COUNCIL OF THE EUROPEAN UNION

Brussels, 15 April 2010

8506/10

JAI 295
USA 59
RELEX 302
DATAPROTECT 33

COVER NOTE

from:	Commission
to:	Delegations
Subject:	Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS)

Delegations find attached the Report of the first joint review of the implementation of the Agreement of 23 and 26 July 2007 between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), in accordance with paragraph 4 of that Agreement.

Encl.: 100406 PNR joint review report

Brussels, 7.4.2010

Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS)

8-9 February 2010

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Following the events of 11 September 2001, the United States enacted legislation requiring each air carrier operating passenger flights to and from the United States to transfer to the U.S. Customs and Border Protection ('CBP') personal data contained in the Passenger Name Record ('PNR') of air passengers. Following two previous agreements between the EU and the U.S. for the sharing of PNR data, the current agreement was signed in July 2007. It is currently provisionally applicable and has been submitted to the European Parliament for giving its consent to its conclusion.

The Agreement provides for a periodic review of the implementation of the agreement and the letter of the U.S. The first joint review of this agreement was carried out between 8 and 9 February 2010 in Washington. There were 4 parameters to the review:

– review the implementation of the agreement and the accompanying letter of the U.S.

– review U.S. and EU PNR policies and practices

– review any instances in which sensitive data was accessed

– The U.S. will reciprocally seek information about Member State PNR systems as part of this periodic review, and representatives of Member States maintaining PNR systems will be invited to participate in the discussions.

Another parameter of the review was to verify that the agreement actually serves its purpose and indeed contributes to the fight against terrorism and serious crime.

A methodology for the review exercise was developed between the EU and the U.S. teams under which the Commission had sent out a questionnaire to the Department of Homeland Security (DHS) in advance of the review. This questionnaire contained specific questions in relation to the commitments of the DHS to the EU as contained both in the agreement and the letter. DHS provided written replies to this questionnaire. During the review, the EU team was granted access to DHS premises and carried out field visits at its National Targeting Center and its Passenger Analytical Unit at Dulles Airport in Washington. The EU team was also given the opportunity to watch the databases being operated with the results shown and explained on screen by the targeters, while it was also given the opportunity to have some direct exchanges with DHS personnel responsible for the PNR program and targeters and analysts who have access to and use PNR data.

It is noted that in order to comply with the agreement and the letter, the U.S. published of a System of Records Notice (SORN) for its Automated Targeting System-Passengers (ATS-P) program on 3.8.2007. DHS adapted its policies, procedures and technologies in order to comply with the agreement.

As regards the question whether PNR serves the purpose of supporting the fight against terrorism and crime, the EU team has been satisfied that this is indeed the case. PNR provides DHS with the possibility of carrying out pre-departure assessments of all passengers which provide it with the opportunity of either taking steps to prevent a passenger from boarding an aircraft or giving DHS sufficient time to carry out all the background checks before the arrival of a passenger and prepare its response. It also provides DHS with the opportunity to perform risk assessments on the basis of scenario-based targeting rules in order to identify the 'unknown' potential high-risk individuals. PNR provides a unique feature of being able to make associations between passengers and identify criminals who belong in the same organised crime group. PNR is also successfully used for

identifying trends of how criminals tend to behave when they travel for example by understanding which routes they use.

Regarding the implementation of the agreement, the general finding is that DHS has made substantial efforts towards the full implementation of the agreement, and generally complies with the terms of the agreement.

The EU team is satisfied that DHS generally implements its commitments towards the EU. For example DHS uses effective filters for filtering out data without U.S. nexus as well as data outside the 19 categories described in the agreement. The masking and deletion of sensitive data are respected and DHS has never accessed sensitive data.

DHS also implements its commitments in relation to passenger rights, namely on providing appropriate information to passengers and implementing the right to access and redress without any exemptions.

Sharing of data with other agencies is handled very well by DHS. Sharing in most instances relates to specific investigations, is always carried out on a case-by-case basis and never in bulk. Sharing of data with third countries is also interpreted strictly.

Despite the overall satisfactory implementation of the agreement, in some areas improvement seems necessary and advisable. Some of these recommendations regard the better keeping of records by DHS of its activities, for example of its access to data, its ad hoc pulls, redress requests, as well as the more regular auditing and evaluation of its systems.

Namely, DHS should evaluate and assess the functioning of the Secure Flight Program in relation to the ATS-P program in order to avoid duplication of data. The Immigration Advisory Program and the Regional Carrier Liaison Group (RCLG) program should also be evaluated and audited as soon as possible. The standing of these programs needs to be explained and assessed, especially vis-à-vis the Secure Flight Program, notably in the light of the purpose limitation of the agreement and data protection.

It is recommended that the U.S. shares with the EU the results of the audit of the new override functionality for accessing PNR data processed in the EU as soon as it is carried out in April 2010 in order to ensure that DHS indeed only accesses data with a U.S. nexus. As regards the level of access to this functionality, it is recommended that such access is further limited to specially authorised senior personnel of DHS on a case-by-case basis. It is further recommended that the number of personnel that can initiate the ad hoc push/pull functionality through which DHS can obtain access to PNR data in addition to the 4 scheduled transmissions, be available to a limited number of specially authorised senior officials.

In addition, the newly introduced tracking categories for requests for access to data is only able to track requests under the general heading ‘travelers’ and it is unable to distinguish between requests for access to PNR data and requests for other data, or to track requests specifically relating to EU-originating PNR data. Further steps should be taken to fine-tune these tracking systems.

Finally, in some areas further monitoring should be required. There are some concerns as regards broad use of PNR data and in particular the matching of PNR against some databases that have immigration and customs policy elements to them; DHS is urged to ensure that all processing of PNR data respects the purpose limitation of the agreement. The EU team also has some concerns both as regards the number of ad hoc requests but also as regards the fact that DHS executes such

request by pulling the data. It is strongly recommended that DHS takes more steps to ensure that it works more intensely with carriers to ensure that they move as quickly as possible to a full and exclusive push method. Ad hoc requests should be substantially reduced, and it is recommended that DHS should reassess its way of using the ad hoc requests functionality and use the push rather than the pull method. Lastly, DHS is urged to respect its commitment to ensure reciprocity and pro-actively share analytical information flowing from PNR data with Member States and where appropriate with Europol and Eurojust.

It has been agreed that a follow up review be carried out in the course of 2011.

This paper consists of four Chapters. Chapter 2 provides an overview of the background to the review and the purpose and procedural aspects of the exercise. Chapter 3 presents the main findings of the review and the recommendations of the EU team to DHS. This Chapter is supplemented by Annex A which contains the detailed findings of the EU in relation to each Commitment. Finally, Chapter 4 presents the overall conclusions of the exercise. Annex B presents the composition of the EU and U.S. teams that carried out the review exercise.

The present report has received the unanimous agreement of the members of the EU team.

2. BACKGROUND AND PROCEDURAL ASPECTS OF THE JOINT REVIEW

Following the 11 September 2001 terrorist attack, the United States enacted a statute in November 2001 and regulations implementing this statute, requiring each air carrier operating passenger flights to and from the United States to transfer to the U.S. Customs and Border Protection ('CBP') personal data contained in the Passenger Name Record ('PNR') of air carriers. In June 2002 the Commission informed the U.S. authorities that these requirements could conflict with European and Member States' legislation on data protection which impose conditions on the transfer of personal data to third countries.

As a result, the EU and the U.S. entered into negotiations aimed at reaching agreement on sharing air passenger data while securing an adequate level of data protection. These negotiations led to the conclusion of an agreement in 2004 between the EC and the U.S. on the processing and transfer of PNR data by air carriers to the US Department of Homeland Security (DHS), CBP[1], which was based on and accompanied by an adequacy decision of the Commission[2]. This agreement foresaw its joint review by the two parties. Such joint review was carried out in 2005 and its report was issued on 12.12.2005 and was presented to the Council and the European Parliament. Following the judgment of the European Court of Justice in joined cases C-317/04 and C-318/04 on 30.5.2006, this agreement and adequacy decision were annulled as having been based on an incorrect legal basis[3]. This resulted in intense negotiations which led to the conclusion of an interim agreement, aimed at covering the intermediate period of one year until the conclusion of a long-term agreement with the U.S.[4]. This agreement was accompanied by a set of commitments from the US DHS as to how it would ensure an adequate level of data protection for PNR data[5].

1 OJ L 183/83, 20.5.2004
2 OJ L 235/11, 6.7.2004
3 European Court reports 2006 Page I-04635
4 OJ L 289/27, 27.10.2006
5 OJ C 259/1, 27.10.2006

The new long-term agreement between the EU and the U.S. was signed on 23 July 2007 by the U.S. and on 26 July 2007 by the EU, and was accompanied by a letter from the US to the EU which contained several commitments as to the way that the US will treat EU originating PNR data[6]. These instruments set out a series of conditions on the processing of PNR data by DHS, which ensure an adequate level of protection of the data by the U.S. authorities. Together, they form the legal framework for the transfer and processing of such passenger data by the DHS.

The Agreement provides for a periodical review of the implementation of the agreement and the letter of the US. The review provisions are contained in paragraph 4 of the agreement and paragraph X of the US letter[7].

