COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.12.2005
COM (2005) final

COMMISSION STAFF WORKING PAPER ON THE JOINT REVIEW

of the implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004

Redacted version

Washington, 20-21 September 2005

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Following the tragic events of 11 September 2001, 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. Bureau of Customs and Border Protection ('CBP') personal data contained in the Passenger Name Record ('PNR') of air passengers. In June 2002 the Commission informed the U.S. authorities that these requirements could conflict with Community and Member States' legislation on data protection, in particular the Data Protection Directive, which imposes conditions on the transfer of personal data to third countries. 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. A set of conditions on the processing of such data by CBP, so-called Undertakings, were agreed between the EU and the U.S., which ensure an adequate level of protection of the PNR data by the U.S. authorities. In particular they provide for an annual Joint Review of the implementation by CBP of these Undertakings.

Prior to the Joint Review the Privacy Office of the Department of Homeland Security ('DHS') proceeded with an internal review of the implementation by CBP of the Undertakings.

In order to conduct the Joint Review in the best possible way, a methodology has been developed by the Commission and DHS, in close co-operation with the EU data protection authorities, which consists of:

- An EU Joint Review team ('the EU team'), whose members had particular expertise with border controls, the role of PNR data, the use of databases and extensive experience in conducting data protection compliance audits;

- an EU questionnaire;

- field visits to CBP operations by the EU team;

- a day's meeting between CBP, the EU team and the DHS Privacy Office discussing in detail the implementation of the various Undertakings.

The EU members of the Joint Review found that, as of the date of the Joint Review (20 and 21 September 2005), CBP is in substantial compliance with the conditions set out in the Undertakings. The EU team also found that it took some time before compliance was achieved, and that CBP had received substantial assistance to achieve compliance from the DHS Privacy Office.

For example, there is compliance as of 14 March 2005 with regard to real-time filtering of sensitive data, flight filtering and filtering of data beyond the 34 permitted PNR data elements. Moreover, retro-active deletion of data received before 14 March 2005 was completed on 19 August 2005.

There is compliance with the Undertakings on passenger rights as of 16 May 2005, when CBP introduced a policy enabling to track requests, including complaints, from the public in relation to EU PNR data.

As of 13 May 2005 CBP is able to differentiate between accessing PNR for automated purposes and accessing PNR for manual purposes, which amongst other things, has a direct bearing on the application of the various data retention periods mentioned in the Undertakings.

The EU team also identified some areas for improvement and monitoring. In particular, CBP is invited to provide clearer guidance to CBP officers as to the meaning and interpretation of the notion of 'serious crimes that are transnational in nature'. During the Joint Review CBP raised its intention to retain some sort of "pull system" even after the change to a "push system" in case CBP needs PNR data prior to 72 hours before a flight's scheduled departure. Notwithstanding the fact that other parties are involved, CBP should more actively contribute to finding acceptable solutions for the implementation of a 'push' system by air carriers without delay in a manner fully consistent with the requirements of the Undertakings, as promises have been made to the Commission by the parties involved that a full functioning "push" system would be in place by the end of 2005.

Information to passengers should be improved, in particular access to information on the handling of PNR data.

The EU team identified two areas where for a considerable amount of time CBP was not in compliance with the Undertakings and where remedial action for the periods concerned is not possible:

The first area concerns Undertaking 5. This Undertaking allows CBP officers to manually review the full 'OSI' (general remarks) and 'SSI/SSR' fields (open fields) only if the passenger has been identified by CBP as high risk in relation to the purposes for which the PNR data have been requested. From 28 May 2004 to 14 March 2005 CBP could not distinguish between automated access of these fields and manual review by CBP officers. This means that for that period CBP is not in a position to demonstrate such data were only manually reviewed for individuals identified by CBP as high risk. Measures have been introduced since 14 March 2005 to address this issue, but the omission cannot be remedied for the period concerned.

The second area concerns passenger rights, where until 16 May 2005 CBP was not able to identify requests and complaints related to EU PNR data. This means that CBP was not in a position to tell the EU team whether or not it received requests and complaints from passengers in relation to EU PNR data during that period. Measures have been introduced since 16 May 2005 to solve this problem, but this omission cannot be remedied for the period concerned.

