



Homeland Security

Privacy Office, Mail Stop 0550

February 15, 2008

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

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

Dear Mr. Sobel:

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

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the redress that is available to individuals who believe that the ATS contains or utilizes inaccurate, incomplete or outdated information about them.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

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

Our November 7, 2007 letter summarized our processing of your request. Our searches directed to the DHS Office of the Executive Secretariat (ES), DHS Office of Policy (PLCY), DHS Privacy Office (PRIV), DHS Office of General Counsel (OGC), the Transportation Security Administration (TSA), and the U.S. Customs and Border Protection (CBP) have thus far produced a combined total of 1,704 pages. Out of those 1,704 pages, we provided you with a combined total of 1137 pages with certain information withheld pursuant to the FOIA. We are continuing to process your request within CBP.

A search directed to CBP has produced an additional 474 pages of records responsive to your request. We have determined that 100 pages are releasable to you with certain information withheld pursuant to Exemptions 1, 2 (low), 5 and 6 of the FOIA, and 374 pages are withheld in their entirety pursuant to Exemptions 2 (high), 5, 6 and 7E of the FOIA. Additionally, I have determined that the supplemental PLCY documents we have been processing, which consist of 70 pages of material responsive to your request, are releasable to you with certain information withheld pursuant to Exemption 1 of the FOIA. This concludes processing of the supplemental PLCY documents.

Enclosed are 170 pages of releasable information. The withheld information, consists of classified information, names or initials, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 1, 2, 5, 6, and 7E of the FOIA, 5 U.S.C. §§ 552 (b)(1), (b)(2), (b)(5), (b)(6), and (b)(7)(E).

Also enclosed are 34 blank sheets with several numbers that represent withheld documents. Each number corresponds to a page of withheld information and has the appropriate exemptions that apply to that document. In this instance, there are 374 pages of withheld information that cover 34 documents.

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 concerns 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.

Exemption 2(low) exempts from disclosure records that are related to internal matters of a relatively trivial nature, such as internal administrative tracking. Exemption 2(high) protects information 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.

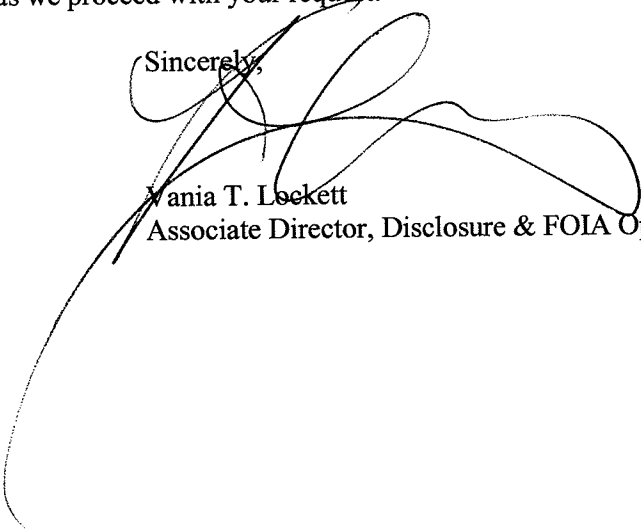
Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure 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.

Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy.

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

As stated in the February 1, 2008 Status Report for the litigation which encompasses this FOIA request, we are continuing to process your request with regard to documents located at the following CBP Offices: Office of Field Operations, National Targeting and Security; Office of the Chief Counsel; and Office of Information Technology. This release completes the Office of Chief Counsel hard copy documents and electronic file documents, except those involving the 2004 agreement with the European Union and the two boxes of documents recently located and mentioned in the Status Report. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-160/Sobel request**. This office can be reached at 866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,


Mania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 204 pages

**A REPORT
CONCERNING PASSENGER NAME RECORD INFORMATION
DERIVED FROM FLIGHTS BETWEEN
THE U.S. AND THE EUROPEAN UNION**

Privacy Office
U.S. Department of Homeland Security

September 19, 2005

Deleted: 6

002354

TABLE OF CONTENTS

- I. Letter from the Chief Privacy Officer**
- II. Executive Summary**
- III. History of the PNR Arrangement**
- IV. DHS Privacy Review: A Chronology**
- V. Findings**
 - A. CBP Implementation Practices**
 - B. Undertakings: Section by Section Review**
 - C. Recommendations**
- VI. Conclusion**

APPENDICES

APPENDIX 1: Lifecycle of PNR in CBP Operations

I. LETTER FROM THE CHIEF PRIVACY OFFICER

Both the United States and Europe have acknowledged that the exchange of information is an essential tool to fight the global terrorist threat. As we have thought more about current needs and how best to appropriately share information for homeland security purposes, we also have recognized the necessity to take on hard questions concerning the proper limitations on collection and use of data and safeguards for personal information received and shared by government. Democracies worry about such questions because it is an imperative to maintaining the fundamental freedoms and rights we enjoy – the values and way of life we seek to protect from the tyranny of terrorism.

Privacy is recognized in Europe and the United States as an essential right and fundamental value that is well developed in law and custom. We look forward to continuing to work together with European countries and the European Union to honor and integrate privacy protections into the means and practices through which we carry out our homeland security missions.

Both appropriate information sharing and privacy protection are important and the two principles must work together in tandem. This is recognized by senior government leaders on both sides of the Atlantic. These principles also were recognized by the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), in its Undertakings of May 11, 2004, concerning Passenger Name Record (PNR) information sharing, and within the U.S.-EU PNR Agreement of May 28, 2004.

The intent of the framework information sharing arrangement is to allow appropriate information sharing to facilitate safe, transatlantic travel and to fight terrorism and other serious crimes. Both sides recognize, however, that access to personal information

should not be unlimited and should be appropriately tailored, both in use and in the treatment of information received. That is why privacy is mentioned throughout the Undertakings and why both sides spent significant amounts of time working to build in operational privacy protections that would allow for necessary and appropriate sharing of individuals' personal data for public safety.

While this paper and the Joint Review must not lose sight of the fundamental and shared security purposes behind the PNR Undertakings, it is my duty as Chief Privacy Officer for the Department to carry out the mandates of Section 222 of the Homeland Security Act. Our enabling statute directs the Department and my role, in particular, to ensure that privacy attentiveness and privacy protections are integrated into the way the Department carries out our Homeland Security mission. I am pleased, along with my staff, to take on this policy and operational oversight role, both as an inside counselor to the Directorates, component agencies and offices within the Department, and in a necessary external role in reporting on progress and areas for continuing effort.

During the course of this past year, the Privacy Office has reviewed efforts by U.S. Customs and Border Protection to fully implement the Undertakings, as contemplated by the information sharing framework for PNR between the Department and the European Union. CBP has worked diligently with the Privacy Office during the review, including providing documents and information as needed. The efforts of CBP are applauded. I would like to personally thank Commissioner Robert Bonner, Deputy Commissioner Deborah Spero, and Executive Director for Border Security and Facilitation, Robert Jacksta and the CBP team he leads, for their efforts and partnership.

Based upon the Privacy Office review, I can report that CBP has achieved compliance with the representations made in the

Undertakings. While the overall report is positive, we believe that certain policy and operational elements took longer than anticipated to implement. As a result, in addition to guidance on necessary compliance measures, the Privacy Office also required certain remediation steps. CBP agreed to accept both the guidance and remediation required and has fully implemented both.

