



Homeland Security

Privacy Office

September 21, 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Re: DHS/OS/PRIV 07-90/Hofmann request

Dear Ms. Hofmann:

Pursuant to the order of the court, this is our ninth partial release to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated October 20, 2006, for DHS records concerning Passenger Name Records (PNR) from May 30, 2006 to the present including:

1. Emails, letters, reports or other correspondence from DHS officials to European Union officials concerning the transfer and use of passenger data from air carriers to the US for prescreening purposes;
2. Emails, letters, statements, memoranda or other correspondence from DHS officials to U.S. government officials or employees interpreting or providing guidance on how to interpret the undertakings;
3. Records describing how passenger data transferred to the U.S. under the temporary agreement is to be retained, secured, used, disclosed to other entities, or combined with information from other sources; and
4. Complaints received from EU citizens or official entities concerning DHS acquisition, maintenance and use of passenger data from EU citizens.

In our December 15, 2006 letter, we advised you that we had determined multiple DHS components or offices may contain records responsive to your request. The DHS Office of the Executive Secretariat (ES), the DHS Office of Policy (PLCY), the DHS Privacy Office (PRIV), the DHS Office of Operations Coordination (OPS), the DHS Office of Intelligence and Analysis (OI&A), the DHS Office of the General Counsel (OGC), the Transportation Security Administration (TSA), and U.S. Customs and Border Protection (CBP) were queried for records responsive to your request. In our July 27, 2007 letter, we advised you that we expanded our search to include U.S. Immigration and Customs Enforcement (ICE).

Continued searches of the DHS components produced an additional 50 documents, consisting of 210 pages, responsive to your request. I have determined that 4 documents, consisting of 8 pages, are releasable in their entirety; 18 documents, consisting of 84 pages, are releasable in part; and 28 documents, consisting of 118 pages, are withholdable in their entirety. The

releasable information is enclosed. The withheld information, which will be noted on the *Vaughn* index when completed, consists of names, telephone numbers, email addresses, deliberative material, legal opinions, Law Enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, and 7(E) of the FOIA, 5 USC §§ 552 (b)(2), (b)(5), (b)(6), and (b)(7)(E).

FOIA Exemption 2(low) exempts from disclosure records that are related to internal matters of a relatively trivial nature, such as internal administrative tracking. FOIA Exemption 2(high) protects information the disclosure of which would risk the circumvention of a statute or agency regulation. Included within such information may be operating rules, guidelines, manuals of procedures for examiners or adjudicators, and homeland security information.

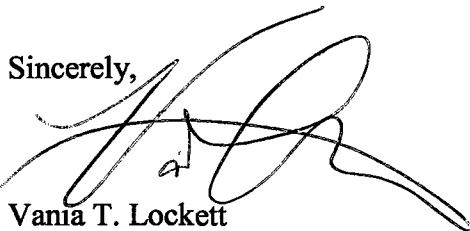
FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. It applies to facts divulged by a client to his attorney, and encompasses any opinions given by an attorney to his client based upon, and thus reflecting, those facts, as well as communications between attorneys that reflect client-supplied information.

FOIA Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Weighed against the privacy interest of the individuals is the lack of public interest in the release of their personal information and the fact that the release adds no information about agency activities, which is the core purpose of the FOIA.

Finally, FOIA Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Our office continues to process your request. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-90/Hofmann request**. The DHS Privacy Office can be reached at 703-235-0790 or 1-866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,



Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 92 pages

Press Information

Decision of the European Court of Justice

On PNR Data Arrangement between the US and European Union

- The Court did not rule against the sharing of PNR data, nor did it determine that the privacy rights of airline passengers were violated or take a view on the content of the PNR arrangement. Rather, the court found that the sharing of PNR data is a law enforcement issue, so the European Commission relied upon the incorrect legal basis in entering into the arrangement with the United States.
- There will be no disruption of transatlantic air traffic as a result of the decision. The European Court of Justice has given the EU until September 30 to identify another legal basis for the PNR arrangement. Until then flights between the U.S. and EU will continue and important security data will continue to flow as normal.
- This is a complex case and we are currently reviewing the decision carefully. We look forward to cooperating with our European counterparts as they work toward a solution.

Background

Passenger Name Record (PNR) is the generic name given to records created by aircraft operators or their authorized agents for each journey booked on behalf of any passenger. The data is used by operators for their own commercial and operational purposes. PNR data comprises a range of elements such as date of ticket reservation, date and place of ticket issue, passenger/travel agent contact details and travel itinerary.

PNR data provides law enforcement officials with a valuable source of data for risk assessment. DHS is working closely with airlines to move expeditiously to a system which sends or “pushes” the data to U.S. Customs and Border Protection (CBP), under the Department of Homeland Security, rather than the current method of CBP “pulling”, or initiating access to, the data from the air carrier’s reservation system. All modifications of CBP systems to support this migration have been made.

The U.S. and the EU concluded a PNR arrangement in May 2004. The PNR arrangement referenced a set of Undertakings which provide a set of

unilateral commitments regarding CBP's collection and handling of PNR data. A September 20-21, 2005 US-EU Joint Review of the Undertakings found CBP in compliance.

This court decision did not criticize DHS's ability to protect personal information or U.S. compliance with the arrangement. The decision states that the European Commission relied upon an inapplicable legal authority to enter into its arrangement with the US. The decision does not question the content of the arrangement, just the basis and process employed. DHS is committed to facilitating safe and efficient travel and appropriate data sharing.

PNR data should not be confused with Advanced Passenger Information System (APIS) data. APIS is created when a passenger checks in for a flight, as well as for a flight's crew – it is designed to provide an exact record of who was on a particular flight and primarily includes data from the machine readable zone of the traveler's passport. APIS data is currently provided to the United States no later than 15 minutes *after* a plane's departure. APIS data has been collected by many countries for over a decade.

of the Undertakings of the Department of Homeland Security, U.S Customs and Border Protection (CBP's) can be found at:

For More Information, Please see the following Websites:

(System down, but would list:

DHS PNR fact sheet

DHS Privacy Office Review



U.S. Customs and
Border Protection

NOV 07 2006

[REDACTED] b(6)
Director
Information Sharing and Knowledge Management
Department of Homeland Security
245 Murray Dr
ATTN: NAC Bldg 19
Washington, DC 20528

[REDACTED] b(6)

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

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

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

imposes personal sanctions on employees who do so. Per CBP policy, all disclosures must be accounted for in CBP's system.