Drawing from the contents of these paragraphs, there were 4 parameters to the review:

– review the implementation of the agreement and the accompanying letter

– review U.S. and EU PNR policies and practices

– review any instances in which sensitive data was accessed

– The U.S. will reciprocally seek information about Member State PNR systems as part of this periodic review, and representatives of Member States maintaining PNR systems will be invited to participate in the discussions.

Another parameter of the review was to verify that the agreement actually serves the purpose of contributes to the fight against terrorism and serious crime.

The first joint review was carried out in Washington on 8 and 9 February 2010 with the participation of teams on behalf of both parties. Under the terms of the review paragraphs of the agreement the EU would be represented by the Commissioner for Justice, Freedom and Security (JLS), and DHS would be represented by the Secretary of Homeland Security, or by such mutually acceptable official as each may agree to designate. The Commissioner for Justice, Freedom and Security delegated this task to Reinhard Priebe, Director in DG JLS, while the Secretary of Homeland Security delegated the task to Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, DHS. Both officials nominated teams to assist them in their tasks. A full list of the members of both teams appears in Annex B. It is noted that the EU team had appointed 2 experts to assist it in its tasks, namely a data protection expert and a law enforcement expert.

---

6 OJ L 204/16, 4.8.2007

7 "(4) DHS and the EU, will periodically review the implementation of this Agreement, the DHS letter, and U.S. and EU PNR policies and practices with a view to mutually assuring the effective operation and privacy protection of their systems" and "X. DHS and the EU will periodically review the implementation of the agreement, this letter, U.S. and EU PNR policies and practices and any instances in which sensitive data was accessed, for the purpose of contributing to the effective operation and privacy protection of our practices for processing PNR. In the review, the EU will be represented by the Commissioner for Justice, Freedom and Security, and DHS will be represented by the Secretary of Homeland Security, or by such mutually acceptable official as each may agree to designate. The EU and DHS will mutually determine the detailed modalities of the reviews. The U.S. will reciprocally seek information about Member State PNR systems as part of this periodic review, and representatives of Member States maintaining PNR systems will be invited to participate in the discussions."

The methodology which was developed and followed for the review exercise was the following:

– The EU team was composed of 5 Commission officials and 2 external experts. A representative of the UK, that is the only Member State having a fully operational PNR system, also participated in the discussions in compliance with the provisions of the review paragraphs of the agreement and letter.

– The Commission had sent out a questionnaire to DHS in advance of the review. This questionnaire contained specific questions in relation to all the commitments of DHS to the EU as contained both in the agreement and the letter. DHS provided written replies to the questionnaire.

– The EU team was granted access to DHS premises and carried out field visits at its National Targeting Center and its Passenger Analytical Unit at Dulles Airport in Washington.

– The EU team was given the opportunity to watch the databases being operated with the results shown and explained on screen by the targeters, while respecting the U.S. confidentiality requirements. For security reasons, only the law enforcement expert had the opportunity to watch the databases being operated in real time, who then reported his findings to the rest of the EU team.

– The EU team had the opportunity to have direct exchanges with DHS personnel responsible for the PNR program and targeters and analysts who use and have access to PNR data.

– The replies to the questionnaire were discussed in detail with DHS. The EU team also had the opportunity and the time to pose further questions to DHS officials and address all the various parameters of the agreement and a full day meeting was dedicated for this purpose

– At the request of DHS, all members of the EU team signed non-disclosure agreements as a condition for their participation in the review exercise.

– DHS had the opportunity to ask questions to the EU team, as well as to the UK representative about the status quo of the EU PNR proposal and the UK e-borders program.

– In preparation of the review exercise, on 18.12.2008 DHS prepared its own Report Concerning Passenger Name Record Information Derived from Flights Between the U.S. and the European Union[8]. This Report was updated on 5.2.2010[9].

– For the preparation of this report, the EU team used information contained in the written replies that DHS provided to the EU questionnaire, information obtained from its discussions with DHS personnel, information contained in the aforementioned DHS report and update, as well as information contained in other publicly available DHS documents.

---

8 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf

9 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_review2010update_2010-02-05.pdf

Due to the sensitive nature of the PNR program, there were limitations on the provision of some internal operational documents. Other information was provided to the EU team with the condition that it would be treated as classified up to the level of EU Restricted. The present report should be read in the light of these limitations, as well as in the light of the fact that all members of the EU team had to sign non-disclosure agreements exposing them to criminal and/or civil sanctions for breaches.

In spite of such limitations, before, during, and after the review there has been an intense exchange of views in an open and constructive spirit which covered all the questions of the EU team. DHS provided all the information that was required by the EU team and replied to all questions. In case where DHS was not able to immediately provide information or documentation it promised to do so after the review exercise.

The Commission acknowledges the professional and constructive assistance that it received from the data protection and law enforcement experts who participated in the EU team.

Finally, it should be noted that the procedure for the issuance of this report was agreed with the US team. Namely, the EU team prepared a draft report. The draft was sent to DHS. DHS had the opportunity to comment on inaccuracies and on information that could not be disclosed to public audiences. To the extent that the EU disagreed with the comments of DHS, DHS sent a letter to the EU which addresses these disagreements. The EU will present the letter, together with this report when it is presenting the issue to the relevant stakeholders. It is clarified that this is the report of the EU team as delegated by the Commissioner for Justice, Freedom and Security and is not a joint report of the EU and U.S. teams.

3. THE OUTCOME OF THE JOINT REVIEW

This Chapter aims to provide the main findings resulting from the review of the EU team. The questionnaire of the EU and the replies of DHS, together with other information that was provided orally by DHS during the review and the detailed findings of the EU team appear in Annex A.

It is noted that in order to comply with the agreement and the letter, the U.S. incorporated their terms into the published System of Records Notice (SORN) for its ATS-P program on 3.8.2007. DHS had to adapt some policies, procedures and technologies in order to comply with the agreement.

As regards the question whether PNR indeed serves the purpose of supporting the fight against terrorism and crime, the EU team has been satisfied that this is indeed the case. PNR provides DHS with the possibility of carrying out pre-departure assessments of all passengers which provide it with the opportunity of either taking steps to prevent a passenger from boarding an aircraft or giving DHS sufficient time to carry out all the background checks before the arrival of a passenger and prepare its response. It also provides DHS with the opportunity to perform risk assessments on the basis of scenario-based targeting rules in order to identify the 'unknown' potential high-risk individuals. PNR provides a unique feature of being able to make associations between passengers and identify serious criminals and their associates. PNR is also successfully used for obtaining intelligence on travel patterns, for example by understanding which routes criminals use.

As regards the agreement, the general finding is that DHS has made substantial efforts towards the implementation of the agreement. The EU team finds that DHS generally complies with the terms of the agreement.

The main findings of the EU team are divided into positive findings, i.e. where DHS fully implements its commitments, recommendations for improvement, i.e. where there is substantial compliance but the EU team recommends some further improvement, and areas to be further monitored/areas of strong recommendations, where the EU team finds that DHS should make more efforts to implement its commitments.

3.1. Positive findings

The EU team found that DHS fully implements several of its commitments under the agreement, namely:

- The method used for processing PNR data follows a logical approach and maximises the added value of using such data for terrorism and related crime and other serious transnational crime purposes.

- DHS has used the two exceptions to the main purposes of the agreement, i.e. protecting the vital interests of the data subject and use in criminal proceedings, in a strict manner.

- DHS filters out flights which are not covered by the agreement using flight numbers and airport codes, in compliance with its commitments.

- DHS filters out PNR data elements that it receives which are outside the 19 data elements listed in the agreement. DHS applies filters and masks sensitive data which is then permanently deleted after 30 days. The level of access to such data during the 30-day period is limited. The filtering mechanisms respect the agreement.

- DHS has indicated that it had never accessed sensitive data until the date of the joint review, even though the agreement provides it with the possibility to do so.

- DHS makes substantial efforts for the implementation of the push system internationally through the IATA working party on common PNR standards.

- DHS has never used the possibility of requesting data earlier than 72 hours before the scheduled flight departure.

- The sharing of PNR data with other U.S. agencies and governmental authorities in third countries is handled well, it is limited and it is audited, in compliance with the agreement.

- DHS achieved important progress in handling requests for access and redress by passengers and implements its commitment to the EU.

- DHS has now added an updated FAQ's and a current Privacy Policy to its existing notice to passengers on its website, These, together with information already provided on its website, through SORN publications and through notice to passengers via the carriers, are in compliance with the agreement.

3.2. Recommendations for improvement

During the review, the EU team identified some areas where, even though DHS generally implements these commitments, some improvements would be recommended. Such areas are:

- Despite the fact that the actual processing of data for the purposes of the Secure Flight Program is consistent with the purposes of the agreement, it is recommended that DHS evaluate and make an assessment of the functioning of the Secure Flight Passenger Database and the ATS-P database which is the database where PNR is kept for the purposes of the agreement in order to avoid the retention of data in two different databases.

- Again as regards the purpose limitation of the agreement, the Regional Carriers Liaison Groups program which is used to advise carriers to deny boarding to some identified persons may be a cause for concern. Even though the EU team appreciates that the more proactive use of this program is very new, it recommends that this program be audited as soon as possible. The standing of this program needs to be explained and assessed, especially vis-à-vis the Secure Flight Program, since this raises concerns regarding the respect of the purpose limitation of the agreement and data protection.

- Even though DHS achieved progress in increasing the number of air carriers that have implemented the necessary technological solution that permits them to push, more needs to be done to ensure that all carriers use the push method.

