U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security

Privacy Office, Mail Stop 0550

March 7, 2008

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

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

Dear Ms. Hofmann:

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

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

In telephonic calls with counsel representing the Department of Homeland Security in December 2007, you agreed to narrow the scope of your request. The Government proposed that plaintiff eliminate non-responsive material within email chains from the scope of the request. Plaintiff agreed that emails within an email chain containing no responsive material may be removed from the scope of the request, and further suggested that defendant may eliminate duplicative copies of emails that contain responsive material from the scope of the request.

As we advised you in our December 7th partial release letter, we have completed our search for responsive documents, and all responsive documents have been processed except for the documents being held at DHS for classification review and the classified documents that were referred outside the agency for releasability review.

We completed our review of 83 responsive documents, consisting of 362 pages, which were being held for possible classification. I have determined that 41 of those documents, consisting of 158 pages, are releasable in part, and 42 documents, consisting of 204 pages, are withholdable in their entirety. The releasable information is enclosed. The withheld information, which will be noted on the *Vaughn* index when completed, consists of properly classified information, names, telephone numbers, email addresses, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 1, 2, 5, 6, and 7(E) of the FOIA, 5 U.S.C. §§ 552 (b)(1), (b)(2), (b)(5), (b)(6), and (b)(7)(E).

We also completed our review of 9 responsive documents, consisting of 51 pages, that were referred to the Department of State (DOS) and the National Security Council (NSC) for releasability review. I have determined that those documents are witholdable in their entirety. The withheld information, which will be noted on the *Vaughn* index when completed, consists of properly classified information and deliberative material. I am withholding this information pursuant to Exemptions 1 and 5 of the FOIA, 5 U.S.C. §§ 552 (b)(1) and (b)(5).

FOIA Exemption 1 provides that an agency may exempt from disclosure matters that are (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive Order. Portions of the withheld documents concern foreign government information relating to the national security and United States government programs and are classified under §§ 1.4(b), 1.4(c), 1.4(d), and 1.4(g) of Executive Order 12958, as amended.

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

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

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

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

Our office continues to process your request insofar as it relates to the remaining classified documents referred outside the agency and the remaining documents being held for DHS classification review. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-90/Hofmann request.** The DHS Privacy Office can be reached at 703-235-0790 or 1-866-431-0486.

Thank you for your patience as we proceed with your request.

Sincerely,

Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: As stated, 158 pages

FOR OFFICIAL USE ONLY

DEPUTIES MEETING ON PNR

DATE: Tuesday, July 25, 2006
TIME: 12:00 - TBD
LOCATION: Facility, Building, Office *(e.g., NAC,* [redacted]
FROM: Stewart Baker, Assistant Secretary for Policy

OBJECTIVES/DESIRED OUTCOME OF MEETING:

- Establish an interagency negotiating position [redacted]

b5 b2 (high) b7E

BACKGROUND:

- On May 30, 2006 the European Court of Justice (ECJ) ruled that the legal instruments the European Union utilized in striking a 2004 agreement with DHS on CBP's access to PNR were in appropriate and required the EU to terminate the agreement by September 30, 2006

b1

b1

PARTICIPANTS:
Non-DHS

DHS
Deputy Secretary Jackson

PRESS PLAN: "Closed"

ATTACHMENTS:

A. Discussion Document: Analysis of United States Interests in the U.S.-EU PNR dialogue (7/13/06)
B. Memo: Summary of Potential Changes to the Undertakings (*PENDING*)
C. Member State Positions known as of 7/20/06
D. Background on EU views of consent as a solution
E. DHS' Response Options to European Court of Justice Decision (February 2006)

Prepared by: Michael Scardaville, PDEV, b2 (low)

FOR OFFICIAL USE ONLY

DEPUTIES MEETING ON PNR (U)

DATE: Tuesday, July 25, 2006
TIME: 12:00 - TBD
LOCATION: Facility, Building, Office *(e.g., MAC, C b2 (low)*
FROM: Stewart Baker, Assistant Secretary for Policy

(C) **OBJECTIVES/DESIRED OUTCOME OF MEETING:**

b1

BACKGROUND: (U)

(U) On May 30, 2006 the European Court of Justice (ECJ) ruled that the legal instruments the European Union utilized in striking a 2004 agreement with DHS on CBP's access to PNR were inappropriate and required the EU to terminate the agreement by September 30, 2006. The EU has since provided notice that it is terminating the agreement effective that date.

(U) (C) In issuing this ruling the ECJ indirectly commented on the substance of the issue by emphasizing that the EU's 1995 directive on data protection in first pillar does not apply to the transfer of PNR data which is a law enforcement (third pillar issue). Concern that CBP regulations conflicted with this directive was the reason the agreement was struck in the first place. However, the ECJ did not comment on the sufficiency of DHS's efforts to protect privacy.

