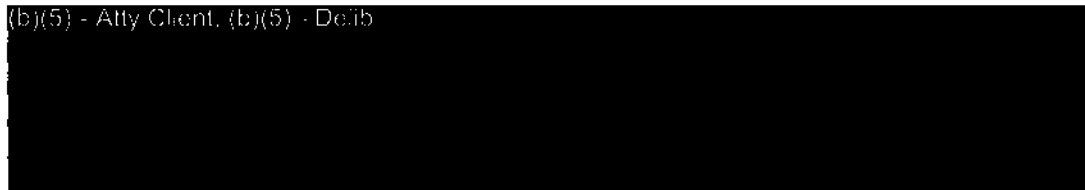


(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)



Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Atty Client, (b)(5) - Delib



If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Atty Client, (b)(5) - Delib

The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Atty Client, (b)(5) - Delib


(b)(5) - Atty Client, (b)(5) - Delib

Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating

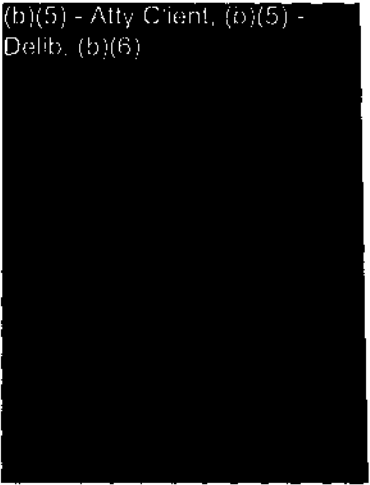
001704

ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Delib, (b)(6)



The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

001705

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)

Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Atty Client, (b)(5) - Delib

What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Delib


The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Delib

(b)(5) - Delib, (b)(6)

001706

(b)(5) Delib



Sincerely,

W. Raiph Basham
Commissioner

001707

The Honorable Bennie G. Thompson
Chairman-elect
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Representative Thompson:

(b)(5) - Delib



Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

(b)(5) - Delib



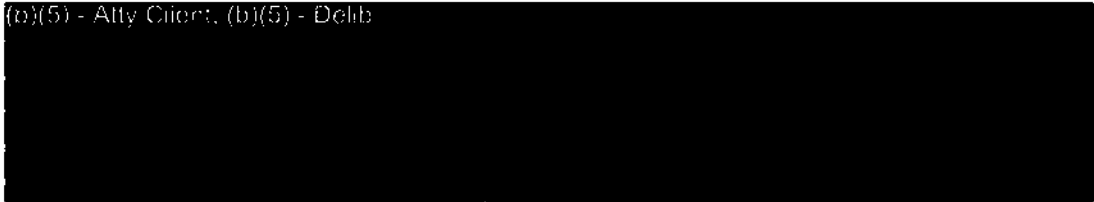
(b)(5) - Delib. (b)(6)



Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

001708

(b)(5) - Atty Client, (b)(5) - Delib

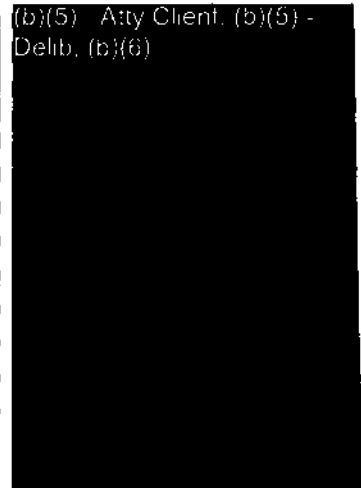


Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



(b)(5) - Atty Client, (b)(5) - Delb

(b)(5) - Atty Client, (b)(5) - Delb, (b)(6)

Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

(b)(5) - Atty Client, (b)(5) - Delb

Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Atty Client, (b)(5) - Delib

Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Delib

(b)(5) - Delib, (b)(6)

If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.


(b)(5) - Delib

If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Delib



(b)(5) - Delib



The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Delib



Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

(b)(5) - Delib



The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual

001712

have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Delib

(b)(5) - Delib, (b)(6)

The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

(b)(5) - Delib

(b)(5) - Delib, (b)(6)

Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Delib

What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Delib

The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Delib

(b)(5) - Del.b



(b)(5) - Del.b, (b)(6)



Sincerely,

W. Ralph Basham
Commissioner

001714

(b)(5) - Atty Client, (b)(5) -
Del.b. (b)(6)

The Honorable Bennie G. Thompson
Chairman-elect
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Representative Thompson:

(b)(5) - Atty Client, (b)(5) - Del b

Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

(b)(5) - Atty Client, (b)(5) - Del b

001715

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)


Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) - Atty Client, (b)(5) - Delib

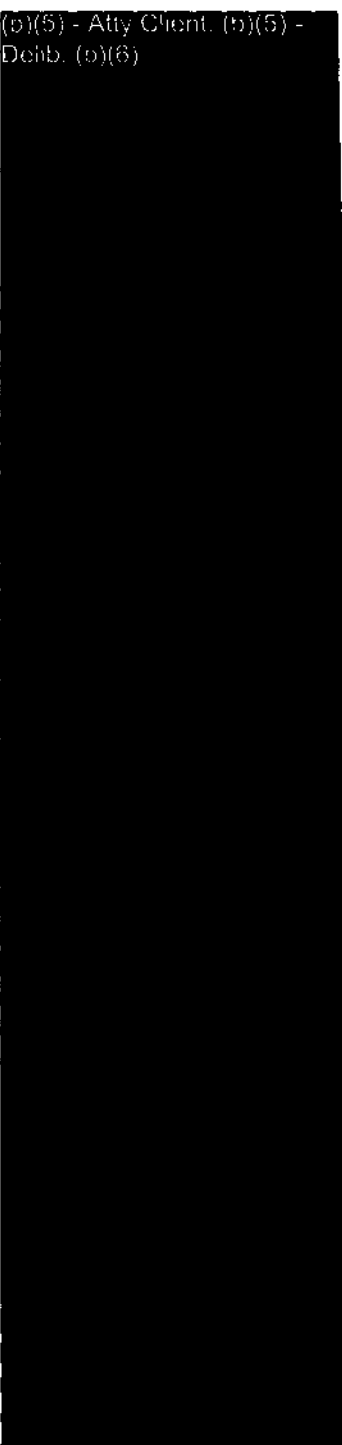
001726

If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

(b)(5) - Atty Client, (b)(5) - Deob



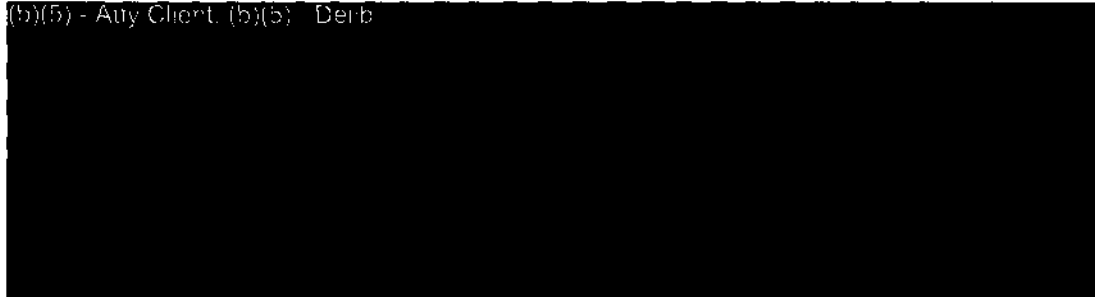
(b)(5) - Atty Client, (b)(5) - Deob, (b)(5)



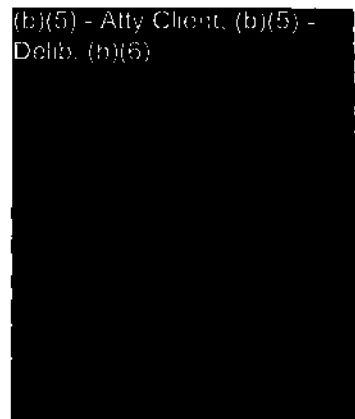
Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