- Even though the initial filter functionality which filters out flights and PNR with no US nexus works well, the override functionality which is operative since October 2009 provides wide possibilities for accessing PNR data of passengers in a pull method that have no U.S. nexus. DHS was not able to confirm the actual use of this functionality, as this functionality had not yet been audited by DHS. It is recommended that DHS shares with the EU the results of the bi-annual audit of this functionality which is scheduled for April 2010. As regards the level of access to this functionality, even though access is already limited, it is recommended that such access be further limited and only available to a limited number of specially authorised senior officials of DHS on a case-by-case basis.

- Even though DHS achieved progress in reducing its backlog regarding requests for access and redress by passengers, it is noted that the newly introduced tracking system for such requests is not ideal. It is only able to track requests under the general heading 'travellers' and it is unable to distinguish between requests for access to PNR data and requests for other data, and it also unable to track requests specifically relating to EU-originating PNR data. Further steps should be taken in order to fine-tune the tracking systems.

- Given that the notion of sensitive data might change over time it is recommended to update the list of sensitive data that DHS uses for filtering such data. Such an update should be made in consultation with the European Commission as outlined in no. III of the DHS letter.

- Finally, as regards the transmission of the data, the EU team recommends that the ad hoc requests functionality is only available to a limited number of specially authorised senior officials of DHS.

3.3. Areas to be particularly monitored/areas of strong recommendations

The EU team has identified some areas where particular monitoring would be required.

- There are some concerns as regards the broad use of PNR data and in particular the matching of PNR against databases that have immigration and customs policy elements to them. The EU team is aware of the fact that these purposes also come under the responsibilities of DHS. However, all processing of PNR by DHS needs to respect the purpose limitation of the agreement. In this context also the notion of serious transnational crime needs further clarification.

- DHS should make more efforts to ensure that all carriers use the push method.

- The EU team also has concerns both as regards the amount of ad hoc requests but also the fact that DHS executes such request by pulling the data. The EU team recommends that the ad hoc requests should be substantially reduced in number, as it raises some concerns whether DHS exercises this right judiciously and proportionately. Furthermore, it is regretted that the negotiations with air carriers for finding an acceptable ad hoc push functionality failed and recommends that DHS work expeditiously towards finding an acceptable way of implementing ad hoc push. The EU team strongly recommends that DHS reassess its way of using the ad hoc requests functionality.

- Finally, the EU urges DHS to respect its commitment to pro-actively share analytical information flowing from PNR data with EU Member States and where appropriate with Europol and Eurojust. Such information would be highly valuable to the police and judicial authorities of the Member States and the two agencies. It is noted the U.S. and the EU have identified improving this sharing of information as a priority under the January 21, 2010 Toledo Declaration on Aviation Security.

4. CONCLUSIONS

The EU team finds that the review mechanism is a valuable tool for the assessment of the level of compliance of DHS with the agreement. It enabled the EU team to witness how the data is used in practice and to have some direct exchanges with targeters, analysts and other officials who use PNR data.

The EU team reiterates its acknowledgement of the good cooperation on the part of all the DHS personnel during the review and for the open way in which all the questions of the EU team have been replied.

Satisfactory information was provided to prove that PNR actually serves the purpose of supporting the fight against terrorism and serious crime.

The EU team also finds that DHS generally implements the agreement. The majority of commitments are implemented according to the provisions of the agreement and that DHS respects its obligations as regards the rights of passengers. It is especially important to note that the U.S. has transposed its commitments towards the EU into domestic rules through the publication of a System of Records Notice in the Federal Register.

While it is acknowledged that the implementation of some commitments is technically and operationally challenging, especially as regards the implementation of the push method, DHS is encouraged to intensify its efforts to ensure that all carriers use the push method and continue to actively working in international fora for an overall resolution of this issue.

A number of recommendations are made to DHS which appear in Chapter 3 above. DHS took note of these recommendations.

The areas of most concern relate to the use of PNR data for immigration and customs purposes, the large numbers and method of implementing the ad hoc requests and the non-proactive implementation of the reciprocity and co-operation commitment by sharing analytical information flowing from PNR data with Members States, Europol and Eurojust.

It is has been agreed that a follow up review be carried out in the course of 2011 to further monitor these matters.

ANNEX A
DETAILED FINDINGS OF THE REVIEW

A.PURPOSE LIMITATION/SCOPE

A.1. The relevant Commitment of the U.S.

The purpose limitation/scope of the use of PNR data by DHS is expressed in paragraph I of the letter accompanying the agreement. It states that:

'I. DHS uses EU PNR strictly 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) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law. DHS will advise the EU regarding the passage of any U.S. legislation which materially affects the statements made in this letter.'

A.2. The relevant written reply of DHS

Question: *Have PNR data ever been used by DHS also in cases where necessary for the protection of vital interests of the data subject or other persons, or in any criminal judicial proceedings or as otherwise required by law (the other two purposes)?*

Response:

DHS has used PNR to protect the vital interests of the data subject and other persons; DHS has used PNR in one criminal judicial proceeding. More specific information will be provided during the PNR Joint Review. [*such details have indeed been given during the joint review]*

Question: *Does DHS cross-reference PNR data with data received under the Electronic System for Travel Authorisation (ESTA) scheme or biometric data DHS receives from arriving or departing passengers? In that case, which retention period applies?*

Response: Yes. DHS cross-references PNR data with ESTA data, Advanced Passenger Information System (APIS), I-94, TECS Enforcement records, National Crime Information Center (NCIC) wants and warrants, and other relevant information using the ATS-P. All of this cross referencing is disclosed in the public Privacy Impact Assessments (PIAs) and system of records notice (SORNs) related to these systems. PNR is retained pursuant to the ATS SORN, which contains the same retention period as the 2007 U.S.-EU PNR Agreement. For additional information see the PIAs published in 2008 and 2007 on the DHS web site.

ATS-P uses this information to conduct risk-based targeting and provide assessments. Each data set used by ATS-P to conduct the risk-based targeting and assessments follows the retention schedule and privacy rules set forth in the applicable PIAs and SORN. Thus, ESTA data are maintained in a separate system and follows the rules described in the privacy documentation that CBP and the DHS Privacy Office have released to the public. If standards or processes change, the PIA and/or SORN will change.

A.3. Other relevant information

When DHS receives the data from the carriers, it immediately filters and deletes PNR categories outside the 19 categories listed in the agreement. On the 19 PNR categories, DHS applies a separate filter aimed at masking sensitive data. The processed 19 categories with the masked data elements are then transferred and retained in a database called ATS-P which is the relevant database under the agreement and which is handled by the Customs and Border Protection (CBP) component of DHS.

DHS informed that 3 PNR elements, i.e. name, date of birth and gender are copied and sent to the Secure Flight Passenger Data database. The Secure Flight database is administered by the Transportation Security Administration, which is a component of DHS. It is a counter-terrorism program aimed specifically at safeguarding aviation security through the application of no-fly and selectee lists. The data is kept in this database for 7 days from the completion of the identified travel itinerary and subsequently erased. It is noted that a final decision to implement a refusal to board order to a carrier is only done once the PNR has been cross checked against API data in order to verify the identity of the person. The added value of using PNR in this case is that PNR is available much earlier (up to 72 hours) than API data which gives DHS advance notice and time to prepare.

The PNR that is kept in the ATS-P database is used by CBP for the purposes of the agreement. The data is used preliminarily in 2 automated ways: (i) it is cross-checked against several law enforcement databases in order to establish whether there is a match, and (ii) it is run against scenario-based targeting rules to identify persons that could pose a risk to security but who were previously 'unknown' to DHS. Following this automated processing, officers at the National Targeting Center-Passenger (NTC-P) process the data of the passengers who have been identified as a result of the automated processing in order to carry out additional checks on them. This process leads to either the clearing of the identification or to the confirmation of the identification. Additional manual checks are carried out as regards such identified persons in order to establish whether they seem to have any associates travelling with them.

Persons that have been identified following the result of this manual processing are marked for the border guards' attention. The border guard who receives such person at the border is tasked with making his own assessment whether this person should be denied entry into the US, sent to secondary screening, arrested or cleared.

All the data that is kept in the ATS-P (both the identified and the non-identified persons) are then assessed by analysts of CBP for the purpose of identifying of criminal and terrorist travel behaviour. On the basis of such trend analysis, the analysts develop scenario-based targeting rules. Such rules are fed into the system and future incoming passengers' PNR data is automatically checked against such rules. DHS analysts noted that such scenario-based targeting rules are developed, amended and updated very often and sometimes on a daily basis.

As regards the cross-checking of PNR against law enforcement databases in order to establish matches, ATS-P is screened against the following:

– API/Manifest data, in order to establish the official identity of a person based on the passport information;

– Border crossing information which basically comprises the entry/exit record held by DHS;

– The I-94 forms that passengers fill in when arriving in the US

– TECS enforcement data which comprises of various criminal watchlists and other criminal databases of DHS, i.e. missing persons, persons against who a warrant is pending. These databases only contain information of persons involved or suspected to be involved in felonies, which are criminal offences which carry a minimum of one year imprisonment;

– The Terrorist Screening Database (TSDB);

– National Crime Information Center (FBI) databases;

– Lost and stolen passports national and Interpol databases;

– ESTA denial and prior refusal records held by DHS; and

– Visa refusal databases of the Department of State including the Consular Lookout and Support System (CLASS) database which is a consular/visa database.