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

If you have any questions, please contact [REDACTED] at [REDACTED]

b(6)

low b(2)
b(6)

Sincerely,

[REDACTED]

b(6)

Executive Director, National Targeting and Security

Enclosure



Homeland Security

Via Electronic Delivery

ATTN: Director General Jonathan Faull
European Commission
B-1049 BRUXELLES
Belgium

ATTN: Ms. Irma Ertman
Presidency of the Council of the
European Union
Ministry of Foreign Affairs
P.O Box 176, Laivastokatu 22
FIN-00161 Helsinki
Finland

Dear Jonathan and Irma:

This letter is intended to set forth our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued on May 11, 2004 by the Department of Homeland Security (DHS). For the purposes of this letter, DHS means the Bureau of Customs and Border Protection, U.S. Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it, but does not include other components of DHS such as the Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, the United States Coast Guard, and the Federal Emergency Management Agency. We look forward to further reviewing these and other issues in the context of future discussions toward a comprehensive, reciprocal agreement based on common principles.

Sharing and Disclosure of PNR

The Intelligence Reform and Terrorism Prevention Act of 2004 required the President to establish an Information Sharing Environment "that facilitates the sharing of terrorism information." Following this enactment, on October 25, 2005 the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to . . . terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the Information Sharing Environment.

Pursuant to Paragraph 35 of the Undertakings (which states that "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law" and allows DHS to "advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings"), the U.S. has now advised the EU that the implementation of the Information Sharing Environment required by the Act and the Executive Order described above may be impeded by certain provisions of the Undertakings that restrict information sharing among U.S. agencies, particularly all or portions of paragraphs 17, 28, 29, 30, 31, and 32.

In light of these developments and in accordance with what follows, the Undertakings should be interpreted and applied so as to not impede the sharing of PNR data by DHS with other authorities of the U.S. government responsible for preventing or combating of terrorism and related crimes as set forth in Paragraph 3 of the Undertakings.

DHS will therefore facilitate the disclosure (without providing unconditional direct electronic access) of PNR data to U.S. government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism and related crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm in writing to DHS that it respects those standards. DHS will inform the EU in writing of the implementation of such facilitated disclosure and respect for the applicable standards before the expiration of the Agreement.

Early Access Period for PNR

While Paragraph 14 limits the number of times PNR can be pulled, the provision puts no such restriction on the "pushing" of data to DHS. The push system is considered by the EU to be less intrusive from a data privacy perspective. The push system does not confer on airlines any discretion to decide when, how or what data to push, however. That decision is conferred on DHS by U.S. law. Therefore, it is understood that DHS will utilize a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment, taking into account the economic impact upon air carriers.

In determining when the initial push of data is to occur, DHS has discretion to obtain PNR more than 72 hours prior to the departure of a flight so long as action is essential to combat an offense enumerated in Paragraph 3. Additionally, while there are instances in which the U.S. government may have specific information regarding a particular threat, in most instances the available intelligence is less definitive and may require the casting of a broader net to try and uncover both the nature of the threat and the persons involved. Paragraph 14 is therefore understood to permit access to PNR outside of the 72 hour mark when there is an indication that early access is likely to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with offenses described in Paragraph 3 of the Undertakings. In exercising this discretion, DHS will act judiciously and with proportionality.

DHS will move as soon as practicable to a push system for the transfer of PNR data in accordance with the Undertakings and will carry out no later than the end of 2006 the necessary tests for at least one system currently in development if DHS's technical requirements are satisfied by the design to be tested. Without derogating from the Undertakings and in order to avoid prejudging the possible future needs of the system any filters employed in a push system, and the design of the system itself must permit any PNR data in the airline reservation or departure control systems to be pushed to DHS in exceptional circumstances where augmented disclosure is strictly necessary to address a threat to the vital interests of the data subject or other persons.

Data Retention

Several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. The Agreement will have expired before Paragraph 15 of the Undertakings requires the destruction of any data, and questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions.

The Joint Review

Given the extensive joint analysis of the Undertakings conducted in September 2005 and the expiration of the agreement prior to the next Joint Review, the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement.

Data Elements

The frequent flyer field may offer addresses, telephone numbers, email addresses; all of these, as well as the frequent flyer number itself, may provide crucial evidence of links to terrorism. Similarly, information about the number of bags carried by a passenger may have value in a counterterrorism context. The Undertakings authorize DHS to add data elements to the 34 previously set forth in Attachment "A" of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3.

With this letter the U.S. has consulted under Paragraph 7 with the EU in connection with item 11 of Attachment A regarding DHS's need to obtain the frequent flier number and any data element listed in Attachment A to the Undertakings wherever that element may be found.

Vital Interests of the Data Subject or Others

Recognizing the potential importance of PNR data in the context of infectious disease and other risks to passengers, DHS reconfirms that access to such information is authorized by paragraph 34, which provides that the Undertakings must not impede the use of PNR for the protection of the vital interests of the data subject or of other persons or inhibit the direct availability of PNR to relevant authorities for the purposes set forth in Paragraph 3 of the Undertakings. "Vital interests" encompasses circumstances in which the lives of the data subject or of others could be at stake and includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay. Such data will be protected in a manner commensurate with its nature and used strictly for the purposes for which it was accessed.

Sincerely yours,



Stewart Baker
Assistant Secretary for Policy

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

I. Use of PNR Information¹

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

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

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

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

B) Available Data Elements

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

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

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

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

high b(2)
b(7)E

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

high b(2)
b(7)E

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

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

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

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

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

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

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

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

[REDACTED]

[REDACTED]

[REDACTED]

high b(2)
b(7)E

II. Disclosure of PNR Information

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

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

2) **Disclosures to Other U.S. Government Authorities with Counterterrorism functions** [REDACTED] b(5)
Authorized DHS Users may disclose PNR to other U.S. government authorities with counterterrorism functions for purposes of preventing or combating terrorism or related crimes, where such authority has been certified by CBP to receive facilitated access to PNR (i.e., where Authorized DHS Users are working jointly with an agency which has facilitated access, but disclosure is to be through a means other than by that agency through ATS-P). All Authorized DHS Users should use the automated disclosure system for such disclosures. For each disclosure, a PNR Disclosure Form and CF 191 must be completed to document the release of information. This form is automated within ATS-P and can be generated before or after accessing the PNR. The system will generate the required forms and pre-populate some of the information.