CBP has shown a willingness to go beyond the requirements of the Undertakings in many cases and to invest on the front end in an information architecture that addresses privacy protections. Additionally, where compliance was not complete during the development of the information system architecture, CBP has taken steps to fully remediate at the request of the Privacy Office. These actions demonstrate the integrity of the Agency and its commitment to integrating appropriate privacy protections into its policies, business processes and technical procedures.

This report summarizes the Privacy Office's review, issues that were raised, guidance shared, and the progress that was achieved during the course of this year.

Signed,

Nuala O'Connor Kelly

Deleted: d.....

II. EXECUTIVE SUMMARY

The fundamental purpose of the Joint Review is to serve as a constructive exercise that contributes to the effective operation of U.S. Customs and Border Protection's Undertakings of May 11, 2004, concerning PNR information derived from flights between the European Union and the U.S. The review conducted by the Department of Homeland Security Privacy Office regarding CBP's implementation of the Undertakings, from November 2004 through September 2005, also was conducted in this spirit.

As of the date of the Joint Review, the Privacy Office finds that CBP is in compliance with representations made in the Undertakings. CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance with the Undertakings. This is a recognizable achievement, particularly considering the state-of-the-art technology solutions that CBP voluntarily undertook to fully implement the Undertakings through the information technology (IT) systems used by CBP offices nation-wide.

During the course of the review this year the Privacy Office found areas for improvement and focus by CBP in order to reach full compliance with the Undertakings. Depending on the nature of the improvement, the Privacy Office made the following determinations: remediation required, recommendations, and areas to monitor closely. While CBP's overall efforts were responsive and the technological solutions are quite sophisticated, some policy and operational measures to meet full compliance took a lengthy period of time to achieve. At this date, however, the Privacy Office can report that all guidance recommended, whether as a remediation requirement, a recommendation, or direction to monitor areas closely, has been accepted by CBP. To that end, both CBP and Border

and Transportation Security leadership and staff are applauded for their partnership in meeting the challenge of being stewards for the Department's privacy and security mandate.

The following is a summary of the DHS Privacy Office review in two parts:

A. Compliance

- As of the date of the Joint Review, CBP is compliant with representations made in the Undertakings.
- We have had no reports of any deliberate misuse of PNR information received. Further, responsible measures have been undertaken to address system deficiencies that were identified by the Privacy Office prior to the full technical solutions implemented to CBP's IT systems to comply with the Undertakings.
- CBP has invested substantial time, capital, and expertise to fully comply with the Undertakings, both through practices and procedures and through the use of its technology systems.
- CBP, with advice and guidance from the DHS Privacy Office, issued privacy notices and implemented suggested improvements for compliance with the representations in the Undertakings, including the development of compliant information system technology architecture.
- CBP instituted specialized training for its officers on handling PNR derived from flights between the U.S. and the EU.

- New procedures were put in place to track and respond to requests from individual travelers for information related to PNR; CBP's systems were modified to reflect the terms of the Undertakings.

B. Remediation and Best Practices Required by Privacy Office

- *Review and Delete Sensitive Terms.* CBP agreed to delete "sensitive" terms and codes agreed to in the Undertakings, which were gathered prior to March 14, 2005, when a functioning technological solution was fully implemented to delete all "sensitive" terms and codes. Such terms and codes collected between May 28, 2004 and March 14, 2005, were deleted. The deletion was completed on August 19, 2005 and verified by the Privacy Office.
- *Review and Delete Data outside the 34 permitted elements.* CBP agreed to delete data elements beyond the 34 data elements noted in the Undertakings which, in certain cases, were gathered prior to March 14, 2005, when a functioning technological solution was fully implemented to assist in complying with the Undertakings. Excess data elements collected between May 28, 2004 and March 14, 2005 were deleted. This deletion was completed on August 19, 2005 and verified by the Privacy Office.
- *Review Audit Logs for PNR Manually Accessed and Plan for Proper Retention Periods.* For the period from May 28, 2004 to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an appropriate retention period for the data when it is unable to determine if PNR was manually accessed. It will implement

(b)(5) - Atty Client & Delib

(b)(5) - Atty Client & Delib

the shorter retention period of 3.5 years in these cases, as contemplated by the Undertakings. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

- *Plan Required for Scheduling Routine Reviews of the Use of PNR Information.* In response to remediation guidance from the Privacy Office, the Office of Management Inspections and Integrity Assurance (MIIA) has established a proactive plan for reviewing audit logs associated with CBP's automated system ("the automated system") which maintains the relevant personal information covered by the Undertakings and the PNR arrangement. The purpose of their audit function is to review the use of PNR information. Additionally, the Office of Information and Technology, since May 30, 2005, has been auditing the system weekly for unauthorized use of all PNR data.
- *Electronic Tracking of Disclosures.* CBP added additional technical features that will electronically track whether a particular PNR has been disclosed and to what agency. This will lead to greater assurance for data integrity than the previous paper-based process, particularly so that if a correction is noted with respect to any PNR, all appropriate parties are notified. This change was completed on September 14, 2005. Electronic tracking is a best practice, but is not required by the Undertakings.
- *Audit Process for Access to Airline Reservation Data.* CBP added additional auditable mechanisms for confirming that supervisory approval is sought before officers of CBP are able to manually access airline reservation data. This change was completed September 14, 2005. The IT audit mechanism is a best practice, but is not required by the Undertakings.

(b)(5) - Atty Client & Delib

C. Areas to Continue to Monitor Closely:

- *Reconcile Guidance.* Upon conclusion of the Joint Review, CBP will update field guidance in order to capture all appropriate procedural changes, including recommendations that may be made by the Joint Review team, so that they may be properly implemented. The updated guidance will be disseminated to officer of CBP in the field.
- *Data Disposition.* For records that are manually accessed but not associated with a law enforcement action, CBP will be archiving materials after 3.5 years. CBP is working on the technical solution and will have it in place prior to November 28, 2007, when this commitment will go into affect. It also is working on the deletion process that will need to be in place by November 28, 2015, at which time manually accessed PNR received since May 28, 2004 will start to be deleted consistent with the Undertakings.
- *Approval of Data Retention Schedule.* CBP has drafted for approval a National Archives and Records Administration (NARA) data retention schedule for PNR that is in conformance with the Undertakings, and submitted it to NARA for consideration on March 29, 2005. The process can take up to six months or longer for NARA approval. CBP will inform the Privacy Office of NARA's determination.

CBP continues to refine its privacy program as it relates to PNR, which we are confident will contribute to the effective implementation of the Undertakings and the operations of CBP. CBP has made all recommended changes requested by the Privacy Office.

The Privacy Office will continue to work with CBP in order to ensure that as the operational needs of CBP evolve, privacy protections are maintained.

III. HISTORY OF THE PNR ARRANGEMENT

In the aftermath of September 11th, the United States Congress enacted legislation authorizing the United States Department of Homeland Security's Bureau of Customs and Border Protection (CBP) to obtain access to passenger name records (PNR) originally collected by airlines and airline reservation systems for commercial purposes. More recently, in Section 7210 of the Intelligence Reform and Terrorism Prevention Act of 2004, the Congress also indicated that, where practicable, the Federal government should conduct passenger screening before individuals depart on a flight destined for the United States. Following these Congressional mandates, CBP actively uses PNR information as an initial screening tool to determine whether individuals of interest are planning to travel to the United States.