It is noted that DHS confirmed that PNR data is not matched against the Terrorist Identities Datamart Environment (TIDE) database, which is a classified system that includes, to the extent permitted by law, all information the U.S. government possess related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism.

As regards the matching of PNR data against scenario-based targeting rules, these are focused on terrorism and people, drugs and currency smuggling. DHS confirmed that the targeting process does not lead to a score in the ATS-P system, but merely to a positive match indication.

DHS noted that PNR data is uses in the above manner in accordance with the agreement, i.e. the fight against terrorism and related crimes, other transnational serious crime, including organised crime and flights from warrants or custody from such crimes.

DHS noted that it used PNR data within the exceptions to the main purposes of the agreement on very rare occasions. Even though it has used PNR data to protect the vital interests of persons on 4 occasions in relation to communicable diseases, none was based on EU-originating PNR data. Further, it used EU PNR data in one criminal judicial proceeding.

In addition, DHS implements since 2004 an Immigration Advisory Program (IAP). This program is intended to increase the number of people who are prevented from boarding an aircraft to the US, rather than permitting people to board but then deny them entry into the U.S. upon their arrival. This program concerns people who are not already in the no-fly database which is used under the Secure Flight Program.

Under this program, when PNR is matched against law enforcement databases and leads to an identification (which is confirmed by API data), then DHS will try to prevent this person from boarding the aircraft. This is achieved through currently 9 liaison officers of the U.S. at UK, Dutch, German, Spanish, Polish and 2 non-Member States' airports. Those liaison officers will evaluate the

person on the spot through further questions and assessment and, where appropriate, contact the airline for coordination. Eventually, the liaison officer will inform the carrier that this person will be denied entry into the US upon arrival. On this basis, he will advise the carrier not to carry this passenger on the aircraft. It is usually in the carrier's interest to follow such advice; otherwise the carrier would have to bear the costs of returning this person when entry is actually denied to the U.S..

In addition, since January 2010 DHS implemented a more proactive use of a program which is called Regional Carrier Liaison Groups (RCLG) program. This program is basically an extension of the Immigration Advisory Program to locations where the U.S. does not have liaison officers at airports. Under this program, which works otherwise in the same way as the Immigration Advisory Program, the National Targeting Centre (NTC) makes direct contact with the carrier and advises it not to carry the specific passenger, rather than having a liaison officer making contact with the carrier.

DHS confirmed that the IAP and the RCLG are not applied to matches resulting from the application of scenario-based targeting rules, but only to matches against the above mentioned law enforcement databases.

A.4. Comments

As regards the Secure Flight Program, the EU team had not been aware that some PNR elements that are sent under the agreement are copied into this separate database. The EU team acknowledges the fact that this is a DHS program whose purpose is the fight against terrorism, but nevertheless has some concerns about the duplication of the data. It is recommended that DHS evaluates the way that this issue is organised in an effort to avoid the duplication of data in different databases, for example by running the no-fly and selectee lists against ATS-P during the initial automated phase.

The method used for processing data is consistent with the use of PNR data by other countries that have PNR systems, it follows a logical approach and maximises the added value of using such data for law enforcement purposes. The US has used the two exceptions to the main purposes of the agreement in a very strict manner.

The processing done on the basis of scenario-based targeting rules is consistent with the main purposes of the agreement. However, as regards the matching of PNR against law enforcement databases, the EU team has some concerns. Namely, the matching of PNR against ESTA denial and prior refusal records and visa refusal databases seem to have some immigration purposes to them. Even though ESTA and visa denials could be based on counter-terrorism and transnational serious crime reasons, they are also done for purely immigration policy related purposes. Further, the matching of PNR against border crossing information seems to be primarily focused on identifying visa overstayers. The EU team considers that this purpose was not intended to be covered by the agreement since it is an immigration based criminal offence which very possibly does not have a transnational element to it, since the overstaying takes place in the U.S. It is strongly recommended that DHS review these practices and use PNR data only for the purposes defined in the agreement. In this context also the notion of crimes that are transnational in nature should bee revised. Not every criminal crossing the US border has committed a serious transnational crime.

Finally, the Immigration Advisory Program and the Regional Carrier Liaison Group may be a cause for concern. DHS was not able to provide us with sufficient information on this, i.e. how often it is

used, whether it is used in all confirmed matches against a database or under stricter conditions, whether they received any complaints from passengers or carriers. It was not clear how this program fits in with the Secure Flight Program and its no-fly lists. In the absence of this crucial information the EU team is not able to draw conclusions on the compliance of this program with the agreement. It is strongly recommended that this program be evaluated and audited as soon as possible. The standing of this program needs to be explained and assessed, especially as regards the purpose limitation of the agreement and data protection.

B.GEOGRAPHICAL SCOPE

B.1. The relevant Commitment of the U.S.

The geographical scope of the agreement is expressed in paragraph 1 of the agreement, which states that:

'1. On the basis of the assurances in DHS's letter explaining its safeguarding of PNR (the DHS letter), the European Union will ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America will make available PNR data contained in their reservation systems as required by DHS.'

B.2. The relevant written reply of DHS

Question: *What mechanisms ensure that pulled information regards solely to flights with a U.S. nexus?*

Response: U.S. Department of Homeland Security, U.S. Customs and Border Protection (CBP) collects PNR data as authorized by legal statute (49 U.S.C. § 44909(c) (3)) and its implementing (interim) regulation for flights to and from the U.S. The CBP system uses flight numbers and airport codes to identify flight numbers with a U.S. nexus. Then, the system takes the PNR for those flight numbers and rescreens them using airport codes to identify only those PNR that actually have a U.S. nexus. This process allows the system to filter out those PNR for earlier segments of a flight where the traveller's journey ends before arrival at a U.S. airport. (e.g., Flight #101 has the routing Mumbai – Manchester – JFK. The system looks for PNR on Flight #101 due to the JFK segment, and then filters out the PNRs of travellers who only fly on the Mumbai-Manchester segment).

There is now an override mechanism in the IT system so that DHS may pull PNR that does not have a U.S. airport code. In order for the override mechanism to be used, the CBP officer must have the authority to access the override capability to view the particular flight and affirmatively acknowledge his access. The affirmative acknowledgement reminds the user that he may only access PNR that has a nexus to the U.S. This override function is a new functionality since the previous PNR report and was implemented to address specific cases where the U.S. airport is not recorded in the PNR, but the plane stops at a U.S. airport. Examples: flights from Australia to Canada, where the flight stops in Hawaii to refuel, but the Hawaiian airport code is not in the PNR; or a flight from Paris to Tahiti that stops in Los Angeles airport for refuelling. This functionality may also be used if a flight is diverted because of weather or other reasons and must land unexpectedly in U.S. DHS is reviewing how the new functionality will be implemented; only a limited number of CBP officers have and will continue to have system permissions to use this tool. This new override functionality is reviewed by Office of Information Technology (OIT) in the same way general access to PNR is reviewed by OIT.

In addition to the technical mechanisms in place to ensure compliance with the 2007 U.S. - EU

PNR Agreement, on December 20, 2004, CBP issued 2 field guidance papers specific to PNR of flights between European Union countries and the United States. This guidance was renewed with a memorandum to the field on August 13, 2007, to reflect the System of Records Notice (SORN) for the Automated Targeting System (ATS) published on August 3, 2007, and the 2007 Agreement between the United States and the European Union, the July 23, 2007, Letter from EU Council President Luis Amado to Secretary Michael Chertoff, and the July 26, 2007 Letter from Secretary Michael Chertoff to EU Council President Luis Amado (all three referred to hereinafter as the "2007 U.S. - EU PNR Agreement"). This 2007 memorandum reiterated that all EU PNR data elements must be used in accordance with the 2007 U.S.-EU Agreement and the CBP field guidance, which was consistent with the terms of the requirements of the SORN, the 2007 U.S. – EU PNR Agreement. More recently, CBP developed a CBP Directive on use of PNR, in order to provide a consolidated formal framework for the appropriate use, handling and disclosure of PNR stored in ATS-P and to clearly set forth the policy concerning access to PNR. This Directive was signed on March 7, 2010.

All CBP officers with access to PNR data are required to review and sign an acknowledgment of the field guidance; the same process will be applicable once the CBP Directive takes the place of the Field Guidance. This acknowledgement is logged in the training system so that it may be regularly reviewed by Headquarters staff to ensure that the field staff is properly trained on the use and disclosure of the data. The August 13, 2007, CBP Memorandum and successor CBP Directive also clearly identify which PNR data categories are allowed to be used and for which purposes. In interviews with the Passenger Analytic Units (PAUs) at both Washington Dulles and Baltimore Washington International Airports conducted for the 2008 PNR review, the personnel at the PAUs had the field guidance on hand and were well-versed in the appropriate uses of the information as demonstrated through the interview process.

The Privacy Office reviewed the extensive materials used for training both PAU and NTC analysts on how to appropriately handle and share PNR data, all of which were consistent with the ATS SORN and the 2007 U.S.-EU PNR Agreement and accompanying Letter.

The Privacy Office confirmed that these policies and related practices were in place during the 2008 review by interviewing NTC, PAU analysts, and CBP management. These policies and practices remain in place today, but the only change between the 2008 review and now is that the PNR is filtered by U.S. airport code instead of flight number. Additionally, PRIV reviewed the training logs to ensure that individuals with access to PNR have been properly trained.