[REDACTED] wis h b(2) b(7)E

3) **Disclosures to other government authorities (except as provided for under paragraphs II(A)(1) and (2) above):**

a) PNR information may be disclosed on a case-by-case basis to such authorities, including foreign government authorities, in the following circumstances and in accordance with the procedures set forth in paragraph II(A)(2)(b) below:

[REDACTED] b(5)

- i) To another government authority that has law enforcement or counter-terrorism functions, where the disclosure is consistent with a purposes identified above in paragraph I(A)(1). Disclosures to such government authorities should only be made if it is determined that:
 - the receiving government authority is responsible for preventing, investigating or prosecuting violations of, or enforcing or implementing, a statute or regulations related to the purpose of the request; and
 - Authorized DHS Users are aware of an indication of a violation or potential violation of law.
- ii) To relevant government authority(s), where disclosure of the PNR data is necessary to protect the vital interests of the subject of the PNR or of other persons (for example, in the case of significant health emergencies or epidemics).

b) Disclosure Procedures and Conditions:

- i) Written Request: If another government authority is requesting information that would include PNR data, a written request from that government authority must explain the specific information requested and the reason(s) for the request. This written request may be submitted via e-mail by the requesting government authority and must be submitted prior to the disclosure of any PNR information. Only under exigent circumstances may PNR information be disclosed based on a verbal request. If this occurs, a written request must be submitted as soon as possible following the disclosure of the PNR information based on verbal representations.
- ii) Review of Purpose: Review the request to insure that the purpose for obtaining the data relates to the purposes for which that government authority is permitted to receive PNR data (see paragraph I(A)(1) above).
- iii) Record of Disclosure: All disclosures (regardless of the citizenship or residence of the data subject) must be recorded in accordance with the following procedures:
 - A PNR Disclosure Form and CF 191 must be completed to document the release of information. This form is automated within ATS-P and can be generated before or after accessing the PNR. The system will generate the required forms and pre-populate some of the information.

high b(2)
b(7)E



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

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

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

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

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

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

high b(2)
b(7)E



C) Mandatory Disclosures of PNR

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

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

III. Corrections and Complaints Regarding PNR Data:

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

IV. Data Security

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

- B) ICE and the DHS Office of the Secretary have implemented policies which comport with those of CBP's with regard to the treatment and handling of PNR data by their users (including these PNR Field Guidelines). Unauthorized access by any personnel to air carrier reservation systems or ATS-P (in which PNR data is stored) is subject to strict disciplinary action (which may include termination of employment) and may result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030).
- C) ICE and the DHS Office of the Secretary policies (consistent with CBP applicable policy and regulations) also provide for stringent disciplinary action (which may include termination of employment) to be taken against any employee who discloses PNR data without official authorization (title 19, Code of Federal Regulations, section 103.34). Criminal penalties (including fines, imprisonment of up to one year, or both) may be assessed against any officer or employee of the United States for disclosing PNR data obtained in the course of his/her employment, where such disclosure is not authorized by law (see title 18, United States Code, sections 641, 1030, 1905).

V. Process for Access to CBP's System

- A) ICE and the Office of the Secretary have established a single point of contact (liaison) for their agency through which to forward PNR access requests. In cases of system misuse or abuse or system inactivity, the agency point of contact will be notified by CBP.
- B) All new requests for access to PNR data from the ATS-P database must be approved by each requestor's supervisor before being forwarded to the agency/office's PNR point of contact. Once approved then the request will be forwarded to the approving official at CBP Headquarters, Office of Field Operations (OFO).
- C) Request for access to CBP's system is to be forwarded by email from the agency/office's PNR point of contact to the ATS-P Program Manager, OFO at CBP Headquarters (currently [REDACTED] at [REDACTED] [REDACTED] low b(2) b(6)
- D) An invitation letter, a Request Letter template, and a CBP Form 7300 will be forwarded to the requestor's agency point of contact, along with the pertinent policies and documents for PNR use and ATS-P access.
- E) Once the Request Letter and CBP Form 7300 is received by OFO and access is approved by CBP's system security and OFO, accounts and passwords will

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

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

VI. Training

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

VII. No Private Right Created

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

Attachment "A"

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

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

Joining effective January, 2007: Bulgaria and Romania

Attachment "B"

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

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

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

entire page
high (b)(2)
(b)(7)(E)

entire page
high (b)(2)
(b)(7)(E)

entire page
with (b)(2)
(b)(7)(C)

entire page
with (b)(2)
(b)(7)(C)

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

[Salutation]

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

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

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

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

2-C

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

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

In addition to the list below, [agency name] is attaching a completed CBP Form 7300 for each user requesting access. [Agency Name] acknowledges the form is necessary to expedite the adjudication of clearance sufficient for access to ATS-P.

[Agency to insert names, SSN or hash ID, job titles, office/ branch/ division/ agency/ department, location of office, supervisor's name and SSN or hash ID.]

Thank you for your consideration [or similar closing].

[Agency signatory, at least Director level]

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

U.S. DEPARTMENT OF HOMELAND SECURITY
Bureau of Customs and Border Protection

**INFORMATION SYSTEMS SECURITY ADMINISTRATION
NON-CBP USER CERTIFICATION**
For Government Employees Only

When filling out manually, please type or print.

Authorized Access to the Bureau of Customs and Border Protection Records

I, _____, certify that the user named below has
(Agency Security Officer)
successfully completed a National Agency Check and written Inquires (NACI) or Background
Investigation (BI) which meets the standards and criteria set forth in the 5 CFR, Chapter 736-13.
Further, I certify that there is currently no internal investigation, or prior investigation with our agency,
for which said user has not been cleared, the allegation of which would call into question the user's
integrity or character in such a way as to make the sharing of sensitive law enforcement information
with the user inappropriate.

USER INFORMATION	
Name:	Title:
Social Security Number:	Date of Birth (mm/dd/yyyy):
Work Location:	Phone Number:
Supervisor's Name:	Phone Number:
Agency:	Agency Headquarters Location:

CERTIFICATION(s)		
NACI Certification (LAN Access)	<input type="checkbox"/> YES <input type="checkbox"/> NO	Date Completed:
BI Certification (LAN/Mainframe Access)	<input type="checkbox"/> YES <input type="checkbox"/> NO	Date Completed:

AGENCY SECURITY OFFICER	
Name:	Title:
Location:	Phone Number:
Signature: X	Date:

Fax completed form and request for system access to the Information Systems Security Branch at (703) 921-6395.
CBP Form 7300 (12/03)

2-D

January 28, 2005

ENF-1-FO-NTS ETS

TO : Directors, Field Operations
Director, Preclearance Operations

FROM : Executive Director, National Targeting and Security /s/ [REDACTED]

b(6)

SUBJECT: Requirements for Access to the Automated Targeting System - Passenger (ATS-P)

Passenger Name Record (PNR) data is some of the most sensitive data used by CBP to identify, target, and intercept persons intent on harming the U.S. Due to the sensitive nature of this data, and to protect personal privacies, CBP is taking a proactive approach in limiting access to sensitive passenger data to CBP employees with an official "need to know."