Beginning in 2002, following the publication of CBP's interim regulations implementing the PNR access requirement referenced above, the European Commission (EC) advised DHS that an EU Data Protection Directive generally prohibited cross-border sharing with non-EU countries, absent a demonstration that the receiving entity in a third country has adequate data protection standards.

Notwithstanding possible exceptions from the Data Protection Directive for law enforcement and national security purposes, as a means to secure CBP's access to PNR and to provide certainty to the airlines and companies operating Global Distribution Systems (GDS), which may be subject to the EU Data Protection Directive, the U.S. and EU governing authorities committed to negotiate an arrangement to share information while maintaining safeguards for

PNR data related to flights to and from the EU. An Interim Arrangement was reached in March, 2003, and CBP implemented guidance to ^{(b)(5) - Atty Client & Delib} in the field so that their treatment of PNR data received was consistent with the Interim Arrangement.

(b)(5) - Atty Client & Delib

On May 28, 2004, an International Agreement regarding the processing of Passenger Name Records (PNR) was signed by the U.S. Department of Homeland Security (DHS) and the European Union (EU). The Agreement followed the issuance by U.S. Customs and Border Protection (CBP) of a set of Undertakings setting forth how CBP would process and transfer PNR data received in connection with flights between the U.S. and the EU and the subsequent issuance of an Adequacy Finding by the EU concerning such transfers. As part of the Undertakings, DHS and CBP provided for a Joint Review to take place between the U.S. and EU to examine CBP's implementation of the Undertakings.

The Undertakings sets up a compliance and complaint resolution role for the DHS Chief Privacy Officer. Prior to the upcoming Joint Review, the DHS Privacy Office conducted an internal review of CBP's implementation of the Undertakings' privacy measures. The internal review has been an iterative process of both reviewing the adequacy of CBP implementation efforts and the Privacy Office providing CBP with internal counseling and conformance measures for achieving consistency with the CBP representations in the Undertakings.

The Privacy Office provided constructive criticism and guidance on many aspects of CBP's implementation efforts at different points along the review and implementation time line. This is entirely consistent with the internal function of the DHS Privacy Office to provide counsel and privacy policy and compliance direction within DHS. The Privacy Office also is facilitating the Joint Review of the implementation of the representations in the

Deleted:

Undertakings on PNR data derived from flights between the U.S. and EU (EU PNR).

As of May 16, 2005, CBP's written policies and procedures, their actual implementation, and the technology solutions adopted for handling PNR received from the EU indicated substantial consistency with the Undertakings, dated May 11, 2004, as referenced in the U.S.- EU PNR Agreement, signed on May 28, 2004. In addition, as of September 16, 2005, CBP has implemented remediation and best practice enhancements in response to Privacy Office recommendations.

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. CBP staff made improvements to policies and procedures, both unilaterally by December 2004, and further modifications thereafter at the request of the Privacy Office during the course of the review.

For the periods during which CBP's implementation of the Undertakings was not consistent with representations made to the EU, remediation was necessary, as discussed previously in Section II of this report.

IV. DHS PRIVACY REVIEW: A CHRONOLOGY

The fundamental purpose of the Joint Review is a constructive one. DHS and the EU, as Joint Review partners, share a view, "... to mutually contributing to the effective operation of the ... Undertakings" (Undertakings at paragraph 43), by periodically meeting to discuss implementation progress. The Privacy Office review also has been conducted in this spirit.

As specified in the Undertakings, the compositions of the Joint Review teams are a cross-section of privacy/data protection, law enforcement, and border and aviation security (Undertakings at paragraph 43, fn.13). In keeping with the Undertaking's dual values of law enforcement and privacy, the make-up of the review teams embodies both principles at the Joint Review.

A. The DHS Privacy Office

1. The DHS Privacy Office Mission

The mission of the Privacy Office is a constructive one. It is an independent voice meant to assist, counsel, recommend, and, where necessary, seek remediation to ensure protection of personal data. It serves a necessary self-critical role for DHS, but one that seeks improvement.

The DHS Privacy Office is the first statutorily required, comprehensive privacy operation in any U.S. federal agency. It operates under the direction of the Chief Privacy Officer, Nuala O'Connor Kelly, who is appointed by the Secretary. The Chief Privacy Officer serves as a steward of Section 222 of the Homeland Security Act of 2002, and the Privacy Office has programmatic responsibilities for the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act, and the numerous laws, Executive Orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personal and Departmental information.

The Privacy Office has oversight of privacy policy matters and information disclosure policy. It is also statutorily required to evaluate all new technologies used by the Department for their impact on personal privacy. The Privacy Office is required to report

to Congress on these matters, as well as on complaints about possible privacy violations. Further, the Privacy Office is responsible for privacy-related education and training initiatives for DHS's more than 180,000 employees.

The construct of a privacy officer is similar, but not identical, to the construct of a data protection commissioner. The very principles that the two offices espouse are exactly the same: a constant vigilance to limiting intrusion, to questioning processes, to educating our employees, to encouraging reform, and to challenging and pointing out mistakes when necessary. At DHS, the Chief Privacy Officer's role and that of her Office is both inside and outside the agency. On the inside, the Privacy Office works to educate, to inform, to create processes and mandate attention to privacy and fair information principles in every evolution of new programs, new procedures, new policies, even the hiring and training of new personnel. On the outside, the Privacy Office champions DHS programs where appropriate, but criticizes where necessary. Also, the DHS Privacy Office reports directly to Congress on activities of the Department in a fair, if sometimes critical, way.

2. The DHS Privacy Office and the Undertakings

Consistent with the stated purpose of the Undertakings, the Privacy Office undertook its mission to contribute to the protection of privacy interests relative to PNR data. Further, the Privacy Office, along with the Border and Transportation Security Directorate and CBP, is facilitating the Joint Review of the implementation of the representations in the Undertakings on EU PNR.

As essential background to the Joint Review, it is worth reviewing the various duties of the Privacy Office as defined in the Undertakings: a) oversight and investigation of disclosure, retention and disposal issues related to PNR; b) resolution of complaints

between individuals and CBP; and c) point of contact for Data Protection Authorities (DPAs) in the EU member states on behalf of an EU resident.

- a. First, Oversight and Investigation. Paragraph 31 recognizes that the Privacy Office has authority to investigate and report on failures to respect conditions for transfer of PNR data with Designated Authorities. We may make findings that the designated authority is ineligible to receive further transfers of PNR data. To date the Privacy Office has not found any of the agencies with which PNR was shared to be ineligible. The review of the policies and procedures surrounding sharing indicates consistency with the representations of the Undertakings.
- b. Second, Resolution of Complaints. Paragraph 41 serves as an appellate function to resolve complaints between individuals and CBP. The Chief Privacy Officer is independent of any directorate within DHS and is statutorily obligated to insure that personal information is used in a manner that complies with relevant laws. To date, the Privacy Office has received no complaints regarding the use of PNR and the Privacy Office has found no instances of misuse of PNR derived from flights between the U.S. and EU by CBP.
- c. Third, Point of Contact and Reporting to Congress. Paragraph 42 establishes the Privacy Office as a point of contact for EU data protection authorities when one of its residents does not believe his/her concern has been satisfactorily addressed by CBP. The Privacy Office will address such complaints on an expedited basis and report back to the member country, as well as to Congress. There have been no requests or complaints received directly by the Privacy Office from any DPA since the Undertakings were issued in May 2004.