B.3. Other relevant information

The agreement applies to flights to and from the EU to and from the U.S. DHS has a filtering mechanism called RESMON which filters out flights which are not covered by the agreement using flight numbers and airport codes. This is especially relevant in connecting/transit/transfer flights. For example, when a flight originates from a third country 'X' to a Member State and continues onward to the U.S., this would be not be filtered out by the flight number filter because the flight number for the whole flight is relevant to the US. However, RESMON would then apply an airport code filter within such a flight and identify the passengers that are actually flying to the U.S. It would then delete the PNR of passengers that have only taken the part of the flight from the third country to the Member State but have not continued onwards to the U.S.

However, since October 2009 DHS has added an override mechanism to the above filtering mechanism. This means in effect that, even though RESMON filters out certain flights and the PNR

data of passengers not covered by the agreement, DHS has the possibility of reversing this function and accessing PNR data that has been originally actually filtered out.

The justification that DHS has given for establishing this function is that sometimes, even though a flight has no U.S. nexus, it physically lands in its territory. The examples given were where the airplane lands in U.S. territory for refuelling, or when a flight with another destination is diverted and lands in US territory due to weather conditions or other security reasons. In addition, DHS uses the override mechanism in cases of an offloaded passenger who DHS determined to be inadmissible prior to boarding through its Immigration Advisory Program (IAP) or liaison officers. In such cases, even though the passenger has not boarded the air craft towards the U.S., DHS stated that it may use the override functionality in order to identify possible co-travellers or to conduct analysis of the offloaded passengers whose intended destination was the U.S.

In all cases where the override mechanism is used, access to the data can only be achieved through pulling and the push facility is not available in such cases.

According to DHS since this functionality was established in October 2009, it has been used to access 2500 individual PNRs for 198 flights. This number refers to all flights to the US and not only those covered under the agreement.

DHS noted that the access to the override mechanism is given to a limited number of senior personnel of CBP. Access to such mechanism does not seem to be limited depending on the seniority of personnel, i.e. access need not be authorised by senior personnel. On the basis of discussions held between the law enforcement representative of the EU team and DHS personnel at the National Targeting Center - Passenger (NTC-P) it would appear that at least all personnel of the NTC-P has such access.

Access to the override functionality is tracked (logged) and can be reviewed by Office of Information and Technology (OIT). The functionality will be reviewed bi-annually and the first review is scheduled for April 2010.

B.4. Comments

The initial filter functionality which is carried out through the RESMON program is satisfactory and complies with the agreement.

However, the new override functionality is a potential source of concern. To the extent that this functionality is used for the purposes given, i.e. cases where a flight with no US nexus actually lands to the territory of the U.S., then access to PNR data of passengers on such flights would be covered by the agreement. However, the use of this functionality by DHS for offloaded passengers raises some concerns, as this would concern passengers who have not actually flown to the U.S. Unfortunately DHS was able to provide only limited data on the cases where this functionality was actually used, as it had not yet audited this functionality. It is recommended that DHS shares with the EU the results of the audit of this functionality which is scheduled to be carried out in April 2010. As this override function is an exclusive pull mechanism further clarification as to its compatibility with the agreed push method seems necessary.

As regards the level of access to this functionality, since this functionality could be intrusive as its possibilities are very wide, it is recommended that such access is limited to a defined number of senior personnel of DHS. The targeters that are working at the NTC should require the permission

of a limited number of senior officials in order to use this functionality and only on a case-by-case basis.

C. TYPES OF INFORMATION COLLECTED AND USE OF SENSITIVE DATA

C.1. The relevant Commitment of the U.S.

The definition of the types of information that DHS can collect, as well as its use of sensitive data is expressed in paragraph III of the letter accompanying the agreement, which states that:

'III. Most data elements contained in PNR data can be obtained by DHS upon examining an individual's airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically significantly enhances DHS's ability to focus its resources on high risk concerns, thereby facilitating and safeguarding bona fide travel.

Types of EU PNR Collected:

1. PNR record locator code

2. Date of reservation/issue of ticket

3. Date(s) of intended travel

4. Name(s)

5. Available frequent flier and benefit information (i.e. free tickets, upgrades, etc.)

6. Other names on PNR, including number of travelers on PNR

7. All available contact information (including originator information)

8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)

9. Travel itinerary for specific PNR

10. Travel agency/travel agent

11. Code share information

12. Split/divided information

13. Travel status of passenger (including confirmations and check-in status)

14. Ticketing information, including ticket number, one-way tickets and Automated Ticket Fare Quote

15. All baggage information

16. Seat information, including seat number

17. General remarks including OSI, SSI and SSR information

18. Any collected APIS information

19. All historical changes to the PNR listed in numbers 1 to 18

To the extent that sensitive EU PNR data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual), as specified by the PNR codes and terms which DHS has identified in consultation with the European Commission, are included in the above types of EU PNR data, DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information. Unless the data is accessed for an exceptional case, as described in the next paragraph, DHS promptly deletes the sensitive EU PNR data.

If necessary, in an exceptional case where the life of a data subject or of others could be imperilled or seriously impaired, DHS officials may require and use information in EU PNR other than those listed above, including sensitive data. In that event, DHS will maintain a log of access to any sensitive data in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law. DHS will provide notice normally within 48 hours to the European Commission (DG JLS) that such data, including sensitive data, has been accessed.'

C.2. The relevant written reply of DHS

Question: *Has DHS become aware of any additional type of PNR information that may be available and required for the purposes set out in Article I?*

Response: As of this time, DHS is not seeking to add to the categories of PNR that it is currently permitted to collect.

Question: *Has DHS become aware of any type of PNR information that is no longer required for the same purposes and if so, which?*

Response: No. In the most recent review of data categories that was conducted after the December 25, 2009 incident, CBP determined that all data in the categories it currently receives are used regularly and provide information necessary for conducting the passenger risk assessments based on threats.

Question: *Has DHS ever used information held in EU PNR other than those types of information listed in the DHS letter, including sensitive information, as set out in Article III, last paragraph?*

Response: Since the effective date of the 2007 U.S. - EU PNR Agreement, DHS has only used EU PNR data from the categories listed in the 2007 U.S. - EU PNR Agreement and the ATS SORN and has not requested sensitive information from the airlines. Sensitive information is filtered out of all PNR prior to it entering the ATS-P system. In conducting interviews with the Privacy Act/Freedom of Information Act staff at CBP in 2010, the DHS Privacy Office found physical evidence of the privacy filters working.

C.3. Other relevant information

When PNR data is received by DHS either through push or pull, an automated filtering mechanism within the RESMON (reservations monitor) function of ATS-P is applied to it. This filtering mechanism filters out and immediately deletes the categories of data that are not covered by the agreement. Then, on the data that is in fact covered by the agreement, another filtering is applied which masks out any sensitive data. This filtering takes place on the basis of codes that represent sensitive information in PNR. The masking out process means that the sensitive information remains in the system but no one can actually see it. The masked out data are retained in the database for 30 days and then it is automatically deleted from the database.

For the period during which the masked out sensitive data are retained in the database, access and unmasking are permitted only for high-ranking senior officials of DHS. The masking mechanism and the access are auditable and have actually been audited by the DHS Privacy Office. The audit confirmed that the masking mechanism works well in practice and that access to sensitive data has not been effected by anyone.

C.4. Comments

The Commitments of this paragraph seem to be fully respected and implemented. It seems, however, advisable to revise the list of sensitive data on a regular basis as terms and the notion of sensitive data might change over time.

D. DATA RETENTION

D.1. The relevant Commitment of the U.S.

The periods of data retention is expressed in paragraph IV of the letter accompanying the agreement, which states that:

'IV. DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status. Data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. We expect that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions. Data that is related to a specific case or investigation may be retained in an active database until the case or investigation is archived. It is DHS' intention to review the effect of these retention rules on operations and investigations based on its experience over the next seven years. DHS will discuss the results of this review with the EU.

The above mentioned retention periods also apply to EU PNR data collected on the basis of the Agreements between the EU and the U.S., of May 28, 2004 and October 19, 2006.'

D.2. The relevant written reply of DHS

The EU team has not posed any written questions to DHS as regards this commitment. DHS was,

however, invited to provide additional information on how it makes sure that the retention period for PNR is respected even in cases where they have been transferred to other national or foreign agencies.

D.3. Other relevant information

This commitment will only become relevant at the moment when the primary seven-year period as from the date of the first 2004 agreement starts expiring, i.e. on 27 July 2011. However, DHS mentioned that it had been necessary to access older PNR data on rare occasions. In case of sharing of PNR data with a law enforcement agency it is because the record meets the requirements for sharing, and the record for that particular PNR follows the retention schedule of the receiving agency under the law enforcement description in their applicable SORN. Where data is shared with a law enforcement agency for the purposes of an investigation, the data is retained by that agency for the period of the investigation.

D.4. Comments

The implementation of this commitment will only become relevant as from 27 July 2011.

E. TRANSMISSION OF PNR

E.1. The relevant Commitment of the U.S.

The method and timing of transmissions is expressed in paragraph 2 of the agreement as supplemented by paragraph VIII of the letter accompanying the agreement, which state that:

'2. DHS will immediately transition to a push system for the transmission of data by such air carriers no later than 1 January 2008 for all such air carriers that have implemented such a system that complies with DHS's technical requirements. For those air carriers that do not implement such a system, the current systems shall remain in effect until the carriers have implemented a system that complies with DHS's technical requirements. Accordingly, DHS will electronically access the PNR from air carriers' reservation systems located within the territory of the Member States of the European Union until there is a satisfactory system in place allowing for the transmission of such data by the air carriers.'