(U) However, the current arrangement does have significant impacts on DHS operations. In particular, the limitations on sharing and retention enshrined in the Undertakings has prohibited broader use within DHS to combat terrorism and crime. C

[b5 b2(high) b7E]

(S)

b1

(C)

b1

(U) The PNR negotiations will be closely intertwined with a broader effort to establish restrictive, EU-wide rules for information sharing in the area of law enforcement. Last October the EU put forward a Council decision on the protection of personal data in criminal

Derived: Schwartz, MPR, Date: 25 JUL 2006

FOR OFFICIAL USE ONLY

(2)

b1

(c) **PARTICIPANTS:**
Non-DHS

DHS
Deputy Secretary Jackson

(d) **PRESS PLAN:** "Closed"

(e) **ATTACHMENTS:**

A. Discussion Document: Analysis of United States Interests in the U.S.-EU PNR dialogue (7/13/06)
B. Memo: Summary of Potential Changes to the Undertakings (*PENDING*)
C. Member State Positions known as of 7/20/06
D. Background on EU views of consent as a solution
E. DHS' Response Options to European Court of Justice Decision (February 2006)

(f) **Prepared by:** Michael Scardaville, PDEV, C b2 (low) 3

Attachment A

SECRET

DISCUSSION DOCUMENT
Analysis of United States Interests in the U.S.-EU PNR dialogue
Department of Homeland Security

July 13, 2006

Purpose

To provide you with background information on the Passenger Name Record (PNR) issue and related developments concerning law enforcement information sharing with the European Union (EU) in preparation for a mid-July "un-DC."

Summary

Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. Some of this information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects prior to arrival, and even before the plane takes off[1], protecting against mid-flight hijackings and bombings.

For flights between Europe and the U.S., the data must be made available from European air carriers. EU law has long prohibited the commercial export of personal data to countries whose legal protections have not been deemed "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that corresponds to every aspect of European law. It has therefore been viewed as "inadequate" by European standards, and commercial data transfers to the U.S. have long been restricted by the lack of a broad adequacy finding. While the EU lacks similar requirements for the transfer of law enforcement information between the EU and third parties, a Framework Decision is currently being considered that would mirror the requirements applied in the commercial realm.

[b5 b2(high) b7E]

b1

[1] CBP may automatically access PNR data from European carriers up to 72 hours in advance of a flight. During this pre-departure period, information is screened against CBP automated systems and risk scores begin to be generated. In some cases, particularly airports where CBP maintains a presence through the Immigration Advisory Program, coordinated law enforcement action is also planned in advance with local authorities. Analysis continues up to arrival and is further supported by the collection of manifest information.

The PNR Agreement was also controversial in Europe. It was challenged by the European Parliament as insufficiently protective of EU privacy rights. On May 30 the European Court of Justice (ECJ) struck down the Agreement. But it chose a ground that was highly procedural – the equivalent under US law of the Supreme Court ducking a Fourth Amendment challenge by finding a law invalid because it exceeded Congress's Commerce Clause power. Under EU law, commercial issues fall within the jurisdiction of the EU as part of its "First Pillar" authority. This is the authority that the EU relied on in entering the Agreement. The ECJ, however, held that the US wanted PNR data for law enforcement and public security reasons. Law enforcement and public security are exempt from the EU's commercial data protection laws and are only partly within the EU's authority. Instead, they fall under the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. This finding by the Court also eliminates the uncertainty that led to the signing of the agreement in the first place, specifically the fear that some Member States might bring action against air carriers under the commercial legal framework.

Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU has obtained authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. As required by the Agreement, the EU also notified the United States that it will terminate the current Agreement on September 30, 2006 and has set a goal of establishing a new agreement by this date. The USG received a proposed replacement text from the Finnish Presidency on July 19th, although Commission officials have indicated that this draft may not be final.[3] Commission representatives have portrayed their proposal as a technical change that would put the same agreement back in place, albeit under a different legal authority.

[3] CBP can share PNR data with other law enforcement agencies, but only on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes. This restriction prevents PNR information from being shared in bulk with the intelligence and law enforcement community, and it denies those agencies direct access to the records. Broader access would allow other agencies to look for patterns in the travel of individuals not deemed to be high risk and to assess connections between passengers. ICE, for example, has expressed its frustration over losing access to this information.

Both the Departments of State and Homeland Security have a number of questions regarding the legal impact of a variety of wording choices, including references to the European Convention on Human Rights. Additional policy analysis is underway and our response will be driven by the decisions of the Deputies.

b1

(S)

b1

(S)

Background

Two converging events in Europe – the recent European Court of Justice decision on the legality of the EU-US PNR Agreement and a draft EU Framework Decision on Exchange of Criminal Data -- have major implications for US law enforcement and security.

The EU-US PNR Agreement. As noted, in May 2004, after substantial negotiations, the Department of Homeland Security entered into an agreement relating to the sharing of PNR information collected by air carriers flying to the United States from Europe. The Agreement was intended to resolve a perceived conflict between EU law (which limits the sharing of personal information collected by commercial entities with governmental entities) and US law (which required the collection and dissemination of PNR data). Central to the Agreement was a set of Undertakings made by Customs and Border Protection (CBP) regarding how it would treat the PNR data transmitted to it.[4] Several of the limitations in those Undertakings

(U)

(C)

b1

(4) The most significant of these limitations, from our perspective are the following:

1.