Authorized CBP employees can access risk-scored passenger information via CBP's computer systems via the Automated Targeting System – Passenger (ATS-P). Access to risk-scored passenger data is to be used strictly for enforcement purposes, including use in threat analysis to identify, interdict and exclude potential terrorists and other serious criminal offenders. Port and Field Office management are required to monitor access to passenger data to ensure only those CBP employees with a need to know have this access.

All new requests for access to ATS-P must be approved by the CBP employee's direct supervisor, (or other person designated by the employee's DFO), before being forwarded to the approving official at Headquarters, Office of Field Operations. The supervisor is responsible for determining if the requested access is necessary for the CBP Officer's performance of their duties. If approved by the supervisor, the request must be forwarded to [REDACTED] of National Targeting and Security for final approval and processing. Only then can access to ATS-P be initiated.

b(6)

If the CBP Officer no longer requires ATS-P access to perform their duties (e.g., change of work assignment or separation from CBP), then the supervisor is required to notify National Targeting and Security of this change. National Targeting and Security staff will remove access for any personnel who no longer require ATS-P and/or Resmon to perform their duties. The process for new requests for access to the Reservation Monitoring System (Resmon) were recently outlined in a memorandum dated December 30, 2004.

A recent review of officers with access to ATS-P and Resmon was conducted which identified a significant number of users who have not accessed these systems in the past 90 days. Due to the sensitive nature of the data and the requirement that only those personnel with a need to know can access the data, effective immediately, employees who have failed to log in to either ATS-P or Resmon within a 90-day period will lose access to that system. If an employee requests to be reinstated, the DFO is responsible for verifying and notifying National Targeting and Security of the employee's need to retain access to ATS-P and/or Resmon.

As a reminder, please ensure that all employees who are authorized access to PNR information have signed a receipt upon receiving these guidelines per the following memorandum "Field Guidance Regarding Use and Disclosure of Passenger Name Record Information (PNR) [redacted] dated December 20, 2004. Additionally, each employee's supervisor is responsible for recording their employee's receipt of the above document in [redacted] using the course titled, [redacted] course code number [redacted]

low
(b)(2)

If you have any questions, please have your staff contact [redacted] at [redacted]


b(6)


[redacted]

low b(2)
b(6)



U.S. Customs and
Border Protection

MEMORANDUM FOR: DIRECTORS, FIELD OPERATIONS
DIRECTOR, PRECLEARANCE OPERATIONS  6(6)

FROM: Acting Director, Border Targeting and Analysis 

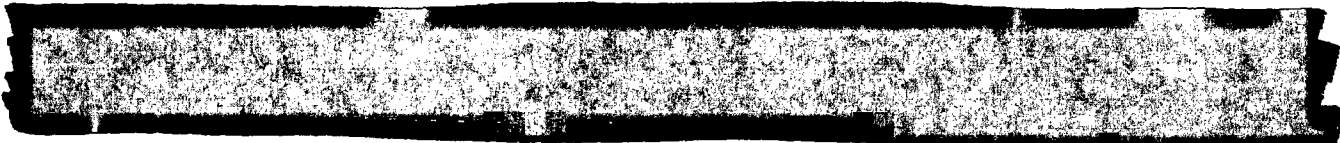
SUBJECT: Standardization of ATS Access Requests for ATS Modules

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

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

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

- The prospective user's supervisor must submit a properly completed access request form to the designated OFO/NTS manager identified for the specified ATS module. RESMON access requires the access request form be submitted by the designated OFO/DFO.
- The following access request fields are required in order to ensure uniformity among field locations. Please note that commas, dashes and periods should not be used when completing the form. LOW (b)(2)



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

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

ATS Modules are comprised of the following:

- **ATS-N (Inbound)** access is provided to CBP personnel assigned in the air and sea cargo environments, Express Courier Hubs, CSI locations, select ICE agents and personnel assigned at the NTCC for cargo targeting and analysis. ATS-N provides enforcement information from TECS, transactional data from ACS as well as exterior data sources, and ensures relevant data is available to ATS-N in time for CBP to effectively evaluate and investigate inbound shipments prior to arrival. Requests for access must be provided in the prescribed format to the appropriate managers, [redacted] at [redacted] or [redacted] a [redacted]

b(6) [redacted] at [redacted] low b(2) [redacted] b(6)

- **ATS-AT (Anti-terrorism / Outbound)** access is provided to CBP personnel assigned to outbound cargo environments and NTC personnel. ATS-AT provides an efficient means of identifying high-risk export shipments among the millions of recorded shipments and incorporates the enforcement of other government agency laws to include Treasury Office of Foreign Asset and Control lists; targeting for materials defined by the Nuclear Regulatory Commission (NRC) as weapons of mass destruction components; and ensures adherence to the State Department’s Office of Defense Trade Controls (ODTC) Regulations. Requests for access must be provided in the prescribed format to the appropriate OFO/NTS managers, [redacted] at [redacted] or [redacted] a [redacted]

b(6) [redacted] at [redacted] low b(2) [redacted] b(6)

- **ATS-L (Land)** access is provided to CBP personnel assigned to Land Border crossing locations. ATS-L capabilities include the automatic crosschecks of information [redacted]

high b(2)
b(7)E

lookout for terrorism, smuggling, etc. Requests for access must be provided in the prescribed format to the appropriate OFO/NTS manager [redacted] at [redacted]

[redacted] low b(2) b(6)

- The Trend Analysis and Analytical Selectivity Program (TAP2K) supports field users and ATS. TAP is an analytical profile tool that aggregates data [redacted]

high b(2) b(7)E

[redacted] This information is utilized by ATS, field personnel and other disciplines to review historical trends and trade patterns [redacted]

high b(2) b(7)E

Requests for access must be provided in the prescribed format to the appropriate OFO/NTS managers [redacted] at [redacted] or [redacted]

b(6)

[redacted] at [redacted] low b(2) b(6)

low b(2) b(6)

b(6)

b(5)

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

low b(2) b(6)

b(6)

- ATS-P (Passenger) utilizes information from a diverse set of databases to allow CBP officers to conduct research queries of international travelers to assist in the inspectional decision-making process. ATS-P contains data such as border crossings, I-94 and visa data, as well as modules for reviewing airline reservation data (PNR), and passenger arrival statistics (ATS-PDA.) Due to an agreement between DHS and the European Union, access to PNR data is limited based on the user roles described below.