B. CBP

1. CBP Mission:

CBP is the unified border agency within DHS. Under the Homeland Security Act, the U.S. Customs Service was renamed CBP and the inspectional and border patrol elements of the former Immigration and Naturalization Service (INS), and the inspectional elements of the Department of Agriculture, were transferred to CBP. As the single, unified border agency, CBP's mission is vital to the protection of the United States. While its priority mission is to prevent terrorists and terrorist weapons from entering the United States, CBP is also responsible with enforcing all import and export laws, while also facilitating the flow of legitimate trade and travel. CBP uses multiple strategies and employs the latest in technology to accomplish its dual goals. CBP's initiatives are designed to protect the U.S. from acts of terrorism, and reduce the vulnerability to the threat of terrorists through a multi-level inspection process.

2. CBP Efforts

In the U.S., we tend to look at technology risks as well as technology solutions that recognize the appropriate use of information and guard against harm and misuse of personal information. To that end, CBP undertook an analysis not only of policies and procedures, but of their technology systems. With assistance and guidance from the Privacy Office, CBP worked to implement the Undertakings representations. CBP also actively looked for ways they could improve handling PNR received from the EU.

DHS and the EU were aware from the start that many of the representations in the Undertakings would require DHS and CBP in

particular, to make substantial technological changes to its systems, as well as changes in policy, the implementation of which would take time. For example, Officers of CBP with access to PNR received specialized training on handling PNR derived from flights between the U.S. and the EU; new procedures were put in place to track and respond to requests for information related to PNR; and CBP's systems were modified to reflect the terms of the Undertakings.

C. Chronology of the Review

In August 2004, the Privacy Office began discussing the internal review process with Customs and Border Protection (CBP). In November 2004, Nuala O'Connor Kelly, Chief Privacy Officer, DHS, contacted Robert Bonner, CBP Commissioner, to recommend an outline of how the internal privacy review would be conducted, and present the criteria that would be used for measuring consistency with the representations in the Undertakings. The internal review described in this report has assessed CBP's effectiveness in acting consistently with those representations.

1. The DHS PNR Review Team

The DHS PNR Review team was led by Rebecca J. Richards, Director of Privacy Compliance, with technical assistance from Peter Sand, Director of Privacy Technology, and Anna Slomovic, Sr. Privacy Analyst. Technical implementation of the Undertakings in the CBP systems has been reviewed by Robert Bollig from the DHS Office of the Chief Information Officer (OCIO). Maureen Cooney, Privacy Office Chief of Staff and Director of International Privacy Policy, and Elizabeth Withnell, Chief Counsel to the Privacy Officer provided assistance and counsel. The Review team has extensive compliance, privacy policy, legal, and technical expertise.

2. DHS PNR Review

The review consisted of an analysis of existing policies and procedures, interviews with key management and staff that handle PNR, and technical review of CBP systems and documentation.

The Privacy Office has reviewed the following materials:

- Data lifecycle map;
- Privacy notices to travelers;
- Documented procedures for specific areas relating to collection, use, sharing, and retention of personal information;
- Training materials;
- Contacts with third party agencies including information requests that have been honored; and
- Technical logs that may be pertinent.

Interviews included:

- CBP's National Targeting Center (NTC) Management on policies, procedures and use of the system;
- Passenger Analytic Unit (PAU) training team (individuals who handle PNR on a regular basis);
- Office of Information Technology (OIT) regarding:
 - Privacy training;
 - Sensitive filters and associated timelines;
 - IT User and Functional Requirements being developed to comply with the Undertakings;
 - How CBP's automated system operates; and
- The Customer Satisfaction Unit (CSU).

In addition, the Review Team received a written statement from the Office of Management Inspections and Integrity Assurance

(MIIA) with examples of how they detect internal problems and perform audits.

CBP's OIT worked with Office of Field Operations (OFO) and the Chief Counsel's Office (OCC) to create technical/technological implementation and enforcement of many of the Undertakings.

Technology implementations were developed, tested, and deployed beginning March 14, 2005. This first phase included the implementation of "sensitive" terms and codes filters, and filtering for the 34 data elements noted in the Undertakings. On May 13, 2005, CBP finalized functional changes to its automated system. This included changes to access control requirements and supervisory approval functions.

Based on the results of our review, the Privacy Office has outlined areas of consistency with the representations in the Undertakings, remediation required, recommendations and areas to monitor closely.

(b)(5) - Atty Client & Delib

V. FINDINGS

During the period of the Privacy Office review, in particular, CBP has worked hard to ensure that its policies, procedures, and information technology conform to the representations in the Undertakings. As stated above, some of the provisions of the Undertakings were covered by existing laws, regulations, policies, and procedures with which CBP complies. Other provisions required the expenditure of extensive time, effort and resources by CBP's operations, technical and counsel staff to build the strong program that has brought them into full consistency with the representations in the Undertakings, as of September 16, 2005.

A. Areas of Consistency

Below are significant CBP activities that demonstrate consistency with the Undertakings:

- The bi-annual privacy training that is required for all (b)(5) - Atty Client & Delib [REDACTED] with access to CBP's information systems is informative and well-developed. The examination at the end of the training requires a working knowledge of privacy to pass and gain or retain access to CBP systems.
- CBP's field guidance on handling PNR data derived from flights between the U.S. and EU tracks the Undertakings, and provides excellent training to [REDACTED] in the field and at CBP's National Targeting Center [REDACTED] (b)(5) - Atty Client & Delib [REDACTED]
- The policies and procedures for disclosure of PNR to third parties, both internal to DHS and external to DHS, are well developed.
- CBP requires that all individuals who have access to PNR sign off on notice of the field guidance. This sign off is recorded specifically in the training portion of CBP's personnel tracking system, and demonstrates the seriousness with which CBP is taking the Undertakings and its full implementation of representations made on behalf of the U.S. to the EU. Deleted: The Deleted: ment Deleted: . This tracking
- The IT User Requirements have been developed in great detail and in collaboration between operations, technical, and counsel staff. Their deployment on May 13, 2005, provides technical support for consistency with the representations in the Undertakings, as articulated in CBP field guidance.
- The updates to policies regarding the approval process for

gaining access to CBP's automated system have decreased the number of individuals overall who have access to PNR.

- The updated access roles for users of CBP's automated system have been well thought out and reduce the number of users with access to PNR seven (7) days after completion of travel by over forty percent (40%).
- The filters for sensitive terms and codes as provided for in the Undertakings have been deployed and have been working successfully since March 14, 2005.
- PNR data derived from flights between the EU and the U.S. has also been automatically filtered to ensure it has a nexus to the U.S. This update was implemented on March 14, 2005.
- CBP has provided guidance to its Freedom of Information Act (FOIA) personnel on how to handle requests from individuals that either specifically request PNR or who ask for information more generally.
- CBP has implemented regularly scheduled processes to obtain PNR data, thereby decreasing the occurrence of manually accessed PNR data.
- For records that are manually accessed but not associated with a law enforcement action, CBP will be archiving materials after 3.5 years. CBP is working on the technical solution and will have it in place prior to November 28, 2007, when this provision will go into effect.