(C) b1

b1

b1

(C) b1

[b5]

(U) b1

(U) b1

(S) b1

(U) **The ECJ PNR Case.** The Agreement was no less controversial in Brussels. Disturbed over what it viewed as an attack on personal privacy and its own authority, the European Parliament (EP) filed two suits in the European Court of Justice (ECJ) challenging the information sharing arrangement.

(U) On May 30, 2006, the ECJ issued its opinion in the lawsuits. The opinion did not address the merits of the EU-US PNR Agreement or the role of the Parliament. Rather, the decision turned

(U) [6] This concern is consistent with Executive Order 13388 and the President's Memorandum issued on December 16, 2006 to Heads of Executive Departments and Agencies on "Guidelines and Requirements in Support of Information Sharing Environment."

(C/FGI-MOD) b1

on the lack of competence of the Commission and Council to enter into the Agreement in the first instance. The EU had based its authority on the so-called "First Pillar," which allows the EU to regulate trade and commercial matters. The ECJ held (as the US had argued earlier) that the requirement that PNR data be sent to the US was a law enforcement and national security matter. Such transfers, the court held, were excluded from the data protection directive governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."[8]

(u) That is what the EU proposes to do. It has obtained authority from its Member States to erect substantially the same agreement on a new foundation. In order to meet the European Court of Justice deadline the Commission will seek to codify its position over the next couple of weeks and then will call for agreement on the new arrangement by September 30.

(S) b1

EU Proposals on Sharing Law Enforcement Information. If that were all that is at stake, this would be an interesting diplomatic and legal problem for DHS. But it is not. The PNR negotiations will be closely intertwined with a broader effort to establish restrictive, EU-wide rules for information sharing in the area of law enforcement. Last October the EU put forward two draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft Framework Directive of the European Parliament and Council on the retention of data and a proposed Council decision on the protection of personal data in criminal matters. [9]

(u) b5 b2(high) b7E

b1

[8] Acting under the First Pillar, the EU has also entered into a PNR sharing agreement with Canada. In light of the EU's determination that the US Undertakings provided "adequate" privacy protections, the EU-Canada agreement authorizes Canada to share PNR data received from the EU with the US. Even though the ECJ has struck down the EU-US agreement, the EU contends that its similar agreement with Canada remains in effect. Some Canadian government sources are concerned, however, that the absence of an "adequacy" finding (which is a First Pillar concept) may now have the effect of *prohibiting* US-Canada information sharing derived from EU-originated flights.

(u) [9] For example, the Draft Decision contains provisions on time limits for retention of shared data, ensuring the accuracy of shared data, logging and audit trails, as well as restrictions limiting further use of the data to the original

b1

(C/fgi-) mod

b1

(C/fgi-) mod

b1

purpose for which it was first transmitted. In effect, it borrows heavily from the PNR Agreement and the Undertakings.

(C/fgi-) mod

b1

(u) [11] The adequacy finding granted to the U.S. was specific to the transfer of PNR data and only extended to its transmission to CBP. The May 30th decision of the ECJ also annuls this decision by the Commission on the grounds that the Commission did not have the legal authority to grant it

(u) [12] If adopted without the offered exemptions, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (MLAT) with the European Union and a 2001 information sharing agreement with Europol (the EU-level police agency); with respect to member states, we signed a 2003 MLAT with Germany,

Communicable Diseases. One indicator of the extent to which EU data protection authorities prioritize the expansion of such roles over public safety concerns can be found in the European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers legal jeopardy because of inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States. [13]

(u)

Analysis & Recommendation (u)

(S)

b1

which builds on numerous other MLATs already in force with other EU member states. The United States also has many executive agreements and memoranda of understanding with member states under which critical information is currently being shared. Under EU law, directives supersede bilateral treaties and agreements and member states must conform their existing agreements to the directive.

(u) [13] Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission nor the Article 29 Committee have challenged the DHS-HHS MOU.

(u) [14] Unlike in 2003, this risk is present now because the Court has conclusively ruled that the transfer of PNR data is a law enforcement matter. While European integration has been the greatest in areas associated with the Common Market, law enforcement and public security is a relatively new area of activity at the community level and many responsibilities still fall to the EU Member States. The ECJ firmly placed PNR in the area of law enforcement and public security, and as result, any actions taken in this area are likely to set precedents for further community involvement in other law enforcement matters.

b1

(S)

Conclusion

b1

The USG has a paramount interest in ensuring that law enforcement and border control information continues to flow to the United States. In creating the Information Sharing Environment we are working to break down walls that restrict the sharing of information between Federal agencies.

(U) [15] Excluding Canada and Mexico, flights originating in these five countries comprise nearly a quarter of all international flights arriving in the United States. In terms of global traffic, flights arriving from the UK rank third (after Canada and Mexico). Germany is 6th; France 9th; the Netherlands 10th; and Italy 17th.