And

'VIII. Given our recent negotiations, you understand that DHS is prepared to move as expeditiously as possible to a "push" system of transmitting PNR from airlines operating flights between the EU and the U.S. to DHS. Thirteen airlines have already adopted this approach. The responsibility for initiating a transition to "push" rests with the carriers, who must make resources available to migrate their systems and work with DHS to comply with DHS's technical requirements. DHS will immediately transition to such a system for the transmission of data by such air carriers no later than January 1, 2008 for all such air carriers that have implemented a system that complies with all DHS technical requirements. For those air carriers that do not implement such a system the current system shall remain in effect until the air carriers have implemented a system that is compatible with DHS technical requirements for the transmission of PNR data. The transition to a "push" system, however, does not confer on airlines any discretion to decide when, how or what data to push. That decision is conferred on DHS by U.S. law.

Under normal circumstances DHS will receive an initial transmission of PNR data 72 hours before a scheduled departure and afterwards will receive updates as necessary to ensure data accuracy. Ensuring that decisions are made based on timely and complete data is among the most essential safeguards for personal data protection and DHS works with individual carriers to build this concept into their push systems. DHS may require PNR prior to 72 hours before the scheduled departure of the flight, when there is an indication that early access is necessary to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with the purposes defined in Article I. In exercising this discretion, DHS will act judiciously and with proportionality.'

E.2. The relevant written reply of DHS

Question: *How many carriers operating flights from the EU do not have a push system in place?*

Response: As of January 2010, thirteen carriers from the EU have transitioned to the push system. For those airlines that are continuing to operate "pull" systems, CBP has provided extensive technical guidance on how to implement a "push" system and how best to interface with CBP once that system is established. CBP does not have authority to force carriers to implement such a "push" system and responsibility for initiating a transition to "push" remains with the carriers, who must make resources available to migrate their systems. CBP has reached out extensively to the carriers regarding the need to move to a "push" system. In 2007, three carriers from the EU had already adopted the push approach.

E.3. Other relevant information

Since the 2007 agreement there has been an important increase in the number of air carriers that have migrated their systems to push. As of January 2010, 43 carriers have transitioned to the push system, compared to 13 carriers that had been using it when the 2007 agreement was signed. Of those 43 carriers carriers, 15 handle flights to and from the EU compared to 3 such carriers when the 2007 agreement was signed[10]. Migration of a system of push is achieved through compliance with a set of technical standards that have been set by DHS.

DHS requires the data to be transmitted four times before each flight, beginning 72 hours before the scheduled time of departure and lastly at the departure time. These transmissions are applied both for where data is pushed as well as where data is pulled. These timings are subject to change but the airlines are informed accordingly.

In cases where DHS has a hit (an alert) on the basis of data found in the first transmission at 72 hours, or if it has intelligence that a certain individual is due to fly on a specific flight, DHS requires that the data is transmitted at additional intervals to the four standard transmissions, in order to have frequent updates of the situation. These updates are called 'ad hoc requests'.

DHS indicated that it had numerous negotiations with carriers in order to agree the best way to implement the ad hoc requests. According to DHS these negotiations failed to find a way to use a push mechanism to support the requirement because carriers have been unwilling to provide a 24/7

[10] These numbers correspond to the most recent information provided by DHS after their written replies to the questionnaire.

service to DHS for such requests. As a result, DHS implements such requests using only the pull method. This is the case for all carriers, whether they are European carriers, U.S. carriers or other.

The ad hoc pull facility can be initiated only by a limited number of DHS personnel that have a special authorisation for this purpose. Namely, of the approximately 26.000 personnel that have a general access to the ATS-P database where PNR is retained, approximately 8.000 can initiate an ad hoc pull.

The operation of the ad hoc possibility is tracked and is auditable. It has in fact been audited but the EU team was not provided with the results of this audit. The audit showed that DHS conducted ad hoc push/pulls on 1.3% of the PNR (including both EU and non-EU PNR) within the 72 hours of a flight departure. These ad hoc push/pulls take place normally when DHS is verifying a possible match to a law enforcement record, when the data appears incomplete or when circumstances indicate that additional research is required. DHS found that the ad hoc pull possibility is used by officers more frequently than it should and this finding is being further investigated.

As regards the possibility of requesting PNR data earlier than the initial 72 hours, DHS noted that it always uses the pull method to access such data and will continue to do so, as it has been unable to agree with carriers an acceptable push possibility. Even if there were an acceptable solution DHS might need to have a pull ad hoc possibility in the future. DHS stated that during 2009 it never accessed data earlier than 72 hours before the scheduled flight departure.

DHS participates at an IATA working group which is working towards adopting common standards for the format and transmission messaging for PNR. The work of this group is very advanced and it is expected to be completed within 2010. DHS believes that this is the most important work which will simplify and promote the push method.

The possibility of issuing fines for non-compliance to carriers has never been used by DHS. There are circumstances when a carrier changes system providers or has technical issues and DHS has been able to work with the carrier to address non-compliance and correct the issue prior to the need to issue penalties.

E.4. Comments

The progress in increasing the number of air carriers that have migrated to push, as well as the fact that DHS does not have the authority to force carriers to implement the push method, are acknowledged. DHS is urged to continue working towards migrating fully to the push method. The efforts of DHS through the IATA working party or via other for a on common PNR standards are welcome.

However, it is strongly recommended that the ad hoc requests be substantially reduced. Even though the agreement gives the right to DHS to request updates, and even though the need for such updates in some instances is appreciated, the reported practice raises some concerns whether DHS exercises this right judiciously and proportionately. The EU team welcomes the internal audit of this functionality and the admission of DHS that it seems to be used by officers more frequently than it should, and looks forward to progress being achieved on this matter. In addition, the number of personnel that can initiate this functionality is rather large and it is recommended that this is limited to specially authorised senior officials.

It is regrettable that the negotiations for finding an acceptable ad hoc push functionality failed. Even though this seems partly attributable to the carriers' unwillingness to provide a 24/7 service which

is essential, it appears that DHS requirements for the frequency of updates were also responsible for the failure of the negotiations. It is recommended that DHS works towards finding an acceptable way of implementing ad hoc push.

It is noted that both the push and the pull methods carry a certain cost each time they are operated, which puts a substantial financial burden on carriers. Even though the U.S. is facing a substantial terrorist threat , which has been highlighted by the failed Detroit flight attack, , other countries in the world with PNR systems do not request the data more than twice at maximum. On this basis, the high number of ad hoc requests, combined with the pull method of transmission, raise concerns on the proportionate use of this functionality. It is strongly recommended that DHS reassess its way of using this functionality.

F. SHARING OF DATA

F.1. The relevant Commitment of the U.S.

The principles upon which DHS can share data with other US authorities and other government authorities in third countries are expressed in paragraph 6 of the agreement as supplemented by paragraph II of the letter accompanying the agreement, which state that:

'6. For the application of this Agreement, DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union. Concomitantly, the EU will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds.'

And

'II. DHS shares EU PNR data only for the purposes named in Article I.

DHS treats EU PNR data as sensitive and confidential in accordance with U.S. laws and, at its discretion, provides PNR data only to other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, transnational crime and public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating, according to law, and pursuant to written understandings and U.S. law on the exchange of information between U.S. government authorities. Access shall be strictly and carefully limited to the cases described above in proportion to the nature of the case.

EU PNR data is only exchanged with other government authorities in third countries after consideration of the recipient's intended use(s) and ability to protect the information. Apart from emergency circumstances, any such exchange of data occurs pursuant to express understandings between the parties that incorporate data privacy protections comparable to those applied to EU PNR by DHS, as described in the second paragraph of this article.'

F.2. The relevant written reply of DHS

Question: *For what purposes has DHS shared PNR information with the Center for Disease Control?*

Response: DHS shares PNR information with the Department of Health and Human Services (HHS) Center for Disease Control (CDC) to properly coordinate appropriate responses to health

concerns associated with international air transportation and as part of a framework for cooperation to enhance the Nation's preparedness against the introduction, transmission, and spread of quarantinable and serious communicable diseases from foreign countries. Sharing for this purpose is clearly envisioned when necessary for the protection of the vital interests of the data subject or other persons. DHS has a 2005 Memorandum of Understanding (MOU) in place with the CDC dictating the specific terms and protocols for the sharing of information, including PNR. The SORN for ATS allows for sharing of information "to appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk."

The amount of PNR shared depends on the particular situation. In certain instances, based on the disease, information regarding the individual or individuals who sat in a specific seat location or locations near the infected individual will be shared, (generally contact information); in other instances information regarding all passengers on the flight is shared. In all instances sharing is logged in ATS.

It is important to note that many responses to data requests from CDC do not contain PNR from ATS. CDC disclosure requests are logged by National Targeting Center – Passenger (NTC-P) personnel and documented on a DHS Form 191, completed by NTC or CDC staffs as appropriate.