001717

(b)(5) - Atty Client, (b)(5) - Delib

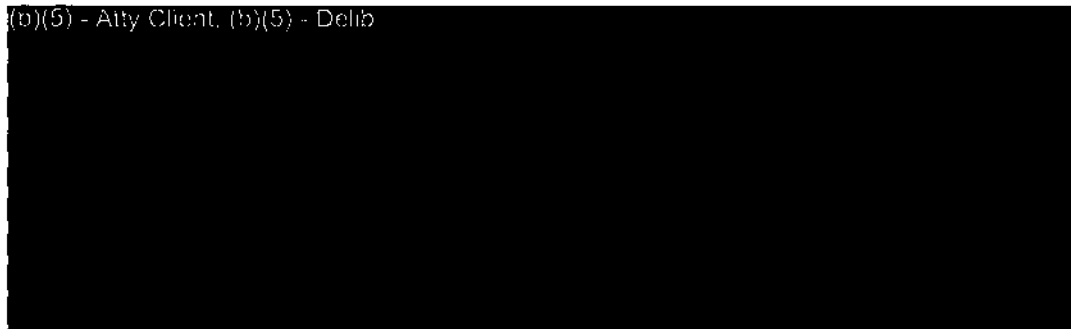


(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

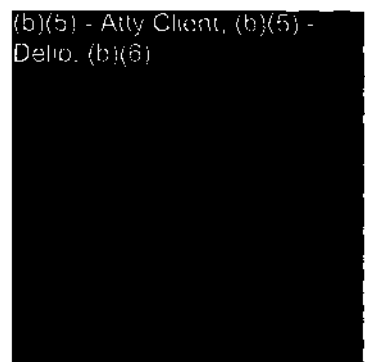


Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

(b)(5) - Atty Client, (b)(5) - Delib

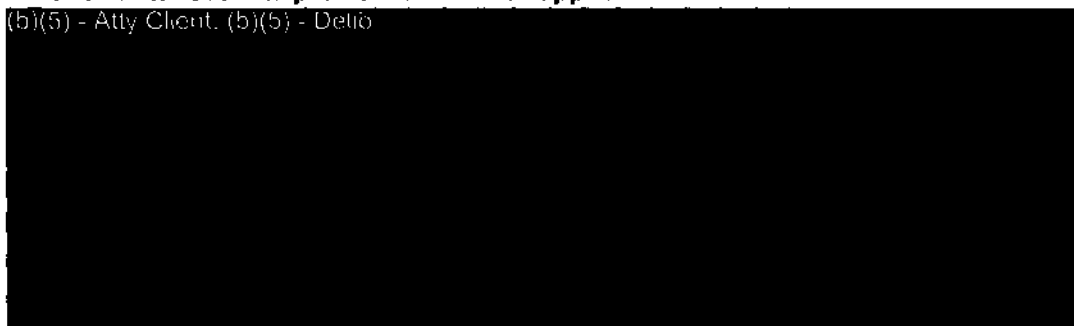


(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

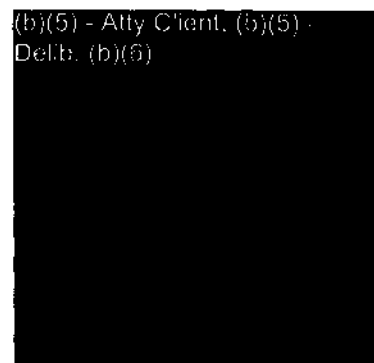


The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)



(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Atty Client, (b)(5) - Delib

Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Atty Client, (b)(5) - Delib

If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

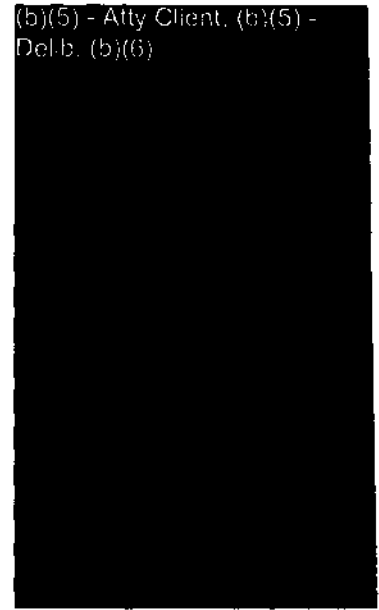
Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Del b



(b)(5) - Atty Client, (b)(5) - Del b, (b)(6)



The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Atty Client, (b)(5) - Del b

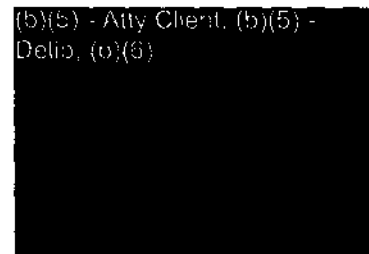


The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

(b)(5) - Atty Client, (b)(5) - Del b



(b)(5) - Atty Client, (b)(5) - Del b, (b)(6)



Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Atty Client, (b)(5) - Delib

What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Atty Client, (b)(5) - Delib

The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

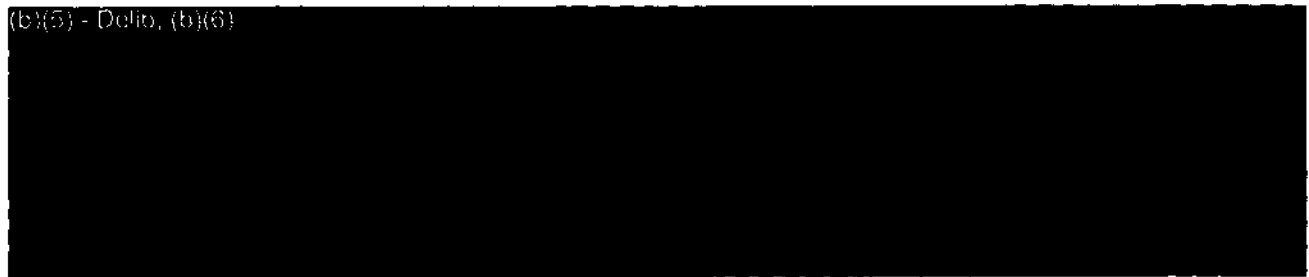
(b)(5) - Delib

Sincerely,

W. Ralph Basham
Commissioner

CG1723

(b)(5) - Deho, (b)(6)



001721

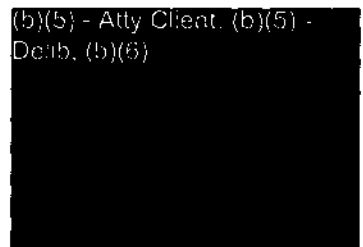
The Honorable Bennie G. Thompson
Chairman-elect
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Representative Thompson:

(b)(5) - Atty Client, (b)(5) - Del/b

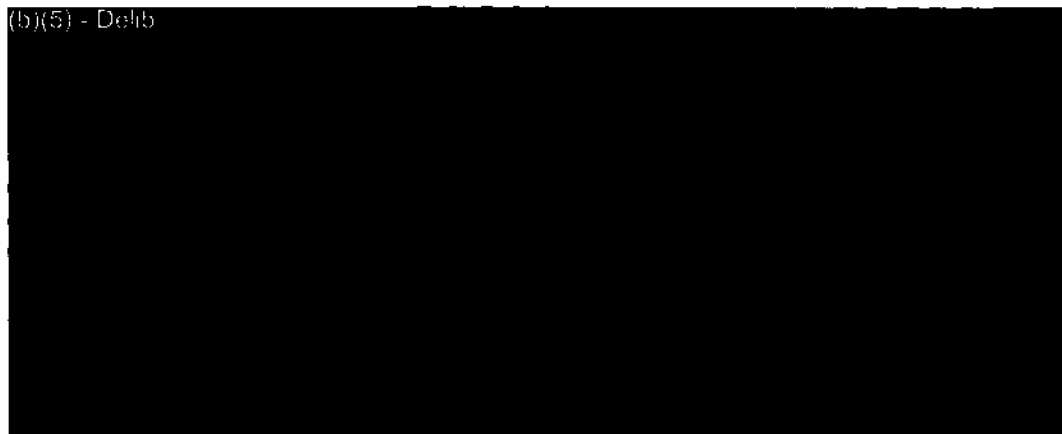


(b)(5) - Atty Client, (b)(5) - Del/b, (b)(6)

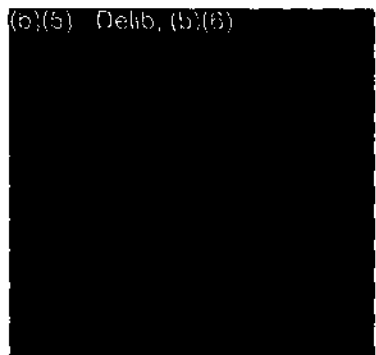


Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

(b)(5) - Del/b



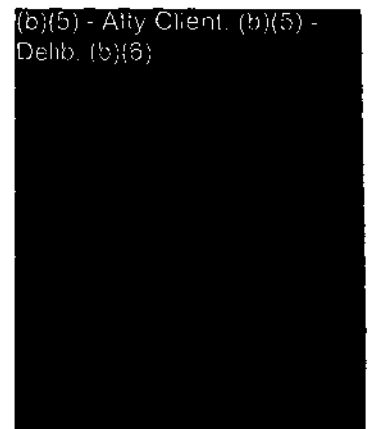
(b)(5) - Del/b, (b)(6)



(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)



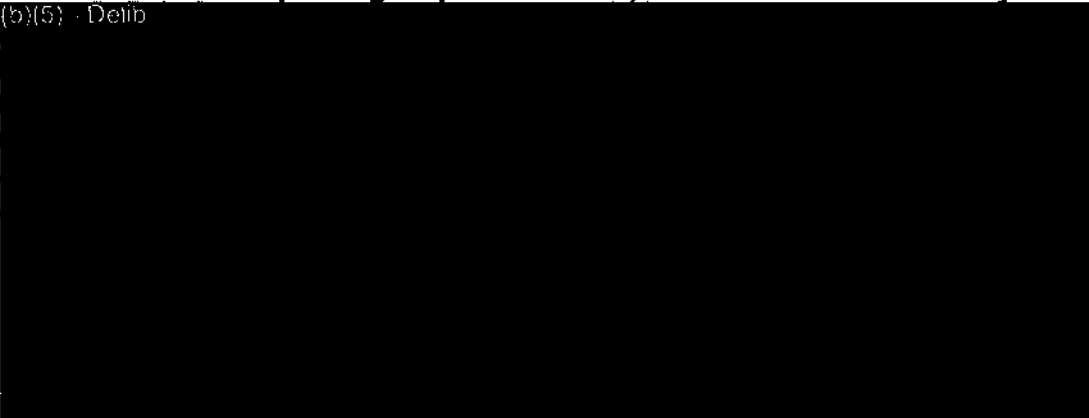
Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