(u) The PNR Agreement that the US signed with the EU in 2004 is an example of the old-style artificial limitation. We entered into the PNR Agreement based upon the EU's argument that the export of commercial information was subject to special restrictions under EU law. The European Court of Justice has now held that the information is law enforcement information, not commercial information, so that the rationale for the agreement has now dissolved.

b1

Attachments

A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995)

B. Excerpt from Draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter (October 2005)

UNCLASS

Attachments:

A. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

UNCLASS

B. Proposal for a COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.
(a) The transfer is provided for by law clearly obliging or authorising it.
(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.
(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.
(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where, under the procedure provided for in Article 16, it is established that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.

5. In accordance with the procedure referred to in Article 16, it may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

UNCLASS

6. Exceptionally, personal data received from the competent authority of another Member State may be further transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.

Attachment B

Pending completion.

Attachment C

Member State Positions known as of 7/20/06

Attachment D

EU Views on Consent

b1

b1

History of DHS Discussions with the EU on Consent and PNR

b1

b1

Attachment E

Issue: DHS' Response Options to European Court of Justice Decision
February 2006

b1

DHS' Optional Responses

b1

1)

(c)

(c)

(c)

(c)

b1

❖

❖

2)

(c)

(c)

b1

(c)

3)

DEPUTIES MEETING ON PNR

DATE: Tuesday, July 25, 2006
TIME: 12:00 - TBD
LOCATION: Facility, Building, Office *(e.g., NAC)* [b2(low)]
FROM: Stewart Baker, Assistant Secretary for Policy

OBJECTIVES/DESIRED OUTCOME OF MEETING:

- Establish an interagency negotiating position [

[b5 b2(high) b7E]

BACKGROUND:

- On May 30, 2006 the European Court of Justice (ECJ) ruled that the legal instruments the European Union utilized in striking a 2004 agreement with DHS on CBP's access to PNR were in appropriate and required the EU to terminate the agreement by September 30, 2006. The EU has since provided notice that it is terminating the agreement effective that date.
- In issuing this ruling the ECJ indirectly commented on the substance of the issue by emphasizing that the EU's 1995 directive on data protection in first pillar does not apply to the transfer of PNR data which is a law enforcement (third pillar issue). Concern that CBP regulations conflicted with this directive where the reason the agreement was struck in the first place. However, the ECJ did not comment on the sufficiency of DHS's efforts to protect privacy.
- However, the current arrangement does have significant impacts on DHS operations. In particular, the limitations on sharing and retention enshrined in the Undertakings has prohibited broader use within DHS to combat terrorism and crime. Most affected by this change has been ICE. [

[b5 b2(high) b7E]

-

b1

-

b1

-

b1

b1

PARTICIPANTS:
Non-DHS

DHS
Deputy Secretary Jackson

PRESS PLAN: "Closed"

ATTACHMENTS:

A. Discussion Document: Analysis of United States Interests in the U.S.-EU PNR dialogue (7/13/06)
B. Memo: Summary of Potential Changes to the Undertakings (*PENDING*)
C. Member State Positions known as of 7/20/06
D. Background on EU views of consent as a solution
E. DHS' Response Options to European Court of Justice Decision (February 2006)

Prepared by: Michael Scardaville, PDEV. b2 (low)

FOR OFFICIAL USE ONLY

DEPUTIES MEETING ON PNR

DATE: Tuesday, July 25, 2006
TIME: 12:00 - TBD
LOCATION: Facility, Building, Office (e.g., NAC, [b2(low)]
FROM: Stewart Baker, Assistant Secretary for Policy

OBJECTIVES/DESIRED OUTCOME OF MEETING:

- Establish an interagency negotiating position [

[b5 b2(high) b7E]

BACKGROUND:

- On May 30, 2006 the European Court of Justice (ECJ) ruled that the legal instrument the European Union utilized as a basis for entering into a 2004 agreement with DHS on CBP's access to PNR was inapplicable and required the EU to terminate the agreement by September 30, 2006. The EU has since provided notice that it is terminating the agreement effective that date.
- In issuing this ruling the ECJ held that the EU's 1995 directive on data protection in the first pillar does not apply to the transfer of PNR data which is a law enforcement (third pillar issue). Concern that U.S. law, and CBP's implementing PNR regulations conflicted with this directive was the basis for entering into the agreement in the first place. However, the ECJ did not comment on the sufficiency of DHS's efforts to protect privacy.
- However, the current arrangement does significantly impact DHS operations. In particular, the limitations on sharing and retention enshrined in the Undertakings have prohibited broader use of PNR within DHS to combat terrorism and crime. Most affected by this change has been ICE, [

[b5 b2(high) b7E]

Deleted: [
Deleted:
Deleted:
Deleted:
Deleted:
Deleted: b5
Deleted: [b5]
Deleted:
Deleted:
Deleted:]

- b1

Deleted: [b5]

- b1

Deleted: [b5]

FOR OFFICIAL USE ONLY

000275

384

(4)

b1

b1

Deleted

Deleted b5

PARTICIPANTS:
Non-DHS

DHS
Deputy Secretary Jackson

PRESS PLAN: "Closed"

ATTACHMENTS:

A. Discussion Document: Analysis of United States Interests in the U.S.-EU PNR dialogue (7/13/06)
B. Memo: Summary of Potential Changes to the Undertakings (*PENDING*)
C. Member State Positions known as of 7/20/06
D. Background on EU views of consent as a solution
E. DHS' Response Options to European Court of Justice Decision (February 2006)

Prepared by: Michael Scardaville, PDEV. C b2 (low) 3

Prioritized Issues:

1. b1

2. b1

3. b1

Operationally, CBP has provided carriers 3 options for making PNR data available: 1.) Pull; 2.) Real-time push (data is transmitted upon creation or at 72 hours before the flight and any changes must be sent at the time they are made. or; 3.) A scheduled method under which carriers transmit PNR per a set schedule. Under this third option the carrier must provide CBP with a functional, automated means of obtaining PNR data outside of the scheduled pushes. Merely having a POC to call and request an independent push is insufficient.

b1

b1

4.

b1

5.

b1

b1

b1

6.

b1

7.

b1

8.

b1

9.

b1

UNCLASS

PNR Implementation: Short-Term Tasks

	Task	Point of contact	Deadline	Date completed
1.	Components will determine which personnel require immediate access to PNR data. Components will report the names and total number to CBP.	• CBP; • ICE; • I&A; • TSA;	7 days	
2.	Each component will designate a data-access point of contact and provide to CBP. CBP will provide the name of its POC to other components.	• CBP; • ICE; • I&A; • TSA;	7 days	
3.	An IT group, comprising representatives from CBP and other components, will be convened to resolve all technical issues surrounding access to PNR data.	• CBP; • ICE; • • TSA;	7 days	
4.	CBP OCC will draft a request letter template for use by other components seeking access to PNR/ATS-P. The letter will include, among other things, a description of the purpose for which the request is being made (by office or individual as appropriate), the number and names of individuals to receive access, a POC for managing the component's access including enforcing accountability for use, and training requirements.	• CBP;	7 days	

b 6
b 2 (low)

6

000384

UNCLASS

	Task	Point of contact	Deadline	Date completed
5.	CBP OCC will draft a request approval letter detailing the obligations the agency and its officers accept by accessing the system, POCs for scheduling training, etc.	• CBP;	7 days	
6.	Components will send memos to CBP requesting access to PNR data.	• ICE; • I&A; • TSA;	14 days	
7.	CBP will ensure that existing audit mechanisms are capable of monitoring the use and potential misuse of PNR by other components. *CBP advises that, for components that will use CBP's existing interface, no changes to the current audit mechanism will be needed;* [b2 (High)]	• CBP; • ICE; • I&A; • TSA;	14 days	
8.	CBP will revise its rules and field guidance regarding access to the PNR database to reflect that personnel from across DHS now will have access. Such guidance should instruct individuals seeking direct access to contact CBP's central POC.	• CBP;	14 days	
9.	Notice of the new PNR uses will be published in the Federal Register.	• OGC; • Privacy; Hugo Teufel;	14 days	

b6 b2 (Low)

000385

	Task	Point of contact	Deadline	Date completed
10.	[b2(High) b7E]	• CBP; • ICE; • I&A; • TSA:	45 days needed to order, install, and implement new equipment and features	
11.	[b2(High) b7E]	• CBP; • ICE; • I&A; • TSA:	14 days (if there is a current connection); 90 days if there is no current connection or a poor connection)	
12.	CBP will send the components replies that grant access to PNR data. These replies will specify that all personnel will be subject to the same policies and procedures that govern CBP personnel access to PNR (including disciplinary policies for improper uses of PNR data). CBP will attach copies of the guidelines and policies it maintains with respect to PNR access.	• CBP:	14days	
13.	CBP will establish accounts and passwords for new users from other components.	• CBP; • ICE; • I&A; • TSA;	14 days	

b6 b2(Low)

000386

	Task	Point of contact	Deadline	Date completed
14.	CBP will provide training to component personnel who have access to PNR data.	• CBP; • TSA: [b6 b2(low)]	21 days	
15.	CBP will make available to other components its mechanism for restoring the PNR user accounts that have gone dark after 90 days of inactivity.	• CBP; [b6 b2(low)]	21 days	

UNCLASS

3 wks

PNR Implementation: Short-Term Tasks

Go-ahead given 10/6/2006

[b6]

	Task	Point of contact	Deadlii	ate pleted
1.	Components will determine which personnel require immediate access to PNR data. Components will report the names and total number to CBP.	• CBP; • ICE; ✓ I&A: Jona • TSA;	7 days (10/13)	
2.	Each component will designate a data-access point of contact and provide to CBP. CBP will provide the name of its POC to other components.	• CBP; • ICE; ✓ I&A; • TSA;	7 days (10/13)	
3.	An IT group, comprising representatives from CBP and other components, will be convened to resolve all technical issues surrounding access to PNR data. The IT group will have an initial organizational meeting.	• CBP; • ICE; • I&A; • TSA;	7 days (10/13)	
4.	CBP OCC will draft a request letter template for use by other components seeking access to PNR/ATS-P. The letter will include, among other things, a description of the purpose for which the request is being made (by office or individual as appropriate), the number and names of individuals to receive access, a POC for managing the component's access including enforcing accountability for use, and training requirements. CBP will share the draft with the components.	• CBP; • ICE; • I&A; • TSA;	7 days (10/13)	

b6
b2(low)