The EU team also found that at some instances CBP went significantly beyond, or intends to go beyond, what is necessary in order to comply with the Undertakings. CBP namely installed technology that will track disclosure of PNR data and monitor manual access to such data. CBP also undertook to delete by January 2006 at the latest any sensitive data received between March 2003 and May 2004 following the Joint Statement in February 2003, although the Joint Review was not concerned with this period.

The present report has received the unanimous agreement of the members of the EU team. There was also unanimous agreement between the members with regard to the methodology and the conclusions of the Joint Review.

1. INTRODUCTION AND BACKGROUND

This chapter provides an overview of the background which led to this EU-U.S. joint monitoring exercise, whereas chapter 2 describes the objective, scope and methodology of the Joint Review.

Chapter 3 contains an overview of the EU team's findings, including recommendations to CBP.

Comprehensive information upon which the findings are based with regard to each of the Undertakings can be found in Annex 1. This annex reproduces the analytical framework - an inventory of questions - that was used as a guide to gather information previous to and during the Joint Review.

Chapter 4 presents the overall conclusion of the EU team, including an assessment of the methodology used for monitoring the implementation of CBP Undertakings.

The Commission services would like to acknowledge the professional and constructive assistance it received from representatives from EU national data protection and law enforcement authorities who were members of the EU team. The Commission services benefited from their experiences and suggestions during the preparations and while conducting the Joint Review in Washington. Their assistance helped to perform a correct Joint Review.

Prior to the Joint Review the DHS Privacy Office proceeded with an internal review of the implementation by CBP of the Undertakings. This report covers a review of the Undertakings conducted from November 2004 to September 2005. The Commission services and the EU team want to acknowledge the excellent cooperation with the DHS Privacy Office during the preparations of the Joint Review and during the in-person meetings in Washington. The Commission services intend to continue to work closely with the Privacy Office in order to enhance international data protection standards. The EU team would also like to thank the U.S. CBP officials who gave generously of their time during the review visit.

The present report has received the unanimous agreement of the members of the EU team. There was also unanimous agreement between the members with regard to the methodology and the conclusions of the Joint Review.

The Joint Review is part of the PNR package concluded in May 2004, forming part of the system of administrative review and control. On 28 May 2004 the European Community and the United States of America entered into an agreement on the processing and transfer of Passenger Name Record[1] (hereafter "PNR") data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (hereafter "CBP").[2] The same day a Commission Decision entered into force which states that CBP ensures an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States, in accordance with Undertakings set out in an

[1]Passenger Name Record is a record of each passenger's travel requirements which contain all information necessary to enable reservations to be processed and controlled by airlines.
[2] Council Decision of 17 May 2004, OJ L 183/83, 20.05.2005.

annex to the Decision.[3] The Decision was taken on the basis of Article 25(6) of Directive 95/46/EC[4] (hereafter "the Data Protection Directive"), which authorises the Commission to issue so-called adequacy decisions. It contains a set of conditions on the processing of PNR data by CBP, so-called Undertakings.

These instruments form a package aimed at reconciling the competing demands of European and U.S. law on the transfer of air passenger data. As part of its response to the tragic events of 11 September 2001 the U.S. enacted a statute[5] in November 2001 and implementing regulations[6] requiring each air carrier operating passenger flights to and from the United States to transfer to CBP personal data contained in the PNR of air passengers. In June 2002 the Commission informed the U.S. authorities that these requirements could conflict with Community and Member States' legislation on data protection, in particular the Data Protection Directive, which imposes restrictions on the transfer of personal data to third countries.

On 18 February 2003, the Commission and the U.S. administration issued a Joint Statement, setting out initial data protection conditions agreed by the then U.S. Customs. On 28 May 2004 the current agreement entered into force. The Joint Review is not concerned with the period following the Joint Statement until the entry into force of the PNR package.

2. PURPOSE, SCOPE AND METHODOLOGY OF THE JOINT REVIEW

The purpose of the Joint Review is spelt out in Undertaking 43, which says that once a year a joint review will be conducted on the implementation by CBP of the Undertakings with a view to "mutually contributing to the effective operation of the processes described in these Undertakings".