- o Basic User Role access is typically provided to [redacted] whose duties do not require access to PNR data.

high b(2) b(7)E

- o CTR User Role access is given to [redacted] whose duties require viewing PNR data no older than seven (7) days after a flight's arrival to, or departure from, the U.S.

high b(2) b(7)E

- o PAU User Role access is given to [redacted] and permits viewing of PNR data older than seven (7) days, but no older than 3.5 years, unless the PNR is linked to an enforcement record.

high b(2) b(7)E

- o The PAU Supervisor User Role access is provided to [redacted] [redacted] This user role allows viewing of PNR data with the same conditions as the PAU User Role. Recipients can grant permission to view restricted PNR fields to officers with PNR access.

high b(2)
b(7)E

b(6) All requests for ATS-P access, including the Resmon and ATS-PDA modules, must be provided in the prescribed format to the appropriate OFO/NTS managers, [redacted] at [redacted] and [redacted] at [redacted] [redacted] low b(2) b(6) low b(2) b(6)

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

Requestors should not contact the approving OFO/NTS manager directly to inquire about the status of their pending access requests. Problems encountered attempting to access the ATS modules should be directed to the ATS Hotline at [redacted] [redacted] low b(2) b(6)

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

If you have any questions, please direct them via email to [redacted] at [redacted] or telephonically [redacted] or [redacted] at [redacted] or telephonically [redacted] [redacted] low b(2) b(6) low b(2) b(6) low b(2) b(6) b(6)

ENF-1-FO-NTS ETS

TO : Directors, Field Operations
FROM : Executive Director, National Targeting and Security
SUBJECT: Requests for Access to Passenger Name Record (PNR) Information via
Customs and Border Protection Computer Systems

Authorized CBP employees access PNR information via CBP's computer systems in two different ways. PNR information is available through the Automated Targeting System – Passenger (ATS-P) and the Reservation Monitoring System (Resmon).

Only employees of CBP with an official "need to know" are to have direct electronic access to reservation/departure control system data. Access to PNR data is to be used strictly for enforcement purposes, including use in threat analysis to identify, interdict and exclude potential terrorists and other serious criminal offenders. CBP considers all data obtained from airline reservation/departure control systems to be sensitive. Port management is required to monitor access to PNR information to ensure only those CBP employees with a need to know have this access.

Effective immediately, all new requests for access to Resmon and the ATS-P PNR database must be approved by the Director, Field Operations (DFO) before being forwarded to the approving official at Headquarters, Office of Field Operations. The Director is responsible for determining if the requested access is necessary for the CBP Officer's performance of their duties. If approved by the Director, the request must be forwarded to [REDACTED] of National Targeting and Security. Only then will access to PNR information be granted. If the CBP Officer no longer requires PNR access to perform their duties (e.g., change of work assignment or separation from CBP), then the DFO is required to notify National Targeting and Security of this change. b(6)

If you have any questions, please have your staff contact [REDACTED] at [REDACTED] b(6)

low b(2)
b(6)

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



U.S. Customs and
Border Protection

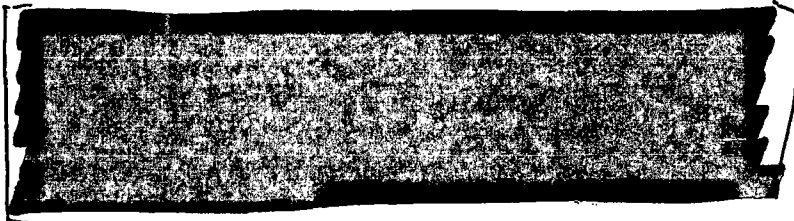
DEC 27 2006

[REDACTED] b(6)
Director, Information Sharing and Knowledge Management
Department of Homeland Security
245 Murray Drive
ATTN: NAC Bldg 19
Washington, DC 20528

[REDACTED] b(6)

Thank you for your recent letter requesting access to Passenger Name Record (PNR) data collected by Customs and Border Protection. CBP has reviewed the request and authorizes access to PNR data contained within the Automated Targeting System – Passenger (ATS-P) for the following Department of Homeland Security I&A personnel:

b(6)



If any of the personnel listed above leave the employment of the Department of Homeland Security, CBP must be notified immediately to remove the user's access to PNR.

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

(6)

If you have any questions, please contact [redacted] [redacted]
All ATS-P users may request technical assistance from the ATS hotline at [redacted]

b(6)

low b(2)
b(6)

[redacted] low b(2)
b(6)

Sincerely,

[redacted signature]


b(6)

Acting Executive Director, National Targeting and Security
Office of Field Operations



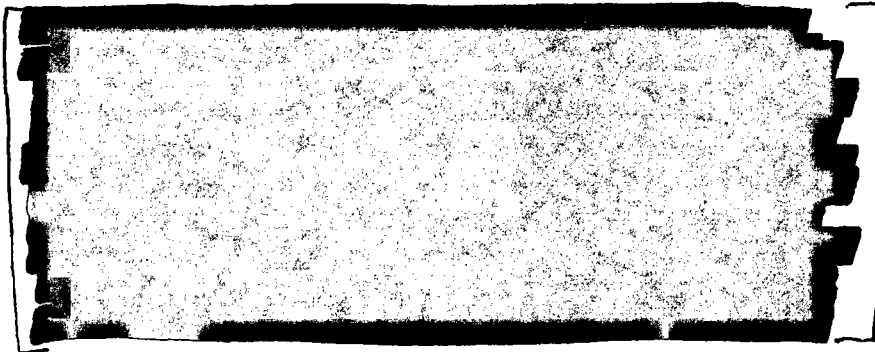
U.S. Customs and
Border Protection

DEC 27 2006

 b(6)
Director, Office of Investigations
Immigration and Customs Enforcement
421 I Street, N.W.
Washington, DC 20536

 b(6)

Thank you for your recent letter requesting access to Passenger Name Record (PNR) data collected by Customs and Border Protection. CBP has reviewed the request and authorizes access to PNR data contained within the Automated Targeting System – Passenger (ATS-P) for the following Office of Investigations personnel:

b(6) 

If any of the personnel listed above leave the employment of the Office of Investigations, CBP must be notified immediately to remove the user's access to PNR.

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

horization and poses personal sanctions on employees who do so. Per CBP policy, all disclosures must be accounted for in CBP's system.