000388

UNCLASS

	Task	Point of contact	Deadline	Date completed
5.	CBP OCC will draft a request approval letter detailing the obligations the agency and its officers accept by accessing the system. POCs for scheduling training, etc. CBP will share the draft with the components.	• CBP; • ICE: • I&A: • TSA;	7 days (10/13)	
6.	Components will send the letters to CBP requesting access to PNR data.	• CBP • ICE • I&A; • TSA	14 days (10/20)	
7.	CBP will ensure that existing audit mechanisms are capable of monitoring the use and potential misuse of PNR by other components. *CBP advises that, for components that will use CBP's existing interface, no changes to the current audit mechanism will be needed.* b2 (High)	• CBP; • ICE: • I&A • TSA;	14 days (10/20)	
8.	CBP will revise its rules and field guidance regarding access to the PNR database to reflect that personnel from across DHS now will have access. Such guidance should instruct individuals seeking direct access to contact CBP's central POC.	• CBP;	14 days (10/20)	
9.	Notice of the new PNR uses will be published in the Federal Register.	• OGC; • Privacy; Hugo Teufel;	14 days (10/20)	

b6 b7(low)

000383

UNCLASS

	Task	Point of contact	Deadline	Date completed
10.	[b2(High) b7E]	• CBI • ICE • I&A; • TSA;	45 days needed to order, install, and implement new equipment and features (11/20)	
11.	[b2(High) b7E]	• CBP • ICE; • I&A; • TSA;	14 days if a current connection (10/20); 90 days if no current connection or poor connection (1/4/07)	
12.	CBP will send the components replies that grant access to PNR data. These replies will specify that all personnel will be subject to the same policies and procedures that govern CBP personnel access to PNR (including disciplinary policies for improper uses of PNR data). CBP will attach copies of the guidelines and policies it maintains with respect to PNR access.	• CBP • ICE; • I&A; • TSA;	14days (10/20)	
13.	CBP will establish accounts and passwords for new users from other components.	• CBP; • ICE; • I&A; • TSA;	14 days (10/20)	

b2(Low) b6

UNCLASS

	Task	Point of contact	Deadline	Date completed
14.	CBP will provide training to component personnel who have access to PNR data.	• CBP; • TSA;	b4	21 days (10/27)	
15.	CBP will make available to other components its mechanism for restoring the PNR user accounts that have gone dark after 90 days of inactivity.	• CBP:	b2(low)	21 days (10/27)	

UNCLASS

cc.1.2

PNR Implementation: Short-Term Tasks

Go-ahead given 10.6.2006

	Task	Point of contact	Deadline	Date completed
1.	Components will determine which personnel require immediate access to PNR data. Components will report the names and total number to CBP.	• CBP; • ICE: • I&A: • TSA;	7 days (10/13)	
2.	Each component will designate a data-access point of contact and provide to CBP. CBP will provide the name of its POC to other components.	• CBP; • ICE; • I&A: • TSA;	7 days (10/13)	
3.	An IT group, comprising representatives from CBP and other components, will be convened to resolve all technical issues surrounding access to PNR data. The IT group will have an initial organizational meeting.	• CBP; • ICE: • I&A: • TSA;	7 days (10/13)	
4.	CBP OCC will draft a request letter template for use by other components seeking access to PNR/ATS-P. The letter will include, among other things, a description of the purpose for which the request is being made (by office or individual as appropriate), the number and names of individuals to receive access, a POC for managing the component's access including enforcing accountability for use, and training requirements. CBP will share the draft with the components.	• CBP; • ICE: • I&A; • TSA;	7 days (10/13)	

b6
b2(low)

1

000392

UNCLASS

	Task	Point of contact	Deadline	Date completed
5.	CBP OCC will draft a request approval letter detailing the obligations the agency and its officers accept by accessing the system, POCs for scheduling training, etc. CBP will share the draft with the components.	• CBP • ICE; • I&A • TSA	7 days (10/13)	
6.	Components will send the letters to CBP requesting access to PNR data.	• CBP • ICE; • I&A; • TSA	14 days (10/20)	
7.	CBP will ensure that existing audit mechanisms are capable of monitoring the use and potential misuse of PNR by other components. *CBP advises that, for components that will use CBP's existing interface, no changes to the current audit mechanism will be needed.* [b2(High)]	• CBP • ICE: • I&A; • TSA;	14 days (10/20)	
8.	CBP will revise its rules and field guidance regarding access to the PNR database to reflect that personnel from across DHS now will have access. Such guidance should instruct individuals seeking direct access to contact CBP's central POC.	• CBP;	14 days (10/20)	
9.	Notice of the new PNR uses will be published in the Federal Register.	• OGC; • Privacy; Hugo Teufel	14 days (10/20)	

b6
b2(low)