The Joint Review clearly is not an inspection of CBP's PNR policies and the EU team had no investigative powers, which means that the Joint Review has its limits in terms of what it can achieve. The EU team has conducted the Joint Review in close co-operation with CBP and DHS on the basis of its understanding of Undertaking 43, namely that the review should provide insight to CBP rules and processes in place in a way which would allow the EU team to arrive at a solid conclusion on the level of compliance by CBP with the Undertakings. It was disappointing that understandable concerns about law enforcement sensitivities meant that there were limitations imposed on the number of records that could be accessed and on the provision of hard copy versions of certain staff procedural guidance. This review report is written in the context of those limitations and the findings should be read in this perspective. The limitations were particularly regrettable as all members of the EU team were required to sign confidentiality agreements exposing them to criminal sanctions for any breach. Hopefully the mutual confidence that has been built between the EU team and their US counterparts during this review will help to allay any such concerns to the benefit of future reviews.

[3] Commission Decision of 14 May 2004, OJ L 235/11, 06.07.2004.
[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.1995. Article 25 of the Directive contains provisions relating to transborder data flow to third countries.
[5] Titel 49, United States Code, section 44909(c(3).
[6] Titel 19, Code of Federal Regulations, section 122.49b.

The Joint Review did not consider the issue of the outlook for the agreement with the U.S. or the legality of the Undertakings as part of the Commission Adequacy Decision. The agreement will come up for re-negotiation in 2007. It was felt that this Joint Review should focus entirely on the implementation of the Undertakings by CBP.

To assess the efforts taken by CBP to implement the Undertakings annexed to the Commission Adequacy Decision, the following methodology has been developed by the Commission and DHS, in close co-operation with the EU data protection authorities:

(1) An EU team especially composed for the Joint Review, comprising Commission officials, including a member of its anti-fraud division OLAF, and representatives from Member States data protection and law enforcement authorities. The law enforcement members and the OLAF representative had particular expertise with border controls, the role of PNR data and the use of databases. The data protection members had extensive experience in conducting data protection compliance audits. This composition enabled the team to call upon its members' legal, data protection, law enforcement and technical expertises.

(2) A questionnaire based on the Undertakings, setting out in detail questions to be asked and issues to be raised with CBP in relation to each Undertaking;

(3) Field visits to CBP operations, allowing the EU team real-time access to live data; these visits also allowed the EU team members to speak to CBP officers in person;

(4) A whole-day meeting aimed at discussing in detail the measures taken and the procedures put in place to oversee and manage the Undertakings as part of CBP's PNR policy; the meeting was held after the field visits allowing the EU team to take into consideration the information gathered during the field visits.

The PNR arrangements consist of a number of components which form the core of the data protection provided by the Undertakings. These are the following:

(a) purpose limitation,

(b) data limitation,

(c) deletion of sensitive data,

(d) data retention periods,

(e) access limitations,

(f) onward transfers limitations,

(g) specific passenger rights.

To assess the efforts being taken by CBP on any of these issues as well as on other data protection conditions set out in the Undertakings, the EU team engaged in talks with CBP officials in the field, reviewed documentation including specific PNR files which had given rise to further investigations in relation to terrorism and serious crimes, obtained information on the way CBP deals with passenger rights at the airport, reviewed audit trails on issues like user access to PNR files, reviewed access arrangements and filtering, and last but not least

discussed in detail with CBP officials which are key stakeholders for implementing the Undertakings the entire set of data protection obligations.

The following Undertakings were not discussed in detail:

a) Undertaking 43 concerns the Joint Review itself and thus does not has to be dealt with separately.

b) Undertaking 44 on CBP issuing policy documents to ensure compliance with the Undertakings has not been dealt with separately but in relation to the above-mentioned categories whenever relevant.

c) Undertakings 45 on reciprocity, 46 on review and termination of the Undertakings and 48 on precedents have not been dealt with since they do not impose operational obligations on CBP.

3. THE OUTCOME OF THE JOINT REVIEW

3.1. Findings of the EU Joint Review Team

This heading describes the various findings in more detail. The reasons for these findings can be found in Annex 1 which contains the inventory of questions used as a guide for the review.

In order to comply with the various obligations set out in the Undertakings, CBP had to adapt existing policies, procedures and information technology to accommodate these obligations or implement new policies, procedures and technologies focused on EU PNR data.