If you have any questions, please contact [redacted] ^{b(6)} at [redacted] ^{low b(2)}
All ATS-P users may request technical assistance from the ATS hotline at [redacted] ^{b(6)}

Sincerely,

[redacted signature] b(6)

Acting Executive Director, National Targeting and Security
Office of Field Operations



U.S. Customs and
Border Protection

NOV 07 2006

[REDACTED] b(6)
Office of Investigations
Immigration and Customs Enforcement
425 I Street, N.W., Washington, DC 20536

[REDACTED] b(6)

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

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

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

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

If you have any questions, please contact [REDACTED]

b(6)

at [REDACTED]

low b(2)
b(6)

Sincerely,

[REDACTED]

b(6)


Executive Director, National Targeting and Security

Enclosure



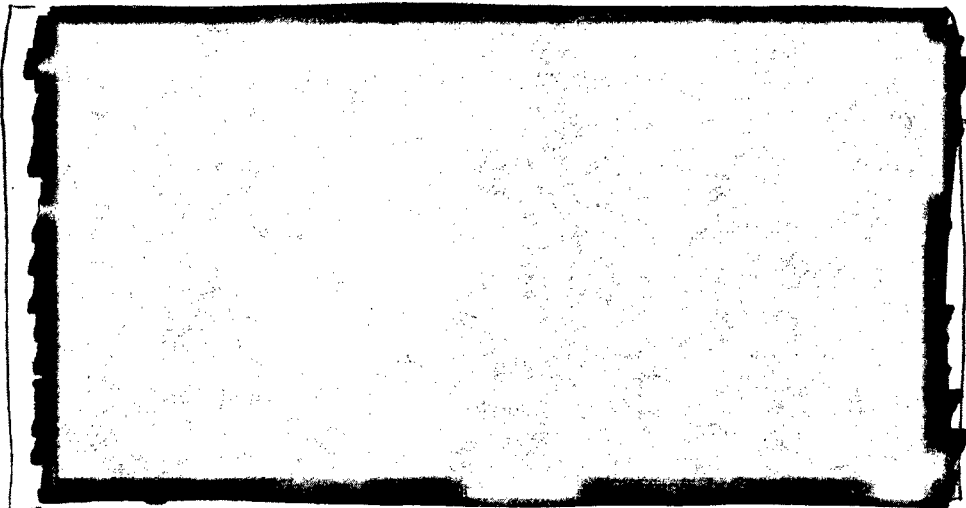
U.S. Customs and
Border Protection

DEC 27 2006

 b(6)
Acting Director, Office of Intelligence
Immigration and Customs Enforcement
425 I Street, N.W.
Room 5300
Washington, DC 20536

 b(6)

Thank you for your recent letter requesting access to Passenger Name Record (PNR) data collected by Customs and Border Protection. CBP has reviewed the request and authorizes access to PNR data contained within the Automated Targeting System – Passenger (ATS-P) for the following Immigration and Customs Enforcement Office of Intelligence personnel.



b(6)

If any of the personnel listed above leave the employment of the Department of Homeland Security, CBP must be notified immediately to remove the user's access to PNR.

All activity within ATS-P is monitored and audited and there are serious consequences for violation of the PNR Field Guidance. As set forth in these policies, CBP considers PNR information to be law enforcement sensitive, confidential personal information of the data subject ("Official Use Only")

Administrative Classification), and confidential commercial information of the air carrier, exempt from disclosure pursuant to 5 U.S.C. 552 (b)(2), (b)(4), (b)(6), and (b)(7)(c). PNR records may also be protected under the Privacy Act if the subject of the record is a U.S. citizen or permanent resident (5 U.S.C. 552a). Furthermore, the Trade Secrets Act (18 U.S.C. 1905) prohibits federal employees from disclosing information defined in that section without authorization and imposes personal sanctions on employees who do so. Per CBP policy, all disclosures must be accounted for in CBP's system.

If you have any questions, please contact [redacted] at [redacted].
All ATS-P users may request technical assistance from the ATS hotline at [redacted].

b(6)

low b(2)
b(6)

[redacted] low b(2)
b(6)

Sincerely,

[redacted signature]

b(6)

Acting Executive Director, National Targeting and Security
Office of Field Operations



U.S. Customs and
Border Protection

NOV 07 2006

[REDACTED]

b(6)

Office of Intelligence
Immigration and Customs Enforcement
425 I Street, N.W.
Room 5300
Washington, DC 20536

[REDACTED]

b(6)

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

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

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

imposes personal sanctions on employees who do so. Per CBP policy, all disclosures must be accounted for in CBP's system.

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

If you have any questions, please contact Mr. [REDACTED]

b(6)

low b(2)

at [REDACTED]

b(6)

Sincerely,

b(6)

[REDACTED]
Executive Director, National Targeting and Security

Enclosure

[b5] PNR Information Sharing

[b5]

1. Data may only be shared for the purpose of preventing and combating: 1) terrorism and related crimes; 2) other "serious crimes," including organized crime, that are "transnational in nature"; and 3) flights from warrants or custody for the crimes described above.

2. Data may not be shared with any agency outside of CBP (including other DHS components, other Federal agencies, or foreign governments) except on a "case-by-case basis" for preventing or combating these identified offenses.

Before transferring the data CBP must determine:

3. that the receiving agency has responsibility for the prevention of prosecution of the forgoing offenses; and
4. that there is an "indication" of a violation or potential violation of law

CBP must insure that data transferred to other agencies is:

5. used only for the purposes identified;
6. disposed of in conformance with agreed upon retention rules;
7. handled as law enforcement sensitive; and
8. not further transferred without CBP's express permission

9. Bulk transfers of data are prohibited - [b7E 62 H&L]

[b5]

10. Data may be retained for only 3 ½ years (or 8 years if the data has been accessed);

11. "Sensitive" PNR data (e.g. race, ethnicity, political opinion, religious or philosophical belief, trade union membership and data concerning health or sex life) may not be collected



Homeland Security

[b2]

INFORMATION

Comment [JL1]:

Deleted: June 27, 2006 June 26, 2006 June 22, 2006 June 22, 2006 June 13, 2006

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy

THROUGH: Paul Rosenzweig, Acting Assistant Secretary, PDEV and Councilor to the Assistant Secretary for Policy

FROM: 2006 Working Group

SUBJECT: Summary of potential changes to seek in the PNR Undertakings

Deleted: Michael Scardaville, Special Assistant/International Policy Advisor

Purpose

Per your request, below is an assessment of areas of the Undertakings DHS should seek to negotiate in the S.O. PNR arrangement.