The Privacy Office reviewed in 2008 and again in 2010 the log kept in ATS for sharing of PNR. Additional specific details about this sharing will be covered during the Joint PNR Review. [*such details have indeed been given during the joint review]*

Question: *With which U.S. and foreign authorities has DHS shared PNR data?*

Response: DHS shares PNR information with other U.S. government and foreign authorities in compliance with the 2007 U.S. - EU PNR Agreement. DHS shared PNR data twice with foreign governments. Specific details about this sharing will be covered during the Joint PNR review. [*such details have indeed been given during the joint review]*

DHS treats EU PNR data as sensitive in accordance with U.S. laws and DHS policies and provides PNR data only to other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, serious transnational crime and public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating, according to law, and pursuant to written understandings and U.S. law on the exchange of information between U.S. government authorities. Access is strictly and carefully limited to the cases described above in proportion to the nature of the case.

EU PNR data will only be exchanged with other government authorities in third countries after consideration of the recipient's intended use(s) and ability to protect the information. Apart from emergency circumstances, any such exchange of data occurs pursuant to express understandings between the parties that incorporate data privacy protections comparable to those applied to EU PNR by DHS.

Under the Privacy Act, absent the consent of the data subject, DHS may only share PNR with another government if there is an appropriate routine use or it adheres to one of the statutory basis for disclosure as outlined in the Privacy Act; the use must be compatible with the purpose of the

original collection. This requirement is in place whether there is an emergency or not.

Question: *Is sharing with foreign authorities initiated by them or by DHS?*

Response: DHS shares PNR information with foreign authorities in compliance with the 2007 U.S. - EU PNR Agreement. As a general matter, whether the sharing is initiated by the foreign authority or DHS will depend on the specifics surrounding the particular case.

F.3. Other relevant information

As regards sharing of PNR data with other US governmental authorities, all cases of sharing are tracked (logged) and are auditable. Sharing needs to be justified. The DHS Privacy Office audited all cases of such sharing. The results have been published in the Update to its own Report on the implementation of the agreement which was published on its website in February 2010. It appears that DHS shared PNR data with other U.S. agencies 694 times, out of which 216 related to EU-originating PNR data. 11% of the EU PNR data was shared with other DHS components, 87% with the Department of Justice, including FBI and 2% with other law enforcement agencies. 75% of sharing took place in relation to terrorism cases, 18% for transnational crimes and 7% for use in law enforcement or criminal proceedings. DHS found that all cases of sharing were properly justified.

DHS explained that the sharing of PNR data with other U.S. agencies takes place following a specific request of such other agency. In some instances however, DHS initiates the sharing itself, where it believes that the information is important for the other agency. Sharing in most instances relates to specific investigations, is always carried out on a case-by-case basis and never in bulk. Predominantly other federal agencies obtained such PNR data, in few instances data was shared with state and municipal levels and in no occasion has PNR been shared with tribal agencies.

The Privacy Act applies to all processing of data which is done by Federal agencies, therefore, sharing of PNR data with such agencies is covered by the provisions of this act. One of the safeguards provided by the Privacy Act is that data which is shared with another agency, cannot be forwarded by the recipient agency to another agency. DHS has a Memorandum of Understanding regulating the sharing of data with the Terrorist Screening Center.

DHS has shared PNR data with the Center for Disease Control (CDC) on 4 occasions in order to safeguard the vital interests of the data subject. No one of these occasions related to EU-originating PNR data. DHS has a Memorandum of Understanding with the CDC. The sharing between the two agencies takes place in relation to a list of communicable and quarantinable diseases that corresponds to the list of the World Health Organisation, and not to the list of diseases referred to when a person applies for an ESTA.

As regards sharing of PNR data with government authorities in other countries, DHS replied that it shared data only twice with such authorities. In addition, DHS has a Memorandum of Understanding with the Canada Border Services Agency (CBSA) since 2005. Under this Memorandum of Understanding, the two agencies set some common scenario-based targeting rules. Once there is a hit in either agency on the basis of these common targeting rules, then the agencies will exchange only the name of the passenger between them for the purpose of informing each other whether they have any further data regarding the passenger. To that extent, the sharing of data between the two agencies cannot be considered as a bulk exchange but rather a case-by-case one. In addition, the two agencies do not exchange the whole PNR record but only the name of the passenger. In any case, it is noted that this Memorandum of Understanding refers to the

Commitments of the U.S. towards the EU as regards EU-originating PNR data. The Memorandum of Understanding until recently referred to the Commitments of the U.S. under the 2005 agreement. This has been corrected in July 2009 through an exchange of letters between the two agencies and the Memorandum of Understanding now refers to the current 2007 agreement.

F.4. Comments

It appears that DHS respects and implements this commitment satisfactorily. The sharing of PNR data with other U.S. agencies is handled well, it is limited and it is audited. The purposes of the sharing seem compatible with the purposes of the agreement. Sharing with government agencies in third countries is rarely used and when it is done, it is under appropriate safeguards.

G. ACCESS AND REDRESS

G.1. The relevant Commitment of the U.S.

The rights of passengers for access and redress is expressed in paragraph 3 of the agreement as supplemented by paragraphs IV and V of the letter accompanying the agreement, which state that:

'(3)DHS shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable U.S. laws, constitutional requirements, and without unlawful discrimination, in particular on the basis of nationality and country of residence. The DHS's letter sets forth these and other safeguards.'

And,

'IV. DHS has made a policy decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with U.S. law, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR. These policies are accessible on the DHS website, www.dhs.gov.

Furthermore, PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U. S. Privacy Act and the U. S. Freedom of Information Act (FOIA). FOIA 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 disclosure by an applicable exemption under the FOIA. DHS does not disclose PNR data to the public, except to the data subjects or their agents in accordance with U.S. law. Requests for access to personally identifiable information contained in PNR that was provided by the requestor may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791).

In certain exceptional circumstances, DHS may exercise its authority under FOIA to deny or postpone disclosure of all or part of the PNR record to a first part requester, pursuant to Title 5, United States Code, Section 552(b). Under FOIA any requester has the authority to administratively and judicially challenge DHS's decision to withhold information.'

And

'V. Administrative, civil, and criminal enforcement measures are available under U.S. law for violations of U.S. privacy rules and unauthorized disclosure of U.S. records. Relevant provisions include but are not limited to Title 18, United States Code, Sections 641 and 1030 and Title 19, Code of Federal Regulations, Section 103.34.'

G.2. The relevant written reply of DHS

Question: *Have any requests been made by passengers to receive a copy of their PNR contained in any of DHS databases under the Freedom of Information Act (FOIA) or under the Privacy Act? If so, how many requests have been made? What was the outcome?*

Response: Yes, DHS/CBP has received requests from individuals for a copy of their PNR under FOIA and the Privacy Act. DHS/CBP does not track the number of requests related specifically to PNR. As noted in the 2008 Review issued by the DHS Privacy Office, the CBP FOIA office had areas in which it needed to improve. As will be noted in the follow up report, the CBP FOIA group has been making substantial improvements in its process and tracking and in December 2009 began categorizing requests into seven categories: 1) Traveler, 2) Border Patrol, 3) Commercial, 4) Human Resources, 5) Internal Affairs, 6) Media, and 7) Other. Requests for PNR would fall into the first category, "Travelers."

Issues related to inconsistencies in applying applicable exemptions to PNR requests and the need for training on various search capabilities for the source system have been addressed in that all FOIA and Privacy Act requests related to the Automated Targeting System – Passenger (ATS-P), the system that maintains PNR, are currently handled by a single individual in the CBP FOIA branch. This individual is well versed in the search methods available to locate PNR records in ATS, as well as traveller-related data maintained in other CBP systems.

Question: *Have any measures for administrative, civil or criminal enforcement been taken under U.S. law for violations of U.S. privacy rules and unauthorized disclosure of U.S. records?*

Response: There have been no violations related to the privacy rules and thus no administrative, civil, or criminal enforcement related to the misuse of PNR.

G.3. Other relevant information

All requests for access are handled by the CBP FOIA Branch. The requests for access may be made through three different means, i.e. the CBP FOIA Branch, the DHS TRIP and the CBP INFO center. The DHS Chief Privacy Officer can also be a direct source of access and redress. Requests for access using FOIA or the Privacy Act are treated in the same manner by the CBP FOIA Branch, applying whichever Act provides wider access.

During 2009 CBP received approximately 25.000 requests for access to data. 50% of such requests were related to traveler data. DHS was unable to specify how many of such requests were related to EU-originating PNR data. However, DHS confirmed that all requests for access have been successful and passengers were always given access to their data. In fact, the System of Records Notice (SORN) regarding that ATS-P database which was published on August 6, 2007 expressly notes that "persons whose PNR data has been collected and maintained in ATS-P will have administrative access to that data under the Privacy Act.".

Moreover, DHS realised that in most instances where travelers request access to their PNR data, they are in fact looking for their whole entry/exit record. In order to address this issue, when DHS receives a request for PNR data, it also supplies the travelers's full entry/exit record.

According to DHS, the largest number of requests for access to PNR data seems to be made from people who want to prove the length of their stay in the U.S. for immigration or litigation purposes. Few requests seem to be made by passengers for other reasons.

During 2009, the CBP FOIA Branch was able to reduce its backlog to less than 2% of its highest 2008 levels, which is a great progress.

DHS has not received any requests for correction of PNR data.

Only one case of request for access ended up in litigation, which is the case of Sophie In't Veld MEP. Ms In't Veld had made a FOIA request for access. The CBP FOIA Branch responded to the request. She considered that the results received from CBP were inadequate and therefore sought a judicial remedy. The United States District Court for the District of Columbia ruled against her request and found that the response of CBP was satisfactory.