On the basis of extensive discussions with CBP officials, the EU questionnaire and the internal review of the DHS Privacy Office, the EU team can report the following findings:

General finding

- There is substantial compliance with the Undertakings as of the date of the Joint Review (20-21 September 2005), but it was late compliance since the PNR agreement with the U.S. entered into force on 28 May 2004. For this reason the conclusion can be drawn that there was no sufficient degree of compliance with the Undertakings until mid-May 2005, after CBP had started implementing measures in March and May 2005, allowing it to respect core obligations on access and data limitation, deletion of sensitive data and passenger rights.

  The report from the DHS Privacy Office indicates at page 13 that "while full implementation was presumed to necessarily take some period of time to achieve, the actual timeline for reaching this level of consistency with U.S. representations to the EU has taken much longer than expected, nearly a year since issuance of the PNR agreement." The report does not provide concrete indications why it took CBP such a long time to implement the Undertakings.

  The EU team received some explanations on this issue from CBP during the review. CBP did not advance specific reasons but explained that its information technology (IT) system, used by CBP officers throughout the U.S., needs to parse and format PNR data it receives from over 117 airlines into a single format before they can be used. The airlines provide

CBP with 'raw data', since the PNR data obviously are not formatted by airlines in a way which assists CBP officers in identifying high risk passengers. The way PNR data are presented by airlines may also differ from one airline to the other. CBP thus needed a considerable amount of time and financial investment to build the necessary IT capability.

CBP also explained that, in order to accommodate the various requirements set out in the Undertakings in connection with EU flights, additional IT solutions including substantial changes to its IT system had to be developed, tested and implemented. This required working closely together with other offices, such as the Office of Field Operations and the Chief Counsel Office to create the necessary technological measures ensuring implementation and enforcement of the Undertakings.

The EU team considers that the explanations provided by CBP for late compliance indicate that CBP could have been more pro-active to ensure earlier compliance with the Undertakings. However, this does not invalidate the EU team's conclusion that CBP is in substantial compliance with the Undertakings as of the date of the Joint Review (20-21 September 2005).

Detailed findings

- The Commission and CBP agreed on 3 November 2004 on a series of sensitive terms and codes in view of filtering out these codes and terms to the extent they may appear in open fields and in other parts of a passenger's PNR. On **14 March 2005**, CBP implemented a filtering system providing for flight filtering, filtering of data beyond the maximum of 34 permitted PNR data elements and filtering of sensitive data, in the sense that data which are filtered out are completely taken out from CBP's system. This allowed CBP to be in compliance with a number of core components of the Undertakings listed above, namely those on data limitation and deletion of sensitive data.

  CBP did not provide specific explanations why a filtering system became operational only on 14 March 2005. Members of the EU team reviewed the filtering system and could confirm that it is in place and working properly.

  Also since that date, CBP's system is able to track manual access of 'OSI' (general remarks) and 'SSI/SSR' (open fields) data elements. This allowed CBP to be in compliance with the core component on access limitations. CBP's attention was drawn to this deficiency by the Privacy Office during its review of CBP's audit logs.

- On **13 May 2005** CBP became able to differentiate between accessing PNR for automated purposes and accessing PNR for manual purposes. This is of great importance, since the capacity to distinguish between the two purposes bears a direct consequence on the period during which EU PNR data may be retained. This will thus be of importance in relation to compliance by CBP with the rules on data retention periods.

  Again, it was the Privacy Office who drew CBP's attention to this deficiency in its IT system upon which CBP undertook to remedy the situation.

- **On 16 May 2005**, CBP introduced a policy enabling it to track requests, including complaints, from the public related to EU PNR data. On the same day CBP also applied additional guidance enabling CBP staff to differentiate FOIA request related to PNR. This allowed CBP to be in compliance with the core component on passenger rights.

The implementation of this policy was the result of the Privacy Office's finding that CBP's IT system could not differentiate between requests and complaints specific to EU data and those related to personal data in general. CBP undertook to remedy this situation. As of 16 May 2005 CBP was in a position to tell whether or not it did receive requests or complaints related to EU PNR data. CBP informed the EU team it has not received any such requests or complaints.

- On **19 August 2005**, CBP completed the permanent deletion of the data elements beyond the 34 data elements, collected between 28 May 2004 and 14 March 2005. On the same day the permanent deletion of sensitive data, collected during the same period, was completed also. This allowed CBP to be in full compliance with the requirements on data limitation and deletion of sensitive data.