Summary

In anticipation of future negotiations with the EU on the PNR Agreement.

b5

Background

b5

b5

x

b5

Likely Top Priorities:

b5
b7E
b2H

X

b5

b7E

b2H

X

X

b5

b7E

b2H

X

X

b5
b7E
b2H

X

|

... X

b5
b7E
b2H

|

X

62 J
INFORMATION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy
THROUGH: Paul Rosenzweig, Acting Assistant Secretary, PDEV and
Councilor to the Assistant Secretary for Policy
FROM: PNR Working Group
SUBJECT: Summary of potential changes to seek in the PNR
Undertakings

Purpose

In anticipation of future negotiations with the EU on the PNR arrangement, below is an assessment of areas of the Undertakings DHS should seek to change in the US-EU PNR arrangement. '

b5

]

As a result, the Department's top priority should be to replace or amend these provisions to allow for

b5

]

Background

b5
b7E
b2 H

b5

]

Discussion

b5
b7E
b2H

b5

b7E

b2H

he

b 5
b 7 E
b 2 H

Attachments:

1. Detailed Assessment of Critical Issues
2. List of Sensitive Terms

Attachment 1: Detailed Assessment of Critical Issues

b 2H
b 5
b 7E

b2H

b5

b7E

b2H

b5

b7E

Attachment 2

"Sensitive Data"

Codes

Description	Data Field type	Code
--------------------	----------------------------	-------------

b7E
b2H

b 2 H
b 7 E

Terms

b 2 H
b 7 E

b2H

b7E

Attachment B

cb2]

~~Deleted: July 21, 2006~~

INFORMATION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy
THROUGH: Paul Rosenzweig, Acting Assistant Secretary, PDEV and
Councilor to the Assistant Secretary for Policy
FROM: PNR Working Group
SUBJECT: Summary of potential changes to seek in the PNR Undertakings

Purpose

In anticipation of future negotiations with the EU on the PNR arrangement, below is an assessment of areas of the Undertakings DHS should seek to change in the US-EU PNR arrangement.

b5

As a result, the Department's top priority should be to replace or amend these provisions to allow for '

b5

~~FOR OFFICIAL USE ONLY~~

Background

b5
b7E
b2H

of

s

n

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

Discussion

b 5
b 7E
b 2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b 5
b 7 E
b 2 H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b5
b7E
b2H

Attachments:

- 1. Detailed Assessment of Critical Issues**
- 2. List of Sensitive Terms**

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

Attachment 1: Detailed Assessment of Critical Issues

b5
b7E
b2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b 5
b 7E
b 2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b 5
b 7E
b 2 H

~~FOR OFFICIAL USE ONLY~~

Attachment 2

"Sensitive Data"

Codes

Description	Data Field type	Code
-------------	-----------------	------

1

b 7E
b 2 H

~~FOR OFFICIAL USE ONLY~~

b7E
b2H

Terms

b7E
b2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b 7E
b 2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b2H
b7E

FOR OFFICIAL USE ONLY

bb

From: []
Sent: Tuesday, August 08, 2006 11:56 AM
To: [] Rosenzweig, Paul;

b4 b2

Scardaville, Michael;

b6

Cc: Baker, Stewart]
Subject: Re: URGENT: DC DISCUSSION PAPER FOR IMMEDIATE COMMENT

Much appreciated.

National Security Council
The White House
Washington, D.C. 20504

bb
b2

-----Original Message-----
From: []
To: []

Rosenzweig, Paul;

b6

Scardaville, Michael;

b6

CC: Baker, Stewart]
Sent: Tue Aug 08 11:54:46 2006
Subject: RE: URGENT: DC DISCUSSION PAPER FOR IMMEDIATE COMMENT

DHS consolidated comments should be waiting for you on the SIPRNET side. Thanks for your patience.

Without going into details, it's pretty difficult for us to receive on SIPRNET and distribute within DHS for comment.

Director of International Privacy Programs
DHS, Privacy Office
Tel.
Fax:
Email:

bb
b2

This communication, along with any attachments, is covered by federal and state law

15

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

From: []
Sent: Tuesday, August 08, 2006 11:39 AM
To: [] Rosenzweig, Paul:

] b6 b2

b6

Scardaville, Michael;

Cc: Baker, Stewart]
Subject: RE: URGENT: DC DISCUSSION PAPER FOR IMMEDIATE COMMENT

Please send on other system to all on the email I sent. Thanks.

[] b6

From: []
Sent: Tuesday, August 08, 2006 11:24 AM
To: [] Rosenzweig, Paul:

] b6 b2

b6

Scardaville, Michael;

Cc: Baker, Stewart]
Subject: RE: URGENT: DC DISCUSSION PAPER FOR IMMEDIATE COMMENT

FOR NSC

[] b6

I will send comments via SIPRNET but as back-up, I'm sending DHS's comments to the August 7 Draft DC Discussion paper. Below are DHS comments:

Page 1-

Page 2 -

b5

Page 2 -

b5

Page 2 -

b5

7

Page 3 -

b5

Page 3 -

b5

Page 3 -

b5

Page 3 -

b5

b5

Page 4 -

b5

Page 4 -

b5

Page 5 -

Page 5 -

b5

p. 6 -

Page 6 -

b5

Page 7 -

b5]

Sent on behalf of:

DHS

Paul Rosenzweig

Counselor to the Asst. Secy. (Policy Directorate) and

Acting Assistant Secretary for Policy Development Dept. of Homeland Security
Washington, DC 20528

Ph:

b2 b6

E:

b6

Director of International Privacy Programs

DHS, Privacy Office

Tel.

b2 b6

Fax:

Email:

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

166

From: Baker, Stewart [b2]
Sent: Sunday, September 24, 2006 1:04 PM
To:

b6
b2

Subject: With apologies, a slightly revised document
Attachments: PNR_interp_letter_edited.doc



PNR_interp_letter_edited.doc (...)

I'm attaching a slightly revised (and tracked) version of the interpretation letter. The changes, which come from our final internal review, aren't intended to revise the understanding reached with DOJ but rather to give greater clarity about the paragraphs that will be affected by the interpretation.