B. Undertakings: Section by Section Review

This section discusses the policies, procedures, practices, and IT support related to various areas of the Undertakings.

1. Legal Authority to Obtain PNR (Paragraph 1 of the Undertakings)

The Undertakings state that CBP has legal authority to collect the PNR.

CBP collects PNR data as authorized by legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing regulation.

CBP issued field guidance specific to the PNR related to flights between the United States and European Union Countries on December 20, 2004. This guidance reflects the terms of the Undertakings. On March 14, 2005, an automated system was deployed that filters and tags PNR related to flights between the United States and European Union countries, which further strengthened compliance with the Undertakings.

Findings: Based on review of documented procedures, regulations, and applicable U.S. laws, CBP operates in a manner consistent with the representations in the Undertakings document.

2. Use of PNR Data by CBP (Paragraph 2-3 of the Undertakings)

The Undertakings lay out specifically the scope for which PNR data may be used by CBP.

Officers of CBP who work within the PAUs and CBP's NTC are trained to identify passengers who are considered high risk and have

received additional training in the form of written field guidance. This field guidance is consistent with the scope of purposes identified in the Undertakings. All Officers of CBP with access to PNR data are required to review and sign an acknowledgment of this guidance. This is logged in the training system so that it may be regularly reviewed by Headquarters staff to ensure that the field staff are properly trained on the use and disclosure of the data.

Although the mission of CBP is broader than the three purposes specified in the Undertakings, CBP's use of PNR data is fully consistent with the three stated purposes in the Undertakings.

Findings: Based on review of documented procedures, technical measures and, in-person interviews, CBP operates in a manner consistent with the representations in the Undertakings.

3. Data Requirements

(Paragraph 4-8 of the Undertakings)

The Undertakings set forth CBP's specific PNR data requirements and also specify when and how additional information may be obtained by CBP.

On March 14, 2005, CBP's automated system was updated to capture only the 34 PNR data elements identified in the Undertakings from an air carrier's system and parse it so that the data can be viewed consistently across air carriers. Any elements outside of the 34, for example number of bags, will be filtered so that the information may not be viewed and is not retrievable. At the same time, CBP deployed the sensitive term and code filters, which delete all sensitive terms and codes that were mutually identified between the EU and U.S. on November 3, 2004. The original PNR is filtered and sensitive terms cannot be re-created.

On May 13, 2005, CBP deployed updates to the automated system to

reduce the number of users who have access to PNR. The system limits who may access the OSI and SSI/SSR open fields. The user must receive specific approval before viewing these fields. An audit trail is created when the OSI and SSI/SSR fields are accessed.

PAUs and the NTC do not have investigative responsibilities. If, based on the information available to PAU and NTC officers, additional information about an individual must be obtained from sources outside the government, the officers may contact appropriate law enforcement authorities for further investigation. Those law enforcement authorities can then obtain additional data through lawful channels. Officers are trained on these procedures prior to gaining access to PNR.

CBP anticipates working with the EU if it finds that additional data fields are required beyond the 34 data elements identified in the Undertakings.

Due to the cancellation of the CAPPs II program, there was no transfer of PNR data for any purpose related to this program. There have been no bulk transfers to any agency of PNR data which CBP obtains pursuant to its legal authority.

Findings: Based on an extensive technical review of the system as well as a review of the documented policies, procedures, training, interviews, applicable regulations and U.S. law, CBP is in compliance with the representations in the Undertakings for data collected as of May 13, 2005. For data received between May 28, 2004 and March 14, 2005, the Privacy Office required CBP to review and filter data elements that were received beyond the 34 data elements set forth in the Undertakings and to permanently delete these items. CBP agreed, and the deletion process was completed on August 19, 2005 and was verified by the Privacy Office.

(b)(5) - Atty Client & Delib

4. Treatment of "Sensitive" Data (Paragraph 9-11 of the Undertakings)

The Undertakings specify that "sensitive" data will be filtered and deleted.

Officers of CBP are trained to follow the Undertakings on the proper use of sensitive personal information such as race, color, age, sexual orientation, religion, sex, national origin, or disability for purposes of identifying persons of concern. The "Standards of Conduct," agency guidance that provides standards of behavior for all CBP employees, specifically states: "Employees will not act or fail to act on an official matter in a manner which improperly takes into consideration an individual's race, color, age, sexual orientation, religion, sex, national origin, or disability." All CBP employees receive a copy of the Standards of Conduct at the start of employment.

CBP's "Table of Offenses and Penalties," which provides guidance to CBP managers, supervisors and practitioners on the appropriate penalties to apply in typical cases of employee misconduct, provides for anywhere from a fourteen (14) day suspension to removal from employment for "[a]cting or failing to act on an official matter in a manner which improperly takes into consideration an individual's race, color, age, sexual orientation, religion, sex, national origin, or disability." (Section B(2), Discriminatory Behavior).

In addition to the general training that all officers of CBP receive, those in the PAUs and CBP's NTC are specifically reminded that the identification of individuals for the purposes of focusing further investigation based on race, religion, or sex is prohibited.

Prior to the implementation of the sensitive data filters in March of 2005, CBP field guidance provided that [REDACTED] were not allowed to use "sensitive" terms and codes, as mutually identified by the U.S. and EU. The guidance required that for discretionary

(b)(5) - Atty Client & Delib

disclosures outside of CBP, either internally to DHS or externally to other government agencies or foreign countries, sensitive data had to be removed prior to disclosure. For non-discretionary disclosures, field guidance provided that the [REDACTED] consult with appropriate counsel to determine what must be disclosed. On March 14, 2005, CBP deployed the "sensitive" data filter, which deletes all sensitive terms and codes, as agreed by the U.S. and EU on November 3, 2004. With the implementation of the "sensitive" data filter, no such terms or codes will appear in the PNR. For PNR received between May 28, 2005 and March 14, 2005, CBP has deleted all "sensitive" terms and codes; therefore manual redaction is no longer necessary.

(b)(5) - Atty Client & Delib

A summary was included in the field guidance issued to CBP supervisors highlighting the key points that must be reviewed prior to further dissemination of the guidance to [REDACTED] in the field. This insured that supervisors were providing consistent training across the different ports. After receiving and reviewing field guidance, all [REDACTED] were required to sign a statement that they read and understood it.

Deleted: n item

(b)(5) - Atty Client & Delib

(b)(5) - Atty Client & Delib

Findings: Based on an extensive technical review of the system as well as a review of the documented policies, procedures, training, interviews and applicable regulations and U.S. law, CBP is in compliance with the representations in the Undertakings for data received on or following March 14, 2005. For data received between May 28, 2004 and March 14, 2005, the Privacy Office required CBP to review data, filter "sensitive" codes and terms, and permanently delete these items. CBP agreed to this remediation course and it was completed on August 19, 2005, and compliance was verified by the Privacy Office.