(b)(5) - Delib



Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) - Delib



(b)(5) - Delib, (b)(5)



(b)(5) - Atty Client, (b)(5) -
Delib, (b)(5)

If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

(b)(5) - Atty Client, (b)(5) - Delib

001727

Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

(b)(5) - Atty Client, (b)(5) - Del b

(b)(5) - Atty Client, (b)(5) Del b, (b)(5)

Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

(b)(5) - Del b

The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Del b

001728

(b)(5) - Any Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

001729

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)

If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

(b)(5) - Atty Client, (b)(5) - Delib

If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Atty Client, (b)(5) - Delib

The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)

001730

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

(b)(5) - Atty Client, (b)(5) - De/b



(b)(5) - Atty Client, (b)(5) -
De/b, (b)(6)



The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

(b)(5) - De/b



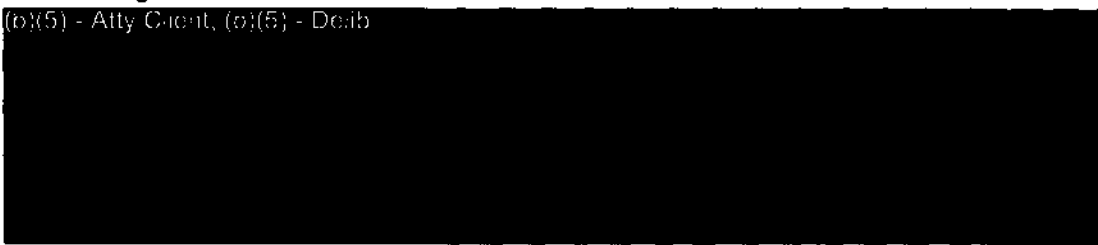
Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Atty Client, (b)(5) - De/b



What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Atty Client, (b)(5) - De/b



001732

(b)(5) - Atty Client, (b)(5) - Del b

(b)(5) - Atty Client, (b)(5) -
Del b, (b)(6)

The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Atty Client, (b)(5) - Del b

(b)(5) - Atty Client, (b)(5) -
Del b, (b)(6)


(b)(5) - Atty Client, (b)(5) - Del b

Sincerely,

W. Ralph Basham
Commissioner

001783

(b)(5) - Atty Client, (b)(5) - Delia, (b)(6)



001734

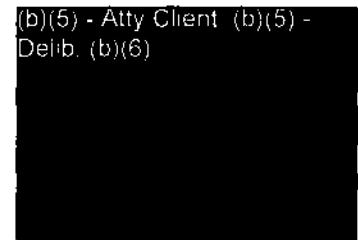
The Honorable Bennie G. Thompson
Chairman-elect
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Representative Thompson:

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client (b)(5) -
Delib, (b)(6)



Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

(b)(5) - Delib



(b)(5) - Delib, (b)(6)

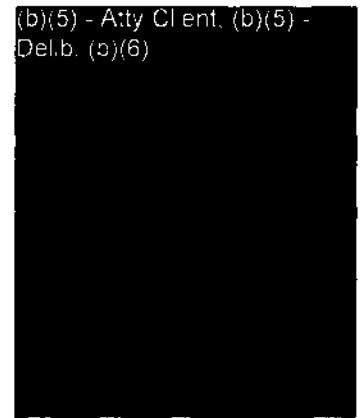


001725

(b)(5) - Atty Client, (b)(5) - Delib

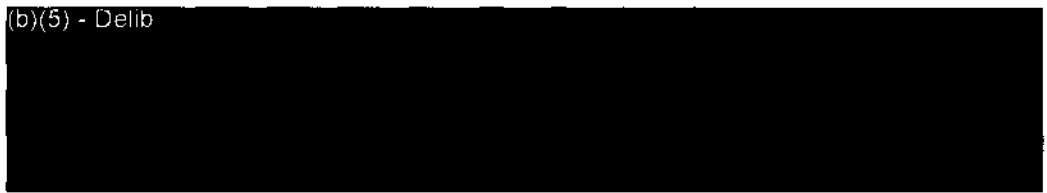


(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

(b)(5) - Delib



Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) - Delib



(b)(5) - Delib, (b)(6)



(b)(5) - Atty Client. (b)(5) - Delib. (b)(6)

If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

(b)(5) - Atty Client. (b)(5) - Delib

Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

(b)(5) - Delib



The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib (b)(6)

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

(b)(5) - Atty Client, (b)(5) - Delib

If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client (b)(5) -
Delib, (b)(6)

Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib (b)(6)

The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)

The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

(b)(5) - Delib

Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Atty Client, (b)(5) - Delib

What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)

The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client (b)(5) -
Delib, (b)(6)


(b)(5) - Atty Client, (b)(5) - Delib

Sincerely,

W. Ralph Basham
Commissioner

001743

(b)(5) - Atty Client. (b)(5) - Del. b (b)(6)



001741

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Thompson:

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) -
Delib

1. The Risk Assessment Portion of the Process

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5)
Delib, (b)(6)

1(b) Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

(b)(5) - Atty Client, (b)(5) - Delib


1(c) Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) - Atty Client, (b)(5) - Delib

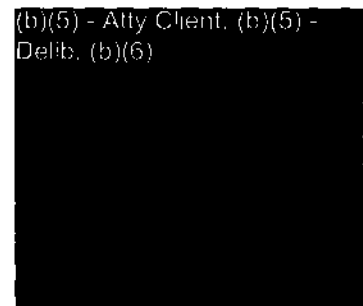


1(d) If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

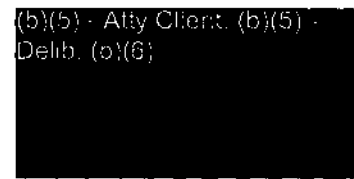
(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



(b)(5) - Atty Client, (b)(5) - Delib

1(e) Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

1(f) Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

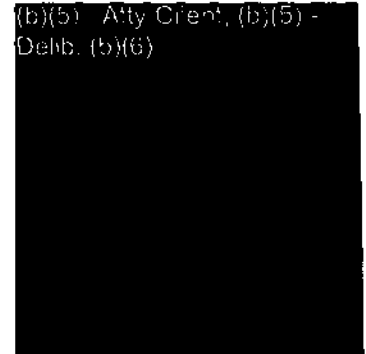
1(g) The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these

circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (b)(5) - Delib, (b)(5) - Delib

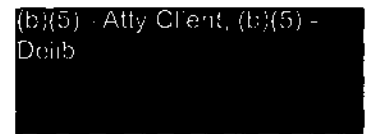


1(h) To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Atty Client, (b)(5) - Delib



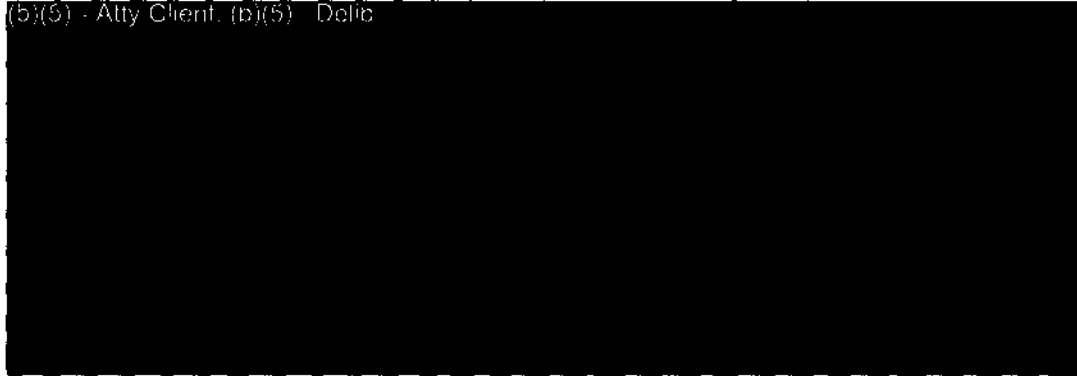
(b)(5) - Atty Client, (b)(5) - Delib



2. Accessibility of Information Contained within the System

2(a) Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Atty Client, (b)(5) - Delib