For those on bbry, the principal change is the last half of the paragraph pasted below:

Paragraph 35 of the Undertakings provides that "No statement herein shall impede the use or disclosure of PNR data ... as ... required by law" and provides that CBP will advise the European Commission regarding the passage of any legislation that materially affects statements made in the Undertakings. The U.S. has now advised the EU that implementation of the information-sharing legal changes described above is impeded by certain provisions of the Undertakings that restrict information sharing among U.S. agencies, particularly all or portions of paragraphs 17, 28, 29, 30 31, and 32. [

b5

Stewart

16

~~FOR OFFICIAL USE ONLY~~

Attachment D

[b2]

INFORMATION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy
THROUGH: Paul Rosenzweig, Acting Assistant Secretary, PDEV and
Counselor to the Assistant Secretary for Policy
FROM: PNR Working Group
SUBJECT: Summary of potential changes to seek in the PNR Undertakings

Purpose

In anticipation of future negotiations with the EU on the PNR arrangement, below is an assessment of areas of the Undertakings DHS should seek to change in the US-EU PNR arrangement.

b5

As a result, the Department's top priority should be to replace or amend these provisions to allow for:

b5

Background

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b5
b7E
b2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b5

Discussion

b5
b7E
b2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b5
b7E
b2H

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

b5
b7c
b2H

Attachments:

- 1. Detailed Assessment of Critical Issues**
- 2. List of Sensative Terms**

~~FOR OFFICIAL USE ONLY~~

[b6]

From: Scardaville, Michael [b2]
Sent: Thursday, June 01, 2006 2:20 PM
To: Isles, Adam; Baker, Stewart; Scardaville, Michael
Cc: [b6] Rosenzweig, Paul; Dunne, Julie
Subject: RE: EU accomplishments memo for POTUS

Attachments: 060523 Draft S1 Memo to POTUS 2.0-sbeds-aieds.doc



060523 Draft S1
Memo to POTUS ...

Updated with Adam's edits.

Mike

[b2]

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

From: Isles, Adam [mailto:[b2]]
Sent: Thursday, June 01, 2006 1:12 PM
To: Baker, Stewart; Scardaville, Michael
Cc: [b6] Rosenzweig, Paul; Dunne, Julie
Subject: Re: EU accomplishments memo for POTUS

In the PNR section, would propose adding couple clarifications, in ALL CAPS

"To combat terrorists' travel to the US, DHS requires that all carriers flying to the US make information from their reservation systems available to Customs & BORDER PROTECTION prior to departure. This was done under the Aviation Transportation Security Act for screening purposes. [b2H b7E]

When this requirement was first put in place, some EU privacy advocates objected on the grounds that the requirement conflicted with European data privacy laws (AIR CARRIERS ARE ALSO REQUIRED TO SUBMIT A MUCH MORE LIMITED SET OF PASSENGER MANIFEST INFORMATION, SUCH AS NAME, BIRTHDATE AND PASSPORT NUMBER, UNDER SEPARATE ADVANCE PASSENGER INFORMATION RULES, WHICH ARE NOT AT ISSUE HERE)."

Sent from my BlackBerry Wireless Handheld

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

From: Baker, Stewart
To: Scardaville, Michael
CC: Isles, Adam; [b6] Rosenzweig, Paul
Sent: Thu Jun 01 11:54:11 2006
Subject: FW: EU accomplishments memo for POTUS

OK, I've edited this a second time. Mike, please look at my edits and ask me if you don't understand why I made them. I think this is ready.

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

From: Scardaville, Michael [mailto:[b2]]
Sent: Thursday, June 01, 2006 10:45 AM
To: Baker, Stewart; Scardaville, Michael; Isles, Adam
Cc: [b6] Rosenzweig, Paul
Subject: EU accomplishments memo for POTUS

Stewart,

Per your request, I've cleaned up this text a bit further and included it in the attached version of the POTUS memo. I also updated the introductory paragraph to reflect this

change. Please let me know if you'd like additional changes.

Thanks

Mike

[b2]

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

From: Baker, Stewart [mailto: E b2]
Sent: Thursday, June 01, 2006 5:30 AM
To: Scardaville, Michael
Cc: [b2]
Subject: RE: Can you review this and correct any errors?

Let's propose this, or something like it, for the memo to the President.

From: Scardaville, Michael [mailto: [b2]]
Sent: Wed 5/31/2006 9:08 PM
To: Baker, Stewart; Scardaville, Michael
Cc: [b6]
Subject: RE: Can you review this and correct any errors?

Stewart,

Some suggested correction's below. I've also attached this in word format so you can see my changes. You'll note that the agreement (technically the Undertakings, but the two are tied so saying agreement is probably fine) expires at the end of 2007, not the end of this year.

At the end of this year we are committed to reviewing the Undertakings during the course of its final year of its effectiveness. If we don't reach a mutually agreeable solution for continuing the Undertakings they expire after 3.5 years from the date of signature, which is November 18, 2007.

[b5]

[b5]

Mike

To protect against terrorists flying to the US, DHS requires that all airlines make information about their US-bound passengers available before the plane takes off. When this requirement was first put in place (prior to Mach 2003 participation was voluntary), EU privacy advocates objected, and the EU negotiated an agreement with DHS that put strict limits on how the data was used. [

b5]

On May 30 of this year, the European Court of Justice invalidated the agreement. In essence the Court said that the European Commission did not have authority to enter into the agreement. [b5] he Court said that the agreement concerned law enforcement and thus did not fall within the European Commission's usual powers. To avoid the disruption of air traffic, the Court held that its decision would not take effect until September 30.

[b5]

The risk is that failure to reach a new agreement could lead to a showdown in which European privacy agencies threaten to fine airlines for providing passenger data to the US, while the US threatens to fine (or deny landing rights) to airlines for not providing the data. [b5] and in any event the deadline for agreement is September 30, not June, and the deadline will likely spur a strong effort to negotiate a mutually acceptable agreement.

[b5] All sides have stressed that they want "the planes to keep flying and the data to keep flowing" while both sides review the impact of the decision.

Mike

[b2]

From: Baker, Stewart [mailto:[b2]]
Sent: Wednesday, May 31, 2006 8:31 PM
To: Scardaville, Michael
Cc: [b6]
Subject: Can you review this and correct any errors?

To protect against terrorists flying from Europe to the US, DHS requires that airlines in Europe provide information about their US-bound passengers before the plane is cleared to take off. When this requirement was first put in place, EU privacy advocates objected, and the EU negotiated an agreement with DHS that put strict limits on how the data was used. [b5]

On May 30 of this year, the European Court of Justice invalidated the agreement. In essence the Court said that the European Commission did not have authority to enter into the agreement. [b5] the Court said that the agreement concerned law enforcement and thus did not fall within the European Commission's usual powers. To avoid disruption, the Court held that its decision would not take effect until September 30.

[

b5

]

The risk is that failure to reach a new agreement could lead to a showdown in which European privacy agencies threaten to fine airlines for providing passenger data to the US, while the US threatens to fine (or deny landing rights) to airlines for not providing the data. [

and in any event the deadline for agreement is September 30, not June, and the deadline will likely spur a strong effort to negotiate a mutually acceptable agreement.]

[sides have stressed that they want "the planes to keep flying and the data to keep flowing" while both sides review the impact of the decision.] All