  CBP gave no other specific explanation why it took them until mid-August to delete the data collected before implementation of real-time filtering on 14 March 2005, except for the technical complexity to put the necessary IT-systems in place.

Areas of concerns

The EU team identified two areas where for a considerable amount of time CBP was not in compliance with the Undertakings and where remedial action for the periods concerned is not possible.

- First, Undertaking 5 was not fully implemented over the period from 28 May 2004 to 14 March 2005 in that CBP could not identify manual reviews of 'OSI' (general remarks) and 'SSI/SSR' fields (open fields) by CBP officers. This means that for that period CBP is not in a position to show such data were only manually viewed for individuals identified by CBP as presenting a high risk. Measures have been introduced to address this issue, but the omission cannot be remedied for the period concerned.

- The second area concerns passenger rights, where until 16 May 2005 CBP was not able to identify requests and complaints related to EU PNR data. This means that CBP was not in a position to tell the EU team whether or not it received requests and complaints from passengers in relation to EU PNR data during that period. Measures have been introduced to solve this problem, but this omission cannot be remedied for the period concerned.

Positive findings

The EU team also found that at some instances CBP went significantly beyond, or intends to go beyond, what is necessary in order to comply with the Undertakings. The EU team welcomes these efforts, since these measures contribute to an enhanced level of protection beyond the strict requirements of the Undertakings:

- In relation to the transfer of PNR data to other agencies than CBP, the latter replaced its paper-based process with an electronic tracking system, allowing CBP in particular to improve the way it notifies corrections of PNR data to those agencies. This change was completed on 14 September 2005.

- CBP introduced an additional audit mechanism in relation to approval given by senior CBP officials to CBP officers in case of manual access of PNR data. This change was also completed on 14 September 2005.

- At the Joint Review CBP undertook to permanently delete by January 2006 at the latest any sensitive data collected by CBP following the Joint Statement in February 2003 until entry into force of the PNR package on 28 May 2004, although the Joint Review was not concerned with this period.

3.2. Recommendations and monitoring

The DHS Privacy Office report indicates that upon conclusion of the Joint Review CBP will update field guidance in order to include recommendations that may be made by the Joint Review team. The EU team welcomes this approach and takes the opportunity to suggest a number of recommendations with an aim to seek improvement of CBP's compliance with the Undertakings.

The following areas for improvement were identified:

- If PNR data from EU flights without an U.S. nexus were collected by CBP between 28 May 2004 and 14 March 2005, the date at which CBP started flight filtering, these data should be permanently deleted.

- Provide clearer guidance to CBP officers as to the meaning and interpretation of the notion of 'serious crimes that are transnational in nature', which forms part of the purposes for which CBP may collect the PNR data as this is necessary to ensure respect of the purpose limitations agreed upon between the EU and the U.S..

- During the Joint Review CBP raised its intention to retain some sort of "pull system" even after the change to a "push system" in case CBP needs PNR data prior to 72 hours before a flight's scheduled departure. Notwithstanding the fact that other parties are involved, CBP should more actively contribute to finding acceptable solutions for the implementation of a 'push' system by air carriers without delay in a manner fully consistent with the requirements of the Undertaking, as promises have been made to the Commission by the parties involved that a full functioning "push" system would be in place by the end of 2005.

- Information to passengers should be improved, in particular access to specific information on the handling of PNR data on CBP's website.

Beside the above-mentioned areas for improvement, the EU team found a particular area for close monitoring:

- The implementation of the various data retention periods is identified as an area for close monitoring, because of CBP's difficulties to differentiate (i) between manually and electronically accessed PNR data and (ii) data related to law enforcement action for the period between 28 May 2004 and 14 May 2005. This has a direct consequence for the application of the data retention periods in the future.

4. CONCLUSION

The Joint Review proved to be a valuable and essential tool to assess the level of compliance by CBP of the Undertakings. It provided further insight into the use of EU PNR data and improved understanding of CBP's mission and the role EU PNR data have to fulfil this mission. The Joint Review is an essential mechanism because, in the EU team's experience, the possibility to see on the spot how data are being used, and to engage in direct dialogues with those working in the field, proved invaluable in gaining the most accurate picture of CBP's activities in this field.