G.4. Comments

This commitment seems to be satisfactorily implemented by DHS. The substantial progress achieved by DHS on this point, which has been one of the most difficult in the past, is acknowledged.

It is however noted that until December 2009 DHS had no system for tracking (logging) the types of requests. It is further noted that the newly introduced tracking system is not ideal. It is only able to track requests under the general heading 'travelers' and it is unable to distinguish between requests for access to PNR data and requests for other data, and it also unable to track requests specifically relating to EU-originating PNR data. It is recommended that this issue be further addressed with fine-tuning of the tracking systems to facilitate audits of the systems.

H. NOTICE

H.1. The relevant Commitment of the U.S.

The obligation to inform passengers is expressed in paragraph 7 of the agreement as supplemented by paragraph VI of the letter accompanying the agreement, which state that:

'7. The U.S. and the EU will work with interested parties in the aviation industry to promote greater visibility for notices describing PNR systems (including redress and collection practices) to the travelling public and will encourage airlines to reference and incorporate these notices in the official contract of carriage.'

And

'VI. DHS has provided information to the travelling public about its processing of PNR data through publications in the Federal Register and on its website. DHS further will provide to airlines a form of notice concerning PNR collection and redress practices to be available for public display. DHS and the EU will work with interested parties in the aviation industry to promote greater visibility of this notice.'

H.2. The relevant written reply of DHS

Question: *How does DHS provide travellers with information on PNR data processing?*

Response: DHS has provided information to the travelling public about its processing of PNR data through publications in the Federal Register and on its website. DHS further provided to airlines a form of notice concerning PNR collection and redress practices to be available for public display.

In 2007 DHS and the Department of Transportation worked with the International Air Transport Association (IATA) to support a review of the standard contract of carriage notices provide by airlines to ensure consistency with the 2007 U.S.-EU PNR Agreement. On July 31, 2007, IATA disseminated recommended language to its carriers.

DHS published the following documents in the Federal Register and on its website (www.dhs.gov/privacy):

– Privacy Impact Assessment Update for the Automated Targeting System (ATS) published December 2, 2008.

– ATS System of Records Notice re-published on August 6, 2007, 72 FR 43650 in response to significant public comment.

– Final Rule related to Privacy Act Exemptions in the Federal Register on February 3, 2010.

– Privacy Impact Assessment Update for the Automated Targeting System, published August 3, 2007.

– System of Records Notice published on November 2, 2006, 71 FR 64543.

– Privacy Impact Assessment for the Automated Targeting System, published November 22, 2006.

Additionally, CBP has published Frequently Asked Questions and the PNR Privacy Policy on its web site www.cbp.gov under "Traveller" (available directly at http://www.cbp.gov/xp/cgov/travel/clearing/pnr/).

H.3. Other relevant information

DHS has published Frequently Asked Questions and the PNR Privacy Policy on its web site www.cbp.gov under "Traveller" (available directly at http://www.cbp.gov/xp/cgov/travel/clearing/pnr/). However, these two documents were only published on its website on 27 January 2010. Prior to such publication, the website of DHS had information relating to the 2004 PNR agreement with the EU.

H.4. Comments

DHS worked satisfactorily with carriers on providing information to the travelling public about the use of PNR data.

However, as regards the DHS website, the PNR Privacy Policy and Frequently Asked Questions were not updated until 27 January 2010. It seems therefore that DHS has not been complying with this obligation until such date. Such delay in compliance is regrettable, especially in light of the fact that the DHS Privacy Office pointed out this issue in December 2008 in its own Report on the implementation of the agreement.

Nevertheless, with the publication of the new Frequently Asked Questions and the PNR Privacy Policy, DHS now satisfactorily implements this commitment.

I. RECIPROCITY/CO-OPERATION

I.1. The relevant Commitment of the U.S.

The reciprocity and cooperation provisions are expressed in paragraph 5 of the agreement as supplemented by paragraph IX of the letter accompanying the agreement, which state that:

'5. By this Agreement, DHS expects that it is not being asked to undertake data protection measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems. DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of the DHS letter while conducting consultations with the EU with a view to reaching a prompt and satisfactory resolution. In the event that a PNR system is implemented in the European Union or in one or more of its Member States that requires air carriers to make available to authorities PNR data for persons whose travel itinerary includes a flight to or from the European Union, DHS shall, strictly on the basis of reciprocity, actively promote the cooperation of the airlines within its jurisdiction.'

And

'IX. During our recent negotiations we agreed that DHS expects that it is not being asked to undertake data protection measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems. DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of the DHS letter while conducting consultations with the EU with a view to reaching a

prompt and satisfactory resolution. In the event that an airline passenger information system is implemented in the European Union or in one or more of its Member States that requires air carriers to make available to authorities PNR data for persons whose travel itinerary includes a flight between the U.S. and the European Union, DHS intends, strictly on the basis of reciprocity, to actively promote the cooperation of the airlines within its jurisdiction.

In order to foster police and judicial cooperation, DHS will encourage the transfer of analytical information flowing from PNR data by competent U.S. authorities to police and judicial authorities of the Member States concerned and, where appropriate, to Europol and Eurojust. DHS expects that the EU and its Member States will likewise encourage their competent authorities to provide analytical information flowing from PNR data to DHS and other U.S. authorities concerned.'

I.2. The relevant written reply of DHS

The EU team did not address a written question to DHS on this point.

I.3. Other relevant information

In preparation for the review exercise, the European Commission addressed letters to Europol and Eurojust seeking information about the instances in which they received either PNR or analytical information flowing from PNR data from DHS under the provisions of this agreement. Both agencies replied that they had never received any such information from DHS.

DHS admitted that it has never shared either PNR data or analytical information flowing from PNR data with Europol, Eurojust or any Member State, with only one exception where PNR was provided to one Member States in relation to an ongoing investigation. This was done following the request of the concerned Member State.

DHS noted that it had not been approached by any other Member State or agency for the provision of such information. It also feels that it needs to have some special arrangements with the relevant bodies if it were to share such information on a standard basis. It therefore wishes to encourage Member States police and judicial authorities, as well as Europol and Eurojust, to establish an analytical information sharing relationship with DHS and explore the collection of PNR.

Nevertheless DHS acknowledged that it could do more to implement this commitment further and noted its willingness to examine ways of doing so. DHS believes that such sharing should be bi-directional.

I.4. Comments

This commitment does not seem to be implemented by DHS. The commitment imposes a pro-active obligation on DHS to encourage the sharing information with Member States and where appropriate with Europol and Eurojust, which DHS has not acted upon. This is regrettable. Such information would be highly valuable to the law enforcement authorities of the Member States and the two agencies.

On the other hand DHS indicated that it would be willing to share analytical information more proactively. DHS, Member States, Europol and Eurojust should consider how to share such information in the future.

It is noted that DHS and the EU have identified improving this sharing of information as a priority under the January 21, 2010 Toledo Declaration on Aviation Security adopted by Secretary Janet Napolitano, former European Commission Vice-President Barrot and the Spanish Presidency represented by Interior Minister Rubalcaba.

ANNEX B
COMPOSITION OF THE REVIEW TEAMS

The members of the EU team were:

- Reinhard Priebe, Director, DG JLS – Head of the delegation
- Marie Helene Boulanger, Head of Unit, DG JLS – Deputy head of the delegation
- Heike Buss, Deputy Head of Unit, DG JLS
- Despina Vassiliadou, Administrator, DG JLS
- Hans Tischler, expert on data protection from the German data protection authority
- Jesper Voigh Andersen, expert on law enforcement issues, police officer from Denmark
- Frank Schmiedel from the EU delegation in Washington.

It is noted that Hans Tischler and Jesper Voigh Andersen participated in the EU team as experts for the Commission and not in their other professional capacities.

John Fitzpatrick, Deputy Director, Border Policy, UK Border Agency also participated in the discussions in compliance with the last parameter of the review paragraphs. He was not considered as part of the EU team.

The members of the US team were:

- Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, DHS
- John Kropf, Deputy Chief Privacy Officer, Privacy Office, DHS
- Shannon Ballard and Lauren Saadat, Co-Directors, International Privacy Policy, Privacy Office, DHS
- Rebecca Richards, Director, Compliance, Privacy Office, DHS
- Jamie Pressman, Associate Director, Compliance, Privacy Office, DHS
- Michael Scardaville, Director for European and Multilateral Affairs, Office of International Affairs, Office of Policy, DHS
- Patricia Cogswell, Acting Deputy Assistant Secretary, Screening Coordination Office, Office of Policy, DHS
- Justin Matthes, Director, Screening Coordination Office, Office of Policy, DHS
- Regina Hart, Senior Counsel, Office of the General Counsel, DHS
- Edward Bolton, Chief, Tactical Operations Division, Customs and Border Protection (CBP), DHS
- Thomas Bush, Director Analysis and Targeting, CBP, DHS
- David Dodson, Passenger Branch Chief, Office of Intelligence and Operations Coordination, CBP, DHS
- Kristin L. Dubelier, Senior Attorney, Office of Chief Counsel, CBP, DHS
- Laurence Castelli, Chief, Privacy Act Policy and Procedures, CBP, DHS
- Steven P. O'Neill, Program Manager, Office of Field Operations, CBP, DHS