	Task	Point of contact	Deadline	Date completed
10.	[b2(High) b7E]	• CBP • ICE; • I&A; • TSA;	45 days needed to order, install, and implement new equipment and features (11/20)	
11.	[b2(High) b7E]	• CBP • ICE; • I&A; • TSA	14 days if a current connection (10/20); 90 days if no current connection or poor connection (1/4/07)	
12.	CBP will send the components replies that grant access to PNR data. These replies will specify that all personnel will be subject to the same policies and procedures that govern CBP personnel access to PNR (including disciplinary policies for improper uses of PNR data). CBP will attach copies of the guidelines and policies it maintains with respect to PNR access.	• CBP • ICE; • I&A; • TSA	14days (10/20)	
13.	CBP will establish accounts and passwords for new users from other components.	• CBP • ICE; • I&A; • TSA;	14 days (10/20)	

b6
b2(low)

UNCLASS

	Task	Point of contact	Deadline	Date completed
14.	CBP will provide training to component personnel who have access to PNR data.	• CBP; • TSA;	21 days (10/27)	
15.	CBP will make available to other components its mechanism for restoring the PNR user accounts that have gone dark after 90 days of inactivity.	• CBP;	21 days (10/27)	

[b6 b2(low)]

UNCLASS

CONFIDENTIAL

DISCUSSION DOCUMENT
DHS Objectives and Critical Factors in Renegotiating the US-EU PNR Arrangement
Department of Homeland Security

[b2]

(u) 1. *Issue:* To establish a negotiating position for the United States government in discussions with the European Union on a replacement PNR arrangement

(c) 2.

b1

3. *DHS Objectives:*

(c)

(c)

b1

(c)

000477

Derived: Schneider MFR
Declassify: (45)
12 Sept 2008

9

CONFIDENTIAL

(c)

(c)

b1

(c)

(c)

(c)

(c)

(c)

•

b1

(c)

4. *Other Important Factors:*

•

(c)

•

(c)

b1

•

(c)

•

(c)

b1

5. *Suggested Approach:*

(c)

(c) 1.

(c) b1

(c) 2.

(c) 3.

(c) 4.

(c)

DISCUSSION DOCUMENT

DHS Objectives and Critical Factors in Renegotiating the US-EU PNR Arrangement
Department of Homeland Security

[b2]

(U) 1. *Issue:* To establish a negotiating position for the United States government in discussions with the European Union on a replacement PNR arrangement

2.

(C) b1

3. *DHS Objectives:*

(C)

(C) b1

(C)

(c)

(c

b1

(c

(c)

(c)

(c)

(c)

(c) b1

4. *Other Important Factors:*

(c)

(c) b1

(c)

(c)

b1

5. *Suggested Approach:*

(c)

(c) b1

2.
(c)

3.
(c)

4.
(c)

(c)

CONFIDENTIAL

DISCUSSION DOCUMENT

DHS Objectives and Critical Factors in Renegotiating the US-EU PNR Arrangement
Department of Homeland Security

[b2]

Deleted: August 31, 2006

(u) 1. *Issue:* To establish a negotiating position for the United States government in discussions with the European Union on a replacement PNR arrangement

2.

(c) b1

3. *DHS Objectives:*

(c)

(c) b1

(c)

Deleted:
Deleted:
Deleted:
Deleted:
Comment

b5

Deleted:
Deleted:

000485

Derived: Schneider MFR
Declassify: 17 Aug. 2022

299.1

(u)

CONFIDENTIAL

(c)

(c)

(c)

(c)

(c)

(c)

(c)

Deleted: [b5]

b1

(c)

b1

(c)

4. *Other Important Factors:*

(c)

(c)

b1

(c)

(c)

b1

(c)

5. *Suggested Approach:*

(c)

(c) 1.

(c) 2.

b1

(c) 3.

(c) 4.

(c)

CONFIDENTIAL

DISCUSSION DOCUMENT

DHS Objectives and Critical Factors in Renegotiating the US-EU PNR Arrangement
Department of Homeland Security

September 1, 2006

Deleted: September 1, 2006
Deleted: August 31, 2006

1. *Issue:* To explain DHS objectives and establish a negotiating position for the United States government in discussions with the European Union on a potential replacement PNR arrangement

(a)

2.

(c) b1

3. *DHS Objectives:*

(c)

Deleted: [b5]

(c) b1

b1

(c)

Deleted: [b5]

[1] Paragraphs 3 (through the narrow use definition), 17, 28 and 31.
[2] Paragraph 15.

000483

Derived: Schneider MFR
Declassify: 1 Sept. 2021

(12)

CONFIDENTIAL

(302)

Comment

Deleted: b5

Deleted:

(c)

b1

Deleted:
Deleted: [b5]
Deleted:

(c)

(c)

Deleted:
Deleted. [b5]
Deleted:

Formatted: Font: Italic

Formatted: Bullets and Numbering

(c)

b1

[1] Paragraphs 6 and 43 and 45 respectively. Paragraph 6 of the Agreement and 45 of the Undertakings oblige DHS to encourage U.S carriers to comply with an EU system without mention of assurances by the EU. Paragraph 43 of the Undertakings obligates DHS to host a joint review for European authorities to monitor DHS compliance. [b5]

[2] Paragraphs 5 and 14.