Deleted: and

(b)(5) - Atty Client & Delib

000000

5. Method of Accessing PNR Data
(Paragraph 12-14 of the Undertakings)

The Undertakings provide for specifics on when and how often CBP may access PNR from air carrier systems.

Before accessing airline reservation data in the automated system, [REDACTED] encounter several system prompts and reminders of field guidance and policies regarding the authorized use of PNR data. Each user must click "I agree" to such statements before he or she is given access to the system.

(b)(5) - Atty Client & Delib

PNR data derived between the EU and the U.S. has also been automatically filtered to ensure it has a nexus to the U.S. This update was implemented on March 14, 2005.

CBP is working with several air carriers and Global Distribution Systems (GDSs) to develop a "push" system that meets the needs of all parties and has had preliminary conversations with representatives of some of the major reservation systems. Currently, CBP is testing a "push" system with the airlines to modernize reservation data access and dissemination methods.

PNR data is retrieved no earlier than 72 hours prior to scheduled flight departure. Non-routine retrievals are documented both manually and electronically and require supervisory approval and coordination with the NTC. In addition, field guidance provides specific processes and reporting requirements to be followed in cases where PNR data is manually accessed.

Findings: Based upon a review of the technical system and documented policies and procedures, beginning May 13, 2005, CBP is in compliance with the representations in the Undertakings. For the

period from May 28, 2004 to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an appropriate retention period for data when it is unable to determine if PNR was manually accessed. It will implement the shorter retention period of 3.5 years in these cases, as contemplated by the Undertakings. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

6. Storage of PNR Data (Paragraph 15 Undertakings)

The Undertakings provide for specific requirements regarding who may have access to PNR and for how long different data sets may be maintained by CBP.

Access: CBP has issued guidance requiring supervisory approval for user access to the automated system. Access privileges are also discontinued after a specified period following lack of use of the system by an authorized user.

On May 13, 2005, CBP deployed four new user roles that restrict the number of individuals with access to PNR for set periods of time:

- Group I Users have access to CBP's automated system, but are not able to view PNR;
- Group II Users have access to PNR for 7 days after the last day of travel and must obtain supervisory approval to view OSI and SSI/SSR open fields;
- Group III Users have access to PNR beyond 7 days after the last day of travel and must obtain supervisory approval to view OSI and SSI/SSR open fields;
- Group IV Users have access to PNR beyond 7 days after the last

day of travel, are able to access OSI and SSI/SSR open fields as needed, and provide permission to those in the previous group that cannot view the open fields without permission.

The number of users who can access a particular PNR drops by over forty percent seven days after completion of travel.

The system restricts users in the appropriate groups to reviewing data only for the appropriate time periods. The system is also able to flag what PNR has been accessed manually and what PNR is related to a law enforcement action so that the information is maintained for the appropriate retention periods.

To ensure that the system is being accessed and used appropriately, audit logs are being created for all access to PNR data.

Retention: CBP continues to work on its National Archived Records Administration (NARA) retention period. A NARA retention schedule has been drafted and submitted to NARA. The process takes roughly six months from March 29, 2005. CBP will notify the Privacy Office of NARA's determination.

CBP is unable to differentiate manually accessed PNR data from other data that was received between the period of May 28, 2004 and May 14, 2005. After the implementation of the access controls on May 14, 2005, CBP obtained the ability to differentiate PNR connected to a law enforcement action. CBP anticipates the development of a mechanism, well in advance of the November 28, 2007 deadline, that will determine when these records will need to be deleted or archived.

Findings: Based upon review of documented policies and review of the technical system, CBP is substantially compliant with the representations in the Undertakings. For the period from May 28,

2004 to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an appropriate retention period for data when it is unable to determine if PNR was manually accessed. It will implement the shorter retention period of 3.5 years in these cases, as contemplated by the Undertakings document. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

7. CBP Computer System Security (Paragraphs 16-23 of the Undertakings)

The Undertakings require that specific technical and training requirements are met to ensure the security and privacy of the system, and that appropriate disciplinary actions can be taken if a problem arises.

CBP's automated system is Certified and Accredited (C&A) under the Federal Information Security Management Act (FISMA). Formal accreditation was issued in February 2003. The C&A is performed every three years.

The automated system is only accessible through the CBP intranet. All information is read only. No other foreign, federal, state, or local agency has direct electronic access to the PNR data.

Access to PNR is controlled through the automated system. Multiple layers of approval are needed for PNR access. Individuals must have a favorable background check, local supervisory approval, Headquarters approval, and approval from the Office of Information Technology.

All officers of CBP with access to systems containing PNR data must take privacy awareness training and pass an exam every two years.

User access is denied if an individual does not take the online class and pass the exam. Supervisory approvals are necessary to regain access to the system. In accordance with CBP policy, failure to complete privacy and security training may be documented in the individual's file.

Training covers the appropriate use and disclosure of personal information by an officer of CBP. It gives an excellent overview of the Privacy Act requirements and application of the third agency rule that are being fully implemented for PNR data. Training also covers Freedom of Information Act (FOIA) and overall required privacy practices. The training includes a test that requires a working knowledge of privacy to pass and gain or retain access to the system.

CBP's "Table of Offenses and Penalties" guidance provides for an appropriate penalty for using government property, property under government custody, or the property of others, for other than official purposes, which includes querying confidential or sensitive databases for other than official purposes. A first offense leads to anywhere from a written reprimand to a fourteen (14) day suspension, and a second offense, anywhere from a fourteen (14) day suspension to removal, depending on the nature of the infraction. (Section J(3), Misuse of Property).

Office of Management Inspections and Integrity Assurance (MIIA) tracks all access to and activities on CBP's automated system. Users are reminded of this every time they log on. MIIA does not have an automated alert system at this time, but has been discussing such an option for several CBP systems, including the automated systems used for PNR. The Integrity Programs Division of MIIA conducts proactive periodic general data queries. MIIA will begin a program of scheduled audits of access to CBP's automated system that is used for PNR.

As a law enforcement agency, CBP (and its predecessor, U.S. Customs Service) has a long history of ensuring compliance. Officers of CBP have a legal obligation to ensure compliance with laws, regulations, and agency policies and take their duties seriously. They are required to, and regularly do, report issues and concerns to the CBP Joint Intake Center in the MIIA or DHS, Office of Inspector General (OIG). If the allegation might have a criminal predicate, it is investigated by the OIG or referred to the Immigration and Customs Enforcement (ICE), Office of Professional Responsibility. If the allegation is not considered to have a criminal predicate, MIIA will routinely refer the matter to CBP management for administrative inquiry and action.

Findings: Based upon review of training materials, documented policies, and procedures and the technical system, CBP is in compliance with the Undertakings. OIT conducts routine audits of the system weekly for unauthorized use of all PNR data. Additionally, MIIA will begin a program of scheduled audits of access to CBP's automated system that is used for PNR.

8. CBP Treatment and Protection of PNR Data (Paragraphs 24 – 27 of the Undertaking)

The Undertakings require that PNR data be afforded appropriate protection when requests for disclosures are made.

When users enter CBP's automated system, a notice reminds them that the system contains trade secrets and information protected by the Privacy Act. They are reminded about the fines associated with inappropriate use. The log-in page also carries a reminder that the information in the system is law-enforcement sensitive and that they may only view information with a nexus to the U.S.