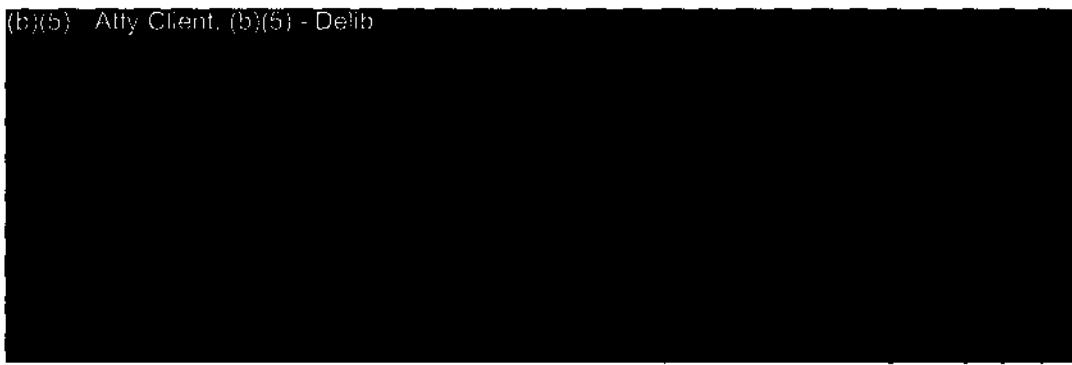


(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

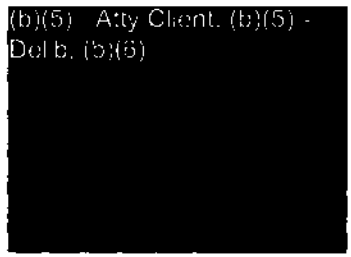


2(b) If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

(b)(5) - Atty Client, (b)(5) - Delib

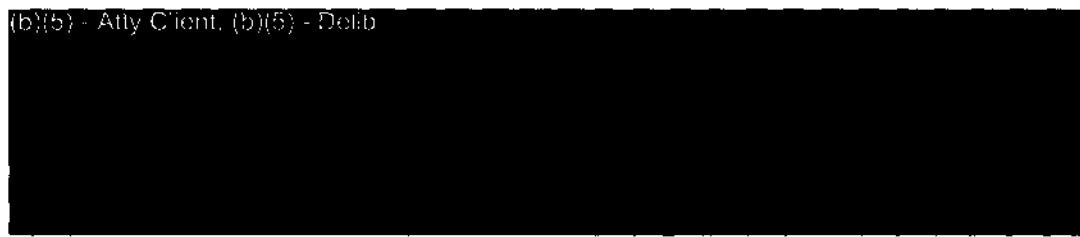


(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



2(c) If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Atty Client, (b)(5) - Delib



2(d) The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

2(e) Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

3. Process for Correcting and Detecting Mistakes

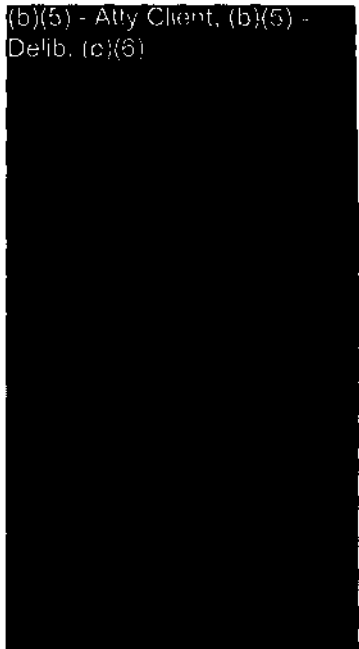
3(a) The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (c)(6)



3(b) The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib, (c)(6)



4. Retention of Information

4(a) Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Atty Client, (b)(5) - Delib

[Redacted]

(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

[Redacted]

4(b) What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

[Redacted]

(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

[Redacted]

4(c) The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Atty Client, (b)(5) - Delib

[Redacted]

(b)(5) - Atty Client, (b)(5) - Delib, (b)(5)

[Redacted]

(b)(5) - Atty Client, (b)(5) - Delib

[Redacted]


(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) -
Delib

Sincerely,

W. Ralph Basham
Commissioner

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)



001754

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Thompson:

(b)(5) - Delib



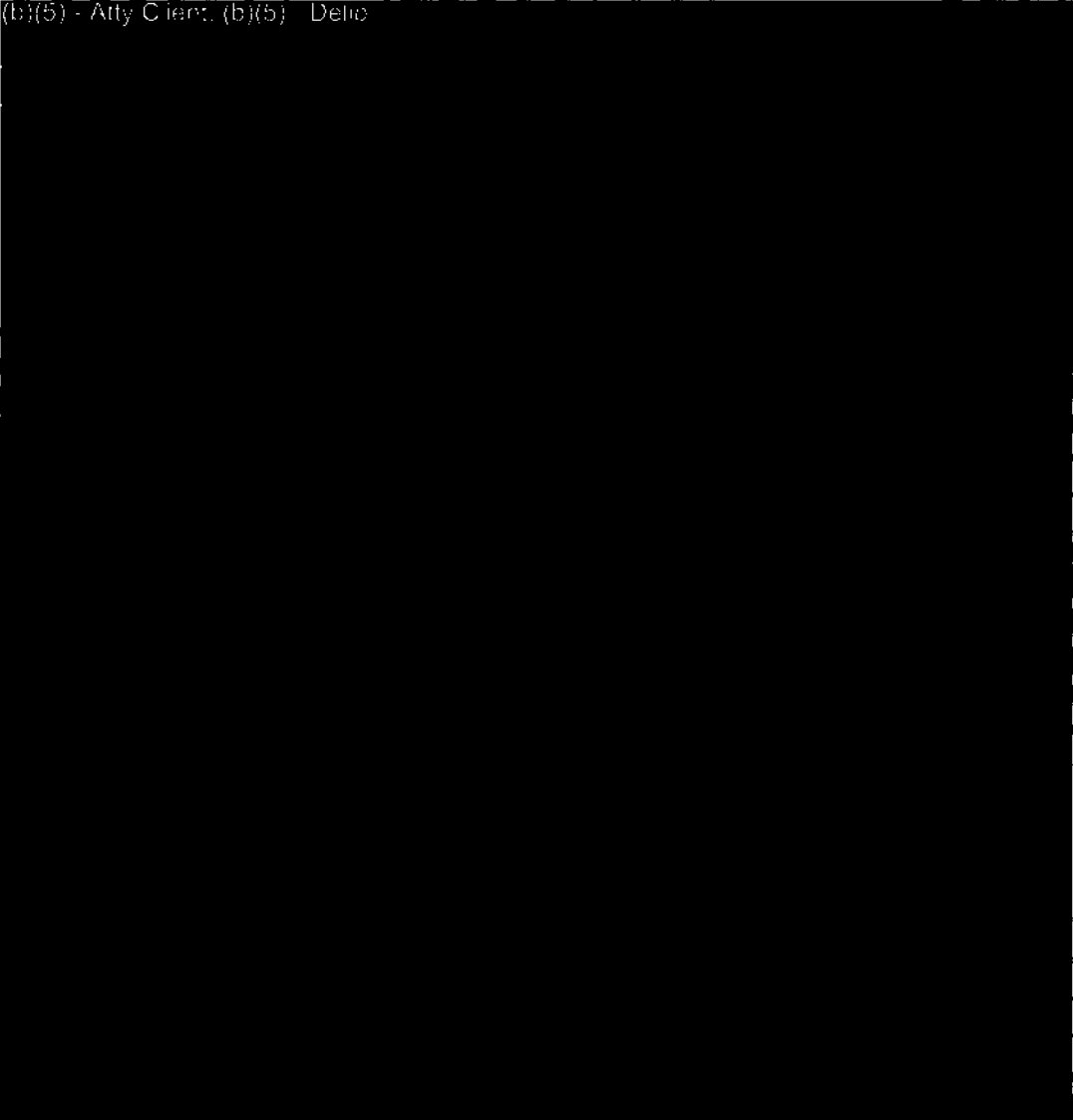
1. The Risk Assessment Portion of the Process

1(a) Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

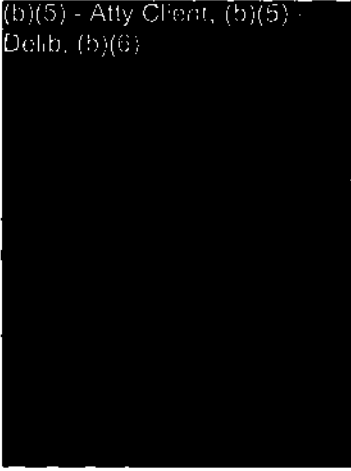
(b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib

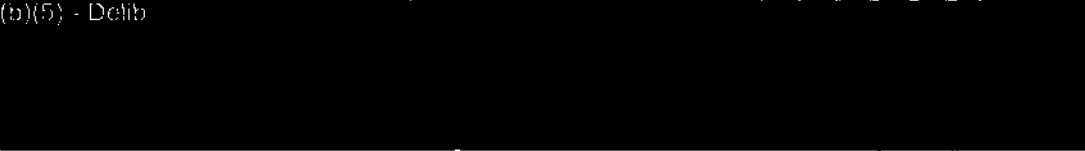


(b)(5) - Atty Client, (b)(5) -
Delib, (b)(6)



1(b) Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

(b)(5) - Delib



(b)(5) - Delib

1(c) Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib, (b)(6)

1(d) If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

1(e) Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?