The methodology established for the Joint Review enabled the EU team to obtain insight to CBP rules and processes in place in a way which allowed arriving at a solid conclusion on the level of compliance by CBP with the Undertakings. The questionnaire, completed by field visits and in-depth discussions with CBP officers proved to be the right mix of instruments available to the EU team within the limits a review of this kind sets.

The EU members of the Joint Review found that, as of the date of the Joint Review (20 and 21 September 2005), CBP is in substantial compliance with the conditions set out in the Undertakings. The EU team also found that it took some time before compliance was achieved, and that CBP had received substantial assistance to achieve compliance from the DHS Privacy Office. Some areas of concern were identified as well as some positive findings where CBP significantly went beyond what is necessary in order to comply with the Undertakings. In particular, at the Joint Review CBP undertook to permanently delete by January 2006 at the latest any sensitive data collected by CBP between March 2003 and May 2004 following the Joint Statement in February 2003, although the Joint Review was not concerned with this period.

The EU Joint Review team recommends CBP to provide its officers with clearer guidance as to the meaning and interpretation of the notion of 'serous crimes that are transnational in nature', to contribute more actively to the implementation of a 'push' system and to improve information to passengers on the transfer of PNR data.

The DHS Privacy Office report indicates that upon conclusion of the Joint Review CBP will update field guidance in order to include recommendations that may be made by the Joint Review team. The EU team welcomes this approach and hopes that the above-mentioned recommendations will be taken on board by CBP with an aim to further improve its compliance with the Undertakings.

The Commission hopes that this report and the experiences gained during the preparations and conduct of this Joint Review may contribute to ensure that the transfer of personal data to the United States is realised in a way which ensures appropriate data protection safeguards.

ANNEX 1

[Deleted]

ANNEX 2

EU and U.S. Joint Review Teams

EU Delegation list

Director, Commission Directorate General Justice, ***[name deleted]*** - Co-Chair

Head of Unit, Data Protection, Commission Directorate General Justice, ***[name deleted]***

Head of Unit, Fight Against Economic, Financial and Cyber Crime, Commission Directorate General Justice, ***[name deleted]***

Desk Officer Transport Issues, Data Protection Unit, Commission Directorate General Justice, ***[name deleted]***

Desk Officer Law Enforcement, Unit Fight Against Economic, Financial and Cyber Crime, Commission Directorate General Justice, ***[name deleted]***

Legal Advisor, Commission Legal Service, ***[name deleted]***

Special Investigator, Commission Anti Fraud Office OLAF, ***[name deleted]*** (currently on secondment from the UK HM Revenue & Customs)

Counselor, Head of Transport, Environment and Energy, Commission Washington Delegation, ***[name deleted]***

Counselor Justice and Home Affairs, Commission Washington Delegation, ***[name deleted]***

Assistant Commissioner, UK Data Protection Authority, ***[name deleted]***

Officer European and International Affairs, French Data Protection Authority, ***[name deleted]***

Data Protection Officer, German Federal Data Protection Authority, ***[name deleted]***

Inspector, UK Home Office, Immigration and Nationality Directorate, Policy and Strategy, e-Borders, ***[name deleted]***

Chief Superintendant, Head Federal Judicial Police Brussels Airport, Belgium Federal Police, ***[name deleted]***

U.S. Delegation list

DHS Chief Privacy Officer, ***[name deleted]*** – Co-Chair

DHS, Office of International Affairs, ***[name deleted]***

DHS Acting General Counsel, ***[name deleted]***

Acting Under Secretary for BTS, ***[name deleted]***

Acting Assistant Secretary, ***[name deleted]***

Policy Adviser, BTS, ***[name deleted]***

CBP Commissioner ***[name deleted]***

CBP Deputy Commissioner, ***[name deleted]***

CBP Director of Operations, ***[name deleted]***

CBP/Technical Operations, ***[name deleted]***

Director, Europe and Multilateral Affairs, DHS Office of International Affairs, ***[name deleted]***

DHS Privacy Office, Chief of Staff and Senior Advisor for International Privacy Policy, ***[name deleted]***

DHS Privacy Office, Director of Privacy Compliance, ***[name deleted]*** (Head of the Privacy Office Audit Team)

DHS, Privacy Office, Director of International Privacy Programs, ***[name deleted]***