Deleted: ,
Deleted: and
Deleted: also

CBP has existing policies and procedures for handling of FOIA and

Privacy Act requests in compliance with the law. PNR requests received are handled in accordance with these policies. CBP's field guidance on PNR specifically describes how requests for information and correction should be handled relative to PNR.

On May 16, 2005, at the request of the Privacy Office, additional guidance was issued to all FOIA and Customer Satisfaction Unit (CSU) staff directing them to send all FOIA requests related to PNR, whether specifically requesting PNR or that may be read to include PNR, to the PNR Program Officer for further research and response. This memo directs the staff to log EU PNR requests separately and to forward any requests for amendment to PNR to the PNR Program Officer.

Findings: Based on review of documented policies and procedures and the system that handles the disclosures, CBP is in compliance with the representations in the Undertakings.

9. Transfer of PNR Data to Other Government Authorities (Paragraphs 28-35 of the Undertakings)

The Undertakings lay out how PNR may be transferred to other government authorities outside of CBP.

DHS components are not treated as "third agencies" for Privacy Act purposes and no special "routine use" legal requirements for data transfer typically apply, other than a need for the specific information. CBP field guidance provides specific requirements for how information related to PNR derived from flights between the EU and U.S. is to be transferred outside CBP. The guidance states that DHS and its components are to be treated as "third agencies" for the purposes of data transfer. CBP maintains a file of all disclosures that have been made to other parts of DHS and a file of all disclosures

made to outside agencies. There have been no disclosures to foreign agencies as of September 16, 2005.

Through the privacy awareness training required for all officers of CBP with access to systems containing PNR and other sensitive data, CBP trains officers repeatedly that information should only be disclosed for specific purposes with prior approval and written documentation. The documentation must include why information was disclosed, to whom, and under what circumstances. There are specific questions on the privacy awareness training test regarding proper and improper disclosure of information. Officers must pass this test in order to gain and maintain access to the information systems at CBP and then on a biannual basis to maintain their access to the system.

CBP field guidance provides specifics regarding how and when PNR derived from flights between the U.S. and EU may be released. All disclosures must be requested in writing and only under exigent circumstances may such PNR data be disclosed based on a verbal request. In the instance of verbal requests, a written request must be submitted as soon as possible. The written request must indicate who is requesting the information and for what purposes. The officer of CBP must review and ensure that the government authority requesting the information has law enforcement or counterterrorism functions and that the subject PNR is being requested for the scope defined in the Undertakings. PNR may also be disclosed to relevant government authorities where necessary to protect the vital interests of a data subject or others, particularly with regard to significant health risks, pursuant to paragraph 34 of the Undertakings. All responses with the PNR must have the following disclosure:
"Property of U.S. Customs and Border Protection. This document is provided to your agency for its official use only and remains the PROPERTY OF U.S.CUSTOMS AND BORDER PROTECTION (CBP). This document contains confidential personal information of the data

subject ("Official Use Only") and confidential commercial information and may not be disclosed to any third party without the express prior written authorization of CBP." In addition, CBP has provided field officers with routine language that must be used for all disclosures in addition to the information noted above.

Prior to the implementation of automated filters to remove sensitive data, [REDACTED] manually removed sensitive data in cases of discretionary disclosure outside of CBP, either internally to DHS or externally to other government agencies or foreign countries. For non-discretionary disclosures, field guidance required that officers of CBP consult with appropriate counsel to determine what would be disclosed.

(b)(5) - Atty Client & Delib

Disclosures of PNR must be recorded and reported to CBP Headquarters on a monthly basis. Headquarters maintains a log of all disclosures that occur both within DHS and externally to other agencies. At the request of the Privacy Office, CBP is implementing a set of technical fixes to allow it to more efficiently monitor the disclosures of information that may be subsequently changed because of a request for correction by a data subject. This update was implemented on September 14, 2005, although it is not a requirement under the Undertakings. As of September 16, 2005, PNR has been shared in a small number of cases with other Department of Homeland Security component agencies or other U.S. government law enforcement and counterterrorism authorities that have a need to know to carry out their official duties. All were consistent with the scope of the Undertakings and had the notice above attached to the data.

(b)(5) - Atty Client & Delib

Findings: Based upon available information and documented policies and procedures, training materials, and the system handling disclosures, CBP is in compliance with the representations in the Undertakings.

Deleted: the Privacy Office assessment is that

Deleted: complying

**10. Notice, Access, and Opportunities for Redress for PNR
Data Subjects**
(Paragraphs 36-44 of the Undertakings)

The Undertakings reflect that CBP will provide individuals with notice, access to their records, and opportunities for redress.

CBP has developed the Customs and Border Protection "Passenger Name Record Privacy Statement for PNR Data Received in Connection with Flights Between the U.S. and the European Union." The statement discusses why CBP receives PNR data, who has access to it, how long data is retained, and how questions and complaints may be filed and appealed.

CBP has a Customer Satisfaction Unit and Freedom of Information Action Officers who respond to requests from the public and handle all requests related to PNR. If a passenger has an issue upon entry into or exit from the country, the first recourse is to speak with a supervisor at the Port of Entry and handle the issue. If the passenger has questions or concerns, the passenger will be given a general fact sheet that directs individuals to contact the FOIA/Customer Satisfaction Unit with any further questions if the issue cannot be resolved while the individual is still at the port.

On May 16, 2005, additional guidance was issued to all FOIA and Customer Satisfaction Unit (CSU) staff directing them to send all FOIA requests related to PNR, whether specifically requesting PNR or potentially related to PNR, to the PNR Program Officer for further research and response. This memo directs the staff to log requests for EU PNR separately and to forward any requests for amendment to PNR to the PNR Program Officer.

FOIA requests received by CBP are handled in accordance with Title

19, Code of Federal Regulations, Section 103.5 and CBP directives. Field guidance on EU PNR reiterates existing statutory provisions and states that first party requests for personal information shall be processed without asserting any exemption based on the fact that the data is confidential personal information of that data subject (5 U.S.C. 552(b)(6)) or that it is confidential commercial information of the air carrier (5 U.S.C. 552(b)(4)). Other exemptions, however, may be applied as appropriate. Requests by persons other than the data subject will result in the assertion of these exemptions (5 U.S. C. 552 (b) (4) and (6)), as well as other applicable exemptions, and information will not be disclosed. This is consistent with the existing Customs Directive, DHS policy and the law.

Requests for corrections related to PNR data will be handled through both policies and procedures, and technical means. Field guidance states that if there is request made in the field, the (b)(5) - Atty Client & Delib should follow normal procedures for FOIA requests or amendment of records. If designated personnel in the NTC and the Security Office determine, whether through a request by the individual or on their own, that information in a PNR is inaccurate, a separate record in CBP's automated system will be created and linked from the PNR. This record will indicate the inaccuracy. The technical implementation will enable those who are authorized to make corrections to PNR records, to enter a FOIA tracking number into the correction record.

All corrections will be forwarded to the PNR Program Officer to determine whether the relevant information in the subject PNR has been disclosed to "third agencies." If disclosures of that information have been made, corrections will be forwarded to the appropriate parties.