(b)(5) - Atty Client, (b)(5) - Delib

(b)(5) - Atty Client, (b)(5) - Delib

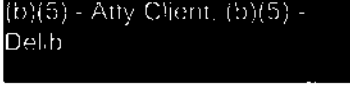
1(f) Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary

restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

(b)(5) - Atty Client, (b)(5) - Delib




(b)(5) - Atty Client, (b)(5) - Delib



1(g) The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Atty Client, (b)(5) - Delib




(b)(5) - Atty Client, (b)(5) - Delib



1(h) To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Atty Client, (b)(5) - Delib



2. Accessibility of Information Contained within the System

2(a) Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Delib



2(b) If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

(b)(5) - Del b



2(c) If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Del b




2(d) The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Del b



2(e) Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

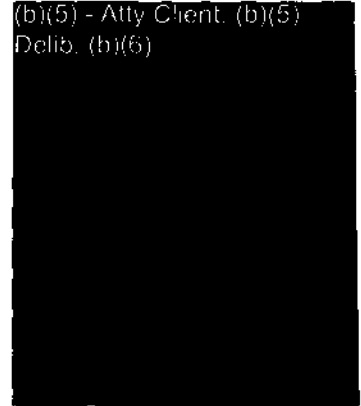
(b)(5) - Del b



(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) Delib, (b)(6)



3. Process for Correcting and Detecting Mistakes

3(a) The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Delib

3(b) The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

(b)(5) - Delib

4. Retention of Information

4(a) Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Atty Client, (b)(5) - Delib


4(b) What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Delib

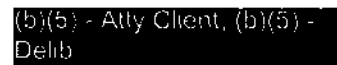
4(c) The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be

accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Atty Client, (b)(5) - Delib



(b)(5) - Atty Client, (b)(5) - Delib



Sincerely,

W. Ralph Basham
Commissioner

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Thompson:

(b)(5) - Delib



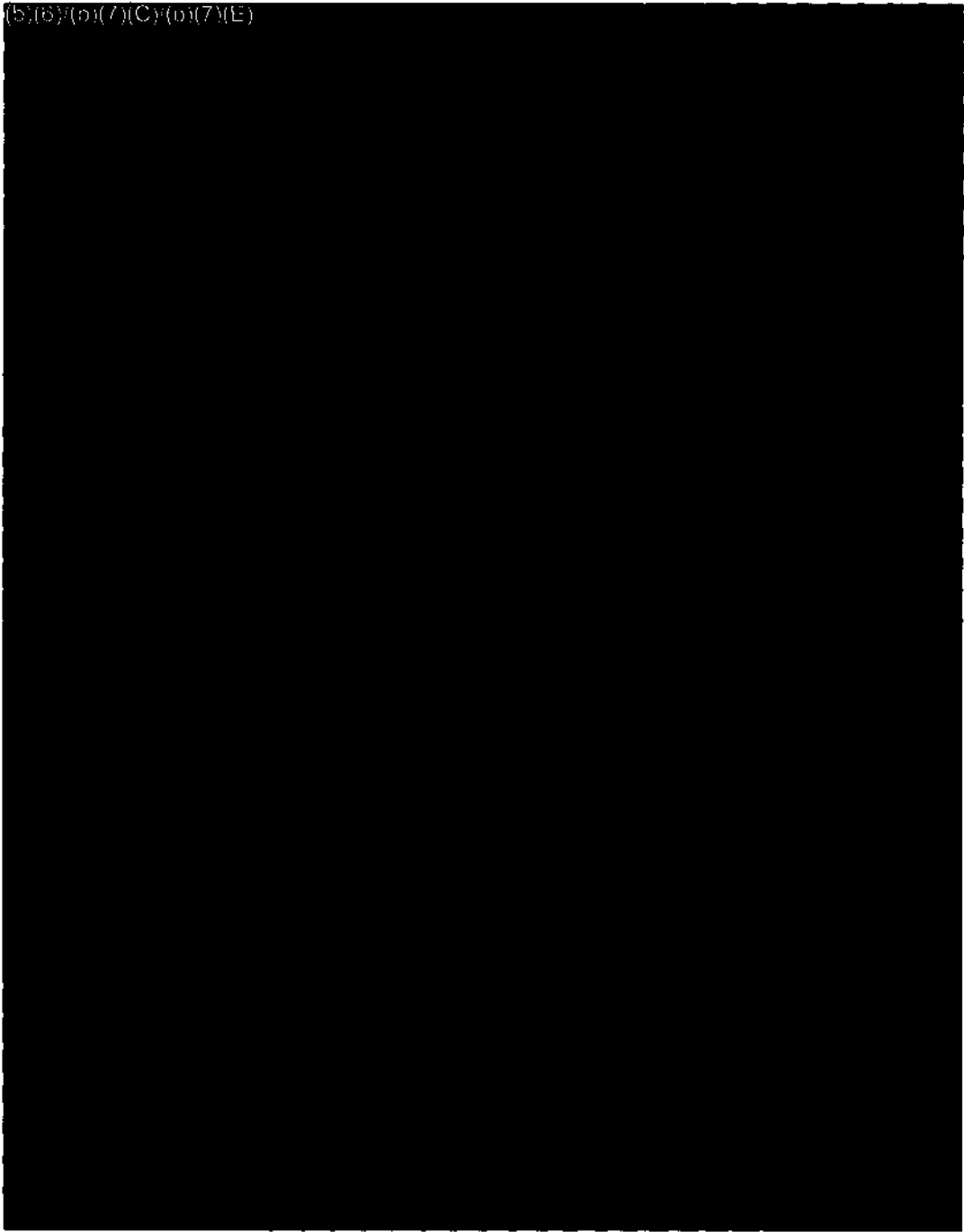
1. The Risk Assessment Portion of the Process

1(a) Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

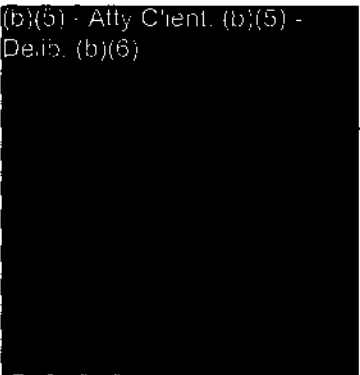
(b)(5) - Delib



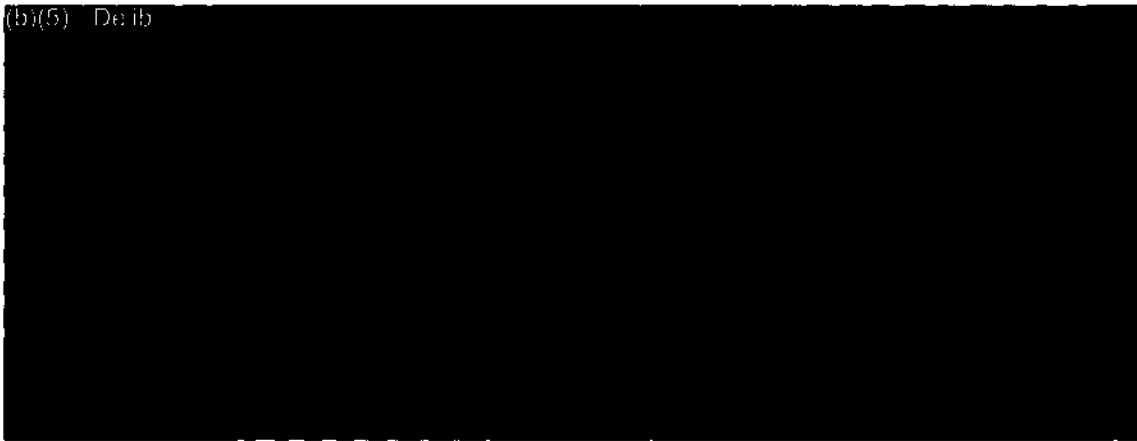
(b)(5)/(b)(7)(C)/(b)(7)(E)



(b)(5) - Atty Client. (b)(5) -
De. (b)(6)



(b)(5) Delib



1(b) Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

(b)(5) - Delib



1(c) Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

(b)(5) Delib




(b)(5) - Deib

1(d) If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?


(b)(5) - Deib

(b)(5) - Del.b



1(e) Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

(b)(5) - Del.b



1(f) Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

(b)(5) - Del.b



1(g) The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these

circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

(b)(5) - Del/b



1(h) To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

(b)(5) - Del/b



2. Accessibility of Information Contained within the System

2(a) Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

(b)(5) - Delib

A large black rectangular redaction box covers the entire response to question 2(a).

2(b) If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

(b)(5) - Delib

A large black rectangular redaction box covers the entire response to question 2(b).

2(c) If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

(b)(5) - Delib

A large black rectangular redaction box covers the entire response to question 2(c).

(b)(5) - Delib

2(d) The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

(b)(5) - Delib

2(e) Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?


(b)(5) - Delib

3. Process for Correcting and Detecting Mistakes

3(a) The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information

permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

(b)(5) - Delib



3(b) The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

(b)(5) - Delib



4. Retention of Information

4(a) Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

(b)(5) - Del/b

A large black rectangular redaction box covering the answer to question 4(a).

4(b) What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

(b)(5) - Del/b


A large black rectangular redaction box covering the answer to question 4(b).

4(c) The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

(b)(5) - Del/b

A large black rectangular redaction box covering the answer to question 4(c).

(c)(5) - Devo



Sincerely,

W. Ralph Basham
Commissioner

Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP), Office of Chief Counsel, (202) 344-2940.

General Information Regarding the Collection of Passenger Name Record (PNR) Data

Statutory and Regulatory Authority to Access PNR

- Pursuant to legal statute (title 49, United States Code, section 44909(c)(3)) and implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide U.S. Customs and Border Protection (CBP) (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems").
- Although this statute provides CBP with PNR data in an electronic format, most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, upon arrival of the passenger in the U.S. Electronic collection of PNR, however, substantially enhances CBP's ability to facilitate legitimate travelers and to conduct the necessary risk assessments, often prior to the boarding of passengers, thereby also increasing aviation security.