[3] Paragraph 13 of the Undertakings and paragraph 1 of the agreement

[4] Paragraphs 4 and 5

(c)

b1

Formatted: Indent: Left: 0"

Formatted: Font: Italic

Formatted: Indent: Left: 0", First line: 0.5"

Comment

[b5]

c

(c)

b1

b1

(c)

Formatted: Font: Not Italic

Deleted:

Deleted: [b5]

Formatted: Font: Italic

Formatted: Bullets and Numbering

c

b1

(c)

Formatted: Font: Italic

Formatted: Font: Italic

Comment

Deleted: [b5]

c

b1

Page 3: [1] Deleted sb 9/1/2006 7:40:00 AM

(c) b1

Page 3: [2] Comment [m4] michael.scardaville 9/1/2006 9:50:00 AM

(c) b1

Page 3: [3] Deleted sb 9/1/2006 7:51:00 AM

Other Important Factors:

(c)

(c) b1

(c)

(c) b1

Suggested Approach:

Page 3: [4] Deleted SD 9/1/2006 7:51:00 AM

(c)

(c) b1

(c)

(c)

(c)

(c)

CONFIDENTIAL

DISCUSSION DOCUMENT
DHS Objectives and Critical Factors in Renegotiating the US-EU PNR Arrangement
Department of Homeland Security

(b2)

Deleted: August 31, 2006

1. *Issue:* To establish a negotiating position for the United States government in discussions with the European Union on a potential replacement PNR arrangement

(u)

2.

(c) b1

3. *DHS Objectives:*

(c)

(c) b1

(c)

Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Terrorism i
Deleted:
Deleted:
Deleted:
Deleted:
Comment

b5

Deleted:

000431

Declassified Schneider MFI
Declassify. 17 Aug 2022

(13)

CONFIDENTIAL

300.1

Deleted

Deleted

Deleted

Deleted

(c)

b1

Deleted:

Deleted:

Deleted:

b5

Deleted:

(c)

Deleted:

Deleted:

Deleted:

Deleted:

b5

(c)

Deleted:

(c)

(c)

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

(c)

b1

(c)

4. *Other Important Factors.*

(c)

(c)

b1

(c)

Deleted:
Deleted:
Deleted:
Deleted:

b5

Deleted:

000436

Deleted

Deleted
Deleted

Deleted:
Deleted:
Deleted:

b1

(c)

b5

5. *Sugge d Approach:*

(c)

Deleted:

1.

(c)

b1

(c) 2.

(c) 3.

(c) 4.

(c)

b1

CONFIDENTIAL

DISCUSSION DOCUMENT
DHS Objectives and Critical Factors in Renegotiating the US-EU PNR Arrangement
Department of Homeland Security

September 1, 2006

1. *Issue:* To explain DHS objectives and establish a negotiating position for the United States government in discussions with the European Union on a potential replacement PNR arrangement

(u)

2.

(c) b1

3. *DHS Objectives:*

[b5]

(c)

(c) b1

(c)

000439

[1] Paragraphs 3 (through the narrow use definition), 17, 28 and 31.
[2] Paragraph 15.

Derived: Schneider MF
Declassify: 1 Sept. 2021

CONFIDENTIAL

14

304

(c)

b)

(c)

(c)

(c) *a.*

b.

c.

(c) (c) (c) b1 b1

[3] Paragraphs 6 and 43 and 45 respectively. Paragraph 6 of the Agreement and 45 of the Undertakings oblige DHS to encourage US carriers to comply with an EU system without mention of assurances by the EU. Paragraph 43 of the Undertakings obligates DHS to host a joint review for European authorities to monitor DHS compliance. [65]

[4] Paragraphs 5 and 14.

[5] Paragraph 13 of the Undertakings and paragraph 1 of the agreement

[6] Paragraphs 4 and 5

(c)

(c)

b1

(c)

(c)

a.

b.

c.

DISCUSSION DOCUMENT

DHS Objectives and Critical Factors in Renegotiating the US-EU PNR Arrangement
Department of Homeland Security

September 1, 2006

1. *Issue:* To explain DHS objectives and establish a negotiating position for the United States government in discussions with the European Union on a potential replacement PNR arrangement

(u)

2.

(c) b1

3. ~~*DHS Objectives:*~~ [b5]

(c).

(c) b1

(c)

[1] Paragraphs 3 (through the narrow use definition), 17, 28 and 31.
[2] Paragraph 15.

(15)

C006533

Derived: Schneider MFR
Declassify: 15 Sept. 2021

303

(c) b1

(c)

(c)

(c)

(c)

[b5]

(c)

[1] Paragraphs 6 and 43 and 45 respectively. Paragraph 6 of the Agreement and 45 of the Undertakings oblige DHS to encourage US carriers to comply with an EU system without mention of assurances by the EU. Paragraph 43 of the Undertakings obligates DHS to host a joint review for European authorities to monitor DHS compliance. [b5]

[2] Paragraphs 5 and 14.

[3] Paragraph 13 of the Undertakings and paragraph 1 of the agreement

[4] Paragraphs 4 and 5