Computer System Security at CBP

- Authorized CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the CBP National Data Center.
- PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.
- Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system.
- Only certain officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data through that system. Access by "contractors" to

001882

Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP) Office of Chief Counsel, (202) 344-2940.

any PNR data contained in the CBP computer systems is for purposes of assisting in the maintenance or development of CBP's computer system.

- CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.
- Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR 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).
- CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34).

U.S. Laws Applicable to CBP's Treatment of PNR Data

- General Policy: CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as required by law (for example, pursuant to a court order).
- Freedom of Information Act: Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA.
 - Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure:
 - ✓ where the information is confidential commercial information;
 - ✓ where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy;
 - ✓ where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an

~~Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP), Office of Chief Counsel, (202) 344-2940~~

unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

(See title 5, United States Code (U.S.C.), sections 552(b)(4), (6), (7)(C)).

- CBP regulations (title 19, Code of Federal Regulations (CFR), section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to:

- ✓ confidential commercial information;
- ✓ material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and
- ✓ information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

CBP invokes these exemptions uniformly based on the character of the data, without regard to the nationality or country of residence of the subject of the data.

- Under the FOIA, any person may request access to their personal information which may be held by CBP. The procedures for making FOIA requests for CBP records are contained in section 103.5 of title 19 of the U.S. Code of Federal Regulations. Decisions by CBP to withhold a record (or part thereof) may be administratively and judicially challenged. (See title 5 U.S.C. section 552(a)(4)(B) and 19 CFR sections 103.7-103.9).
- The Privacy Act: Provides certain protections for personal data held by U.S. government agencies regarding U.S. citizens and lawful permanent residents. (title 5 U.S.C. section 552a.)
- Criminal penalties
 - Unauthorized Access: see above.
 - Unauthorized Disclosures: 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 employment, where such disclosure is not authorized by law (see title 18 U.S.C. sections 641, 1030, 1905).
- Department of Homeland Security's (DHS) Chief Privacy Officer: The DHS Chief Privacy Officer is required by statute to ensure that personal information

~~Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP), Office of Chief Counsel, (202) 344-2946.~~

is used in a manner than complies with relevant laws (see section 222 of the Homeland Security Act of 2002 (Public Law 107-296, dated November 25, 2002)). The Chief Privacy Officer is independent of any directorate within the Department of Homeland Security (CBP is an agency within DHS). The determinations of the Chief Privacy Officer are binding on the Department and may not be overturned on political grounds.

001885

~~Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP), Office of Chief Counsel, (202) 344-2640.~~

General Information Regarding the Collection of Passenger Name Record (PNR) Data

Statutory and Regulatory Authority to Access PNR

- Pursuant to legal statute (title 49, United States Code, section 44909(c)(3)) and implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide U.S. Customs and Border Protection (CBP) (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems").
- Although this statute provides CBP with PNR data in an electronic format, most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, upon arrival of the passenger in the U.S. Electronic collection of PNR, however, substantially enhances CBP's ability to facilitate legitimate travelers and to conduct the necessary risk assessments, often prior to the boarding of passengers, thereby also increasing aviation security.

Computer System Security at CBP

- Authorized CBP personnel generally obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the CBP National Data Center.
- PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.
- Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system.
- Only certain officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data through that system. Access by "contractors" to

001386

~~Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP), Office of Chief Counsel, (202) 344-2940~~

any PNR data contained in the CBP computer systems is for purposes of assisting in the maintenance or development of CBP's computer system.

- CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.
- Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR 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).
- CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34).

U.S. Laws Applicable to CBP's Treatment of PNR Data

- General Policy: CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as required by law (for example, pursuant to a court order).
- Freedom of Information Act: Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA.
 - Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure:
 - ✓ where the information is confidential commercial information;
 - ✓ where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy;
 - ✓ where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an

001087

~~Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP), Office of Chief Counsel, (202) 344-2940.~~

unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

(See title 5, United States Code (U.S.C.), sections 552(b)(4), (6), (7)(C)).

- CBP regulations (title 19, Code of Federal Regulations (CFR), section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to:

- ✓ confidential commercial information;
- ✓ material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and
- ✓ information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

CBP invokes these exemptions uniformly based on the character of the data, without regard to the nationality or country of residence of the subject of the data.

- Under the FOIA, any person may request access to their personal information which may be held by CBP. The procedures for making FOIA requests for CBP records are contained in section 103.5 of title 19 of the U.S. Code of Federal Regulations. Decisions by CBP to withhold a record (or part thereof) may be administratively and judicially challenged. (See title 5 U.S.C. section 552(a)(4)(B) and 19 CFR sections 103.7-103.9).
- The Privacy Act: Provides certain protections for personal data held by U.S. government agencies regarding U.S. citizens and lawful permanent residents. (title 5 U.S.C. section 552a.)
- Criminal penalties
 - Unauthorized Access: see above.
 - Unauthorized Disclosures: 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 employment, where such disclosure is not authorized by law (see title 18 U.S.C. sections 641, 1030, 1905).
- Department of Homeland Security's (DHS) Chief Privacy Officer: The DHS Chief Privacy Officer is required by statute to ensure that personal information

001088

~~Do not disseminate without the express prior written approval of U.S. Customs and Border Protection (CBP), Office of Chief Counsel, (202) 344-2040.~~

is used in a manner than complies with relevant laws (see section 222 of the Homeland Security Act of 2002 (Public Law 107-296, dated November 25, 2002)). The Chief Privacy Officer is independent of any directorate within the Department of Homeland Security (CBP is an agency within DHS). The determinations of the Chief Privacy Officer are binding on the Department and may not be overturned on political grounds.

001083

WEEKLY MUSTER

Week of Muster: December 28, 2006

Topic: Amendment to the Field Guidelines Regarding Use and Disclosure Passenger Name Record Information (PNR)

Reference Materials: -Annex A – Office of the Secretary, DHS Headquarters Offices
-2005 Field Guidelines

Headquarters POC: Low (b)(2)/(b)(6)

Message: Field Guidelines dated December 1, 2005 were sent to the field regarding the use and disclosure of PNR, particularly for flights to and from the European Union (EU) member states. This memorandum explains the amendments to those Guidelines since the signing of the new interim U.S.-EU PNR Agreement on October 19, 2006. This interim agreement will expire upon the date of any superseding agreement, but no later than July 31, 2007.

- PNR Sensitive Data will continue to be restricted and stored for use upon request. The request must be submitted through the port's chain of command to the Director of Field Operations, and through the Assistant Commissioner of the Office of Field Operations to the Deputy Commissioner of CBP. The request should be submitted in writing and should include all reasons for needing access to the data. Once approval is received, a National Targeting Center supervisor may provide authorization to access the data in the Automated Targeting System-Passenger.
- Certain DHS Components are no longer considered third parties for the transfer of PNR data and have been provided with the same access that CBP has to PNR through the Automated Targeting System-Passenger (ATS-P). Those DHS Components are the entities that directly support the Office of the Secretary, such as all DHS Headquarters offices, including Immigration and Customs Enforcement (ICE). When CBP shares information with these specific components, no disclosure record is needed.
- The following DHS components or U.S. government agencies with counterterrorism functions are excluded from the definition of DHS for the above policy on the transfer and access to PNR data: Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, the United States Coast Guard, and the Federal Emergency Management Agency. These agencies will not have direct access to ATS-P, but may receive PNR through an alternative mechanism described as "facilitated disclosure," or may request access to certain PNR data on a case-by-case basis. When sharing PNR data with these agencies follow the established procedures set forth in section II(B) of the 2005 Field Guidelines.

001890

- Disclosure of PNR data to other government authorities (except as provided for above) will be conducted on a case-by-case basis to such authorities, including foreign government authorities, in accordance with the procedures set forth in section II of the 2005 Field Guidelines.

U.S. CUSTOMS AND BORDER PROTECTION
Department of Homeland Security

Memorandum

July 22, 2003

ENF-1-FO-BTA ETS

TO : Directors, Field Operations
Interim Director, Preclearance Operations
Director, Office of Intelligence

FROM : Assistant Commissioner
Office of Field Operations

SUBJECT: Interim Guidance Regarding Disclosure of Passenger Name Record
(PNR) Information

The attached Guidelines describe the procedures for disclosing PNR information to non-CBP employees. For purposes of this guidance, information contained in a PNR is categorized in two ways: general PNR information and "sensitive" PNR information. This memorandum will provide interim guidance for the disclosure of both types of information. Due to on-going discussions with the European Commission regarding CBP's ability to access PNR data from airline system, it is especially imperative that all CBP personnel with access to this data be familiar with these guidelines and strictly follow the stated procedures.

On June 26, 2002, the Bureau of Customs and Border Protection (CBP) (then, the Customs Service) published a rule implementing 49 U.S.C. 44909(c)(3), regarding CBP access to PNR information. This interim rule requires airlines to establish an electronic connection between their reservation or departure control systems and CBP within 30 days of receiving a written request.

The primary purpose for access to the airline reservation and departure control systems is to prevent and combat terrorism or other threats to national security. CBP treats all PNR data as confidential personal information of the traveler ("Official Use Only" Administrative Classification), and as confidential commercial information of the carrier.

Any unauthorized disclosures of PNR information from CBP computerized systems will result in the imposition of appropriate discipline. Applicable disciplinary action is delineated in Section N, Subsection 2, of the Customs Table of Offenses and Penalties, Unauthorized disclosure of material classified or sensitive to the government.

Vigilance ★ Service ★ Integrity

001899

Also, note that disclosure of such data, including confidential commercial information obtained in the course of employment, where such disclosure is not authorized by law, may lead to criminal sanctions.

If you or a member of your staff have questions regarding this memorandum, feel free to contact Low (b)(2)/(b)(6)

/s/

Jayson P. Ahern

December 28, 2006

MEMORANDUM FOR: DIRECTORS, FIELD OPERATIONS
DIRECTOR, PRECLEARANCE OPERATIONS

FROM: Assistant Commissioner
Office of Field Operations

SUBJECT: Amendment to the Field Guidance Regarding Use and
Disclosure of Passenger Name Record Information (PNR)
(ACTION: TC# 07-0421 TSF: Due: Immediately)

Field Guidelines dated December 1, 2005 were sent to the field regarding the use and disclosure of PNR, particularly for flights to and from the European Union (EU) member states. This memorandum explains the amendments to those Guidelines since the signing of the new interim U.S.-EU PNR Agreement on October 19, 2006. This interim agreement will expire upon the date of any superseding agreement, but no later than July 31, 2007.

The most significant change in this new interim agreement is that DHS is now a party to the agreement (rather than CBP specifically) and DHS has the ability to facilitate the disclosure of PNR data to other U.S. government authorities that exercise counter-terrorism functions. The new approach to disclosure of PNR will primarily benefit the other agencies that will now have more fluid access to this data to help support their counter-terrorism functions. Where applicable, these particular amendments supersede the corresponding policy in the 2005 Field Guidelines, which still apply to flights between the U.S. and Switzerland and Iceland, until further notice. The following is a list of the amendments to be noted to the 2005 Field Guidelines to the extent such guidelines apply to EU PNR; the amendments are referenced by applicable section:

- I(B)(2) – Sensitive Data will continue to be restricted, but may be used in some instances to protect the vital interests of the data subject or others. Access to this data will require the permission from the Deputy Commissioner, CBP. This data will be blocked and, once approved by the Deputy Commissioner, access can be authorized only by a National Targeting Center supervisor in an automated fashion similar to the method used for accessing the restricted OSI, SSI/SSR fields.

- The request should be in writing and it should include all reasons for needing access to such data. It should be forwarded through the appropriate chain of command from the Director of Field Operations through the Assistant Commissioner of the Office of Field Operations to the Deputy Commissioner.
- II(A) – Certain DHS components (Immigration and Customs Enforcement (ICE), Intelligence and Analysis Directorate (I&A), and the Office of the Secretary and the entities that directly support it, i.e., all DHS headquarters offices) are no longer considered third parties for the transfer of PNR data. They will be provided with the same access to PNR as CBP, including access to PNR through the Automated Targeting System-Passenger (ATS-P). When CBP shares information with these specific components, no disclosure record needs to be provided. Attached is a list of those DHS components, which are authorized to obtain PNR through ATS. (*See attached Annex A*)
 - The following DHS components or U.S. government agencies with counterterrorism functions are excluded from the definition of DHS for the above policy on the transfer and access to PNR data: Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, the United States Coast Guard, and the Federal Emergency Management Agency. These agencies will not have direct access to ATS-P, but may receive PNR through an alternative mechanism described as "facilitated disclosure," or may request access to certain PNR data on a case-by-case basis. (*See section II(B) of the 2005 Field Guidelines*)
 - Before disclosing PNR information to these other agencies (including DHS components noted directly above), the relevant agency must certify that they need and would use PNR for the purposes of exercising a counterterrorism function, in order to prevent or combat terrorism or related crimes. The automated disclosure system currently in place (see II(B)(2)(c)(i) of the 2005 Field Guidelines) must be used when disclosing PNR data to these components. These agencies/components can only provide onward disclosures to another agency exercising counterterrorism functions for purposes of preventing or combating terrorism and related crimes in cases (broadly understood to include more generally threats, flights, and routes of concern) that the other agency is examining or investigating. Per the 2005 Field Guidelines, permission from CBP must be obtained before disclosing PNR data for any other permissible purposes.
 - Disclosure of PNR data to other government authorities (except as provided for above) will be conducted on a case-by-case basis to such authorities, including foreign government authorities, in accordance with the procedures set forth in the 2005 Field Guidelines. (*See section II of the 2005 Field Guidelines.*)

- I(B) - CBP will continue to have access to the 34 data elements, but if any of the 34 data elements are listed in a PNR's frequent flyer field (as opposed to the dedicated fields in the main PNR), then the automated system will access that information (or the information will be pushed to CBP by the air carrier, if applicable). Prior to the interim agreement, CBP's access was limited to miles flown and addresses in the frequent flyer field (such data will continue to be obtained under the interim agreement). (See Attachment B of the 2005 Field Guidelines.)
- I(C)(2) – Non-Routine Access: The circumstances under which a non-routine pull or push of PNR data may be requested have been expanded under the interim agreement. Now, if there is an indication that early access to PNR is likely to assist in responding to a specific threat to a flight, set of flights, route(s) or other circumstances associated with an offense referenced in section I(A) of the 2005 Field Guidelines, then follow the procedure set forth in I(C)(2) of the same document.

These amendments are effective immediately. Ensure that all authorized employees know and comply with the guidelines and procedures contained within this document.

If you have any questions, please contact Low (b)(2)/(b)(6)

A muster sheet is attached for use during your daily port musters.

/s/

Jayson P. Ahern

Attachments

**Annex A – Office of the Secretary, DHS Headquarters Offices*

**2005 EU-PNR Field Guidelines*

**Muster*

Annex A

The following individuals and entities are deemed part of "DHS" for purposes of the PNR arrangement:

- Deputy Secretary
- Directorate of Management
- Directorate of Science and Technology
- Directorate for Preparedness
- Office of Policy
- Office of the General Counsel
- Office of Legislative and Intergovernmental Affairs
- Office of Public Affairs
- Office of the Inspector General
- Office of Intelligence and Analysis
- Director, Operations Coordination
- Office of Counter-narcotics Enforcement
- Ombudsman, Citizenship and Immigration Services
- Chief Privacy Officer
- Civil Rights and Civil Liberties Officer
- Director, Federal Law Enforcement Training Center
- Director, Domestic Nuclear Detection Office
- Federal Coordinator, Recovery and Rebuilding of the Gulf Coast Region
- Screening Coordination Office

APPENDIX B

General Information Regarding the Collection of Passenger Name Record (PNR) Data

Statutory and Regulatory Authority to Access PNR

- Pursuant to legal statute (title 49, United States Code, section 44909(c)(3)) and implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide U.S. Customs and Border Protection (CBP) (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems"). CBP does not require air carriers to collect any information in the PNR beyond that which is collected in the reservation and/or departure control systems in the air carrier's ordinary course of business. A copy of the referenced statute and interim regulation is attached hereto.
- Although this statute provides CBP with PNR data in an electronic format, most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, upon arrival of the passenger in the U.S. Electronic collection of PNR, however, substantially enhances CBP's ability to conduct the necessary risk assessments, with the goal of facilitating legitimate travelers and identifying persons of concern, often prior to the boarding of passengers, thereby also increasing aviation security.
- CBP uses PNR data for purposes of preventing and combating terrorism and related crimes and other serious unlawful acts related to CBP's enforcement mission.

Computer System Security at CBP

- Authorized CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the CBP National Data Center.
- PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.
- Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically

recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system.

- Only certain officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data through that system. Access by "contractors" to any PNR data contained in the CBP computer systems is for purposes of assisting in the maintenance or development of CBP's computer system.
- Officers, employees and contractors of CBP are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.
- Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR 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).
- CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34).

U.S. Laws Applicable to CBP's Treatment of PNR Data

- General Policy: CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as required by law (for example, pursuant to a court order).
- Freedom of Information Act: Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA.

- Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure:
 - ✓ where the information is confidential commercial information;
 - ✓ where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy;
 - ✓ where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

(See title 5, United States Code (U.S.C.), sections 552(b)(4), (6), (7)(C)).

- CBP regulations (title 19, Code of Federal Regulations (CFR), section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to:
 - ✓ confidential commercial information;
 - ✓ material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and
 - ✓ information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

CBP invokes these exemptions uniformly based on the character of the data, without regard to the nationality or country of residence of the subject of the data.

- Under the FOIA, any person may request access to their personal information which may be held by CBP. The procedures for making FOIA requests for CBP records are contained in section 103.5 of title 19 of the U.S. Code of Federal Regulations. Decisions by CBP to withhold a record (or part thereof) may be administratively and judicially challenged. (See title 5 U.S.C. section 552(a)(4)(B) and 19 CFR sections 103.7-103.9).
- The Privacy Act: Provides certain protections for personal data held by U.S. government agencies regarding U.S. citizens and lawful permanent residents. (title 5 U.S.C. section 552a.)
- Criminal penalties
 - Unauthorized Access: see above.

- **Unauthorized Disclosures:** 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 employment, where such disclosure is not authorized by law (see title 18 U.S.C. sections 641, 1030, 1905).
- **Department of Homeland Security's (DHS) Chief Privacy Officer:** The DHS Chief Privacy Officer is required by statute to ensure that personal information is used in a manner that complies with relevant laws (see section 222 of the Homeland Security Act of 2002 (Public Law 107-296, dated November 25, 2002)). The Chief Privacy Officer is independent of any directorate within the Department of Homeland Security (CBP is an agency within DHS). The determinations of the Chief Privacy Officer are binding on the Department and may not be overturned on political grounds.

General Information Regarding the Collection of Passenger Name Record (PNR) Data

Statutory and Regulatory Authority to Access PNR

- Pursuant to legal statute (title 49, United States Code, section 44909(c)(3)) and implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide U.S. Customs and Border Protection (CBP) (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems").
- Although this statute provides CBP with PNR data in an electronic format, most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, upon arrival of the passenger in the U.S. Electronic collection of PNR, however, substantially enhances CBP's ability to facilitate legitimate travelers and to conduct the necessary risk assessments, often prior to the boarding of passengers, thereby also increasing aviation security.

Computer System Security at CBP

- Authorized CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the CBP National Data Center.
- PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.
- Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system.
- Only certain officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data through that system. Access by "contractors" to

any PNR data contained in the CBP computer systems is for purposes of assisting in the maintenance or development of CBP's computer system.

- CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.
- Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR 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).
- CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34).

U.S. Laws Applicable to CBP's Treatment of PNR Data

- **General Policy:** CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as required by law (for example, pursuant to a court order).
- **Freedom of Information Act:** Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA.
 - Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure:
 - ✓ where the information is confidential commercial information;
 - ✓ where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy;
 - ✓ where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an

unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

(See title 5, United States Code (U.S.C.), sections 552(b)(4), (6), (7)(C)).

- CBP regulations (title 19, Code of Federal Regulations (CFR), section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to:

- ✓ confidential commercial information;
- ✓ material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and
- ✓ information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

CBP invokes these exemptions uniformly based on the character of the data, without regard to the nationality or country of residence of the subject of the data.

- Under the FOIA, any person may request access to their personal information which may be held by CBP. The procedures for making FOIA requests for CBP records are contained in section 103.5 of title 19 of the U.S. Code of Federal Regulations. Decisions by CBP to withhold a record (or part thereof) may be administratively and judicially challenged. (See title 5 U.S.C. section 552(a)(4)(B) and 19 CFR sections 103.7-103.9).
- The Privacy Act: Provides certain protections for personal data held by U.S. government agencies regarding U.S. citizens and lawful permanent residents. (title 5 U.S.C. section 552a.)
- Criminal penalties
 - Unauthorized Access: see above.
 - Unauthorized Disclosures: 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 employment, where such disclosure is not authorized by law (see title 18 U.S.C. sections 641, 1030, 1905).
- Department of Homeland Security's (DHS) Chief Privacy Officer: The DHS Chief Privacy Officer is required by statute to ensure that personal information is used in a manner that complies with relevant laws (see section 222 of the

Homeland Security Act of 2002 (Public Law 107-296, dated November 25, 2002)). The Chief Privacy Officer is independent of any directorate within the Department of Homeland Security (CBP is an agency within DHS). The determinations of the Chief Privacy Officer are binding on the Department and may not be overturned on political grounds.

General Privacy Protections for Passenger Name Record (PNR) Data

PNR and General Privacy at the U.S. Border

- Although U.S. law permits CBP to access PNR data in an electronic format, most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, upon arrival of the passenger in the U.S. Electronic collection of PNR, however, substantially enhances CBP's ability to facilitate legitimate travelers and to conduct the necessary risk assessments, often prior to the boarding of passengers, thereby also increasing aviation security.

Computer System Security at CBP

- Authorized CBP personnel generally obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the CBP National Data Center.
- PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.
- Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system.
- Only certain officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data through that system. Access by "contractors" to any PNR data contained in the CBP computer systems is for purposes of assisting in the maintenance or development of CBP's computer system.
- CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.
- Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR is subject to strict disciplinary action (which may include termination of employment) and may

001032

result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030).

- CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34).

U.S. Laws Applicable to Treatment of PNR Data

- **General Policy:** CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as necessary to enforce U.S. law (e.g., criminal prosecution) or as otherwise required by law (e.g., pursuant to a court order).
- **Freedom of Information Act:** Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA.
 - Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure:
 - ✓ where the information is confidential commercial information;
 - ✓ where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy;
 - ✓ where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

(See title 5, United States Code (U.S.C.), sections 552(b)(4), (6), (7)(C).)

- CBP regulations (title 19, Code of Federal Regulations (CFR), section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to:

- ✓ confidential commercial information;
- ✓ material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and
- ✓ information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

CBP invokes these exemptions uniformly based on the character of the data, without regard to the nationality or country of residence of the subject of the data.

- Under the FOIA, any person may request access to their personal information which may be held by CBP. The procedures for making FOIA requests for CBP records are contained in section 103.5 of title 19 of the U.S. Code of Federal Regulations. Decisions by CBP to withhold a record (or part thereof) may be administratively and judicially challenged. (See title 5 U.S.C. section 552(a)(4)(B) and 19 CFR sections 103.7-103.9).
- The Privacy Act: Provides certain protections for personal data held by U.S. government agencies regarding U.S. citizens and lawful permanent residents. (title 5 U.S.C. section 552a.)
- Criminal penalties
 - Unauthorized Access: see above.
 - Unauthorized Disclosures: 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 records/information (such as PNR) obtained in the course of his employment, where such disclosure is not authorized by law (see title 18 U.S.C. sections 641, 1030, 1905).
- Department of Homeland Security's (DHS) Chief Privacy Officer: The DHS Chief Privacy Officer is required by statute to ensure that personal information is used in a manner than complies with relevant laws (see section 222 of the Homeland Security Act of 2002 (Public Law 107-296, dated November 25, 2002)). The Chief Privacy Officer is independent of any directorate within the Department of Homeland Security (CBP is an agency within DHS). The determinations of the Chief Privacy Officer are binding on the Department and may not be overturned on political grounds.

U.S. CUSTOMS AND BORDER PROTECTION
Department of Homeland Security

Memorandum

July 22, 2003

ENF-1-FO-BTA ETS

TO : Directors, Field Operations
Interim Director, Preclearance Operations
Director, Office of Intelligence

FROM : Assistant Commissioner
Office of Field Operations

SUBJECT: Interim Guidance Regarding Disclosure of Passenger Name Record
(PNR) Information

The attached Guidelines describe the procedures for disclosing PNR information to non-CBP employees. For purposes of this guidance, information contained in a PNR is categorized in two ways: general PNR information and "sensitive" PNR information. This memorandum will provide interim guidance for the disclosure of both types of information. Due to on-going discussions with the European Commission regarding CBP's ability to access PNR data from airline system, it is especially imperative that all CBP personnel with access to this data be familiar with these guidelines and strictly follow the stated procedures.

On June 26, 2002, the Bureau of Customs and Border Protection (CBP) (then, the Customs Service) published a rule implementing 49 U.S.C. 44909(c)(3), regarding CBP access to PNR information. This interim rule requires airlines to establish an electronic connection between their reservation or departure control systems and CBP within 30 days of receiving a written request.

The primary purpose for access to the airline reservation and departure control systems is to prevent and combat terrorism or other threats to national security. CBP treats all PNR data as confidential personal information of the traveler ("Official Use Only" Administrative Classification), and as confidential commercial information of the carrier.

Any unauthorized disclosures of PNR information from CBP computerized systems will result in the imposition of appropriate discipline. Applicable disciplinary action is delineated in Section N, Subsection 2, of the Customs Table of Offenses and Penalties, Unauthorized disclosure of material classified or sensitive to the government.

Also, note that disclosure of such data, including confidential commercial information obtained in the course of employment, where such disclosure is not authorized by law, may lead to criminal sanctions.

If you or a member of your staff have questions regarding this memorandum, feel free to contact Erik Shoberg, Border Targeting and Analysis, at (202) 927-2531.

/s/

Jayson P. Ahern

Passenger Name Record (PNR) Data

Statutory and Regulatory Authority to Access PNR

- By legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide U.S. Customs and Border Protection (CBP) (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems").

Computer System Security at CBP

- Authorized CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the Customs Data Center.
- PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.
- Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system.
- Only certain officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data. Access by "contractors" to any PNR data contained in the CBP computer systems is for purposes of assisting in the maintenance or development of CBP's computer system.
- CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.
- Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR 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).

- CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34).

U.S. Laws Applicable to the Treatment of PNR Data by CBP

- **General Policy:** CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as required by law.
 - **Freedom of Information Act:** Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA.
 - Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure:
 - ✓ where the information is confidential commercial information, where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy;
 - ✓ where the information is compiled for law enforcement purposes; or
 - ✓ to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy. (See title 5, United States Code, sections 552(b)(4), (6), (7)(C)).
 - CBP regulations (title 19, Code of Federal Regulations, section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to:
 - ✓ confidential commercial information;
 - ✓ material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and
 - ✓ information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy.
- CBP invokes these exemptions uniformly based on the character of the data, without regard to the nationality or country of residence of the subject of the data.

- **Criminal penalties**

- **Unauthorized Access:** see above.
- **Unauthorized Disclosures:** 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 employment, where such disclosure is not authorized by law (see title 18, United States Code, sections 641, 1030, 1905).