If an individual has a concern, issue, or appeal after working with CBP, the matter may come to the attention of the Chief Privacy

Officer. Customs and Border Protection's "Passenger Name Record Privacy Statement for PNR Data Received in Connection with Flights Between the U.S. and the European Union" specifies that the DHS Chief Privacy Officer may review CBP decisions resolving inquiries and complaints.

Findings: Based on review of documented policies and procedures, as well as the system handling disclosures, interviews, and technical capabilities, CBP is in compliance with the representations in the Undertakings. At the request of the Privacy Office, CBP is implementing additional technical means to track the information that is shared to ensure that agencies that have received PNR information receive appropriate corrected information, including improvements to the data's integrity. This is a best practice measure and was not required by the Undertakings.

11. Usage Compliance Issues

(Paragraphs 43-44 of the Undertakings)

On July 22, 2003, CBP issued interim field guidance to provide officers of CBP with specifics on the handling of PNR consistent with the interim arrangement with the EU. On December 20, 2004, the Office of Field Operations issued guidance to all field offices and CBP's National Targeting Center to provide further guidance on EU PNR specific to the Undertakings. During weekly musters at that time, CBP supervisors highlighted the high level issues that needed to be addressed as the guidance was distributed. Anyone with access to PNR signed an acknowledgment that they had received and understood the field guidance. This was tracked in the training system.

Findings: Based on review of documented policies and procedures, training materials and interviews, CBP is complying with the representations in the Undertakings.

C. Areas for Improvement

The DHS Privacy Office found areas for improvement during this review process. CBP has made all the recommended changes or provided a timeline for when the recommended changes will be made. While CBP's overall efforts are good and the technological solutions are quite sophisticated, some efforts took longer than expected or should have. With the exception of language regarding the sensitive data elements that said "with the least possible delay," there was no provision in the Undertakings for a phased in approach to implementation (although arguably there should have been, as demonstrated by the fact that even after the issuance of the Undertakings and signing of the agreement, the list of "sensitive" data terms and codes were not settled by the parties until the fall of 2004). But, in any case, the reasonable expectation was for a speedier implementation.

1. Remediation

Efforts to remediate CBP treatment of PNR derived from flights between the U.S. and EU since issuance of the Undertakings and signing of the PNR Agreement were necessary to the extent that actual treatment had been inconsistent with formal representations to the EU and to citizens and other individuals whose data has been transferred since May of 2004.

- *Review and Delete "Sensitive" Terms.* CBP agreed to delete sensitive terms and codes as represented in the Undertakings, which were gathered between May 28, 2004 and March 14, 2005, when a functioning technological solution was fully implemented to delete all "sensitive" terms and codes. The time period for the deletion was May 28, 2004 to March 14, 2005. The deletion was completed on August 19, 2005 and

(b)(5) - Atty Client & Delib

verified by the Privacy Office.

- *Review and Delete Data Outside the 34 Agreed upon Fields.* CBP agreed to delete data elements beyond the 34 noted in the Undertakings which in certain cases were gathered between May 28, 2004 and March 14, 2005, when a functioning technological solution was implemented. The time period for the deletion was from May 28, 2004 to March 14, 2005. This deletion was completed on August 19, 2005 and verified by the Privacy Office.
- *Review Audit Logs for Retention Periods.* For the period prior to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an appropriate retention period for data when it is unable to determine if PNR was manually accessed. It will implement the shorter retention period of 3.5 years, as contemplated by the Undertakings. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

Deleted: has

(b)(5) - Atty Client & Delib

3. Recommendations

The following recommendations were made to strengthen consistency with the representations in the Undertakings and to generally enhance privacy interests. CBP has made all of these changes effective September 14, 2005.

(b)(5) - Atty Client & Delib

- *Electronic Tracking of Disclosures.* CBP created additional technical features that will electronically track whether a particular PNR has been disclosed and to what agency. This will lead to greater assurance for data integrity than the previous paper-based process, particularly so that if a

correction is noted with respect to any PNR, all appropriate parties are notified

- *Website Contact Information.* CBP and the Privacy Office have updated their websites to include a phone number to receive comments, complaints, and concerns and to reflect the implementation of the "sensitive" data filters.

4. Areas to Continue to Monitor Closely

In some instances, the representations in the Undertakings will take effect over time and so the Privacy Office will continue to monitor the implementation over time. These activities include:

- *Update CBP guidance to the field.* Throughout the review process, CBP has refined its approach to protecting privacy to ensure that it is fully consistent with the Undertakings. At the conclusion of the Joint Review, CBP will make a single set of changes to field guidance to incorporate the minor changes that have been made operationally over the last year.
- For records that are manually accessed but not associated with a law enforcement action, CBP will be archiving PNR after 3.5 years. CBP is working on the technical solution and will have it in place prior to November 28, 2007, when this provision will go into affect. CBP is also working on the deletion process that will need to be in place by November 28, 2015, at which time manually accessed PNR received starting on May 28, 2004 will start to be deleted in accordance with the Undertakings.
- CBP has drafted for approval a National Archives and Records Administration (NARA) data retention schedule for PNR that is in conformance with the Undertakings. The schedule was submitted on March 29, 2005, to NARA and takes about six

months to be approved.

D. Conclusion

Deleted: E

During the course of the Privacy Review this year, CBP has worked to make the changes required to bring it into full compliance with representation made in the Undertakings. The review helped to clarify the efforts required to fully actualize the framework for information sharing, including the necessity to build a technology system that integrated the Undertakings privacy provisions into the online operational screening process. This required a significant effort by CBP. While the discussions which preceded issuance of the Undertakings anticipated that it would take time to phase in the policies and operational measures to meet full compliance, the view of the Privacy Office is that it took too long on the part of our component agency CBP. For this reason, the Privacy Office made recommendations to CBP that would further enhance privacy protections above and beyond the obligations of the Undertakings. These recommendations were acknowledged, undertaken, and have been completed by CBP. The Privacy Office will continue to work closely with CBP to ensure that privacy protections are a part of any new operational policies and procedures implemented by CBP.

Deleted:

APPENDIX 1: Lifecycle of EU PNR in CBP Operations

What is PNR?

Anyone traveling on a commercial air carrier into or out of the United States has a reservation known as the Passenger Name Record (PNR). PNRs are generally created within air carriers' reservation and/or departure control systems ("reservation systems") to fill seats and collect revenue. There are five basic air carrier reservation systems, although each air carrier has made changes to their system tailored to their specific needs. As a result, very few of the air carriers' systems are exactly the same or provide CBP with the same information in the same format. Thirty-four (34) different air carriers with twenty-four (24) different systems engage in flights which are covered by the Undertakings.

PNR has three primary sections: *Active Portion*, which contains the name(s) of the passenger(s), the itinerary, and *Supplemental Information* (such as baggage, frequent flier information, special requests, or other information related to the reservation); and *Historical Portion*, which contains changes made to the active component. When CBP receives PNR from an air carrier it may have all this information or, more likely, it will have some portions of this information. CBP takes the PNR in unformatted form and parses it so that no matter which air carrier system is involved, the PNR is displayed in a common format for [REDACTED] who are reviewing it to identify high-risk passengers.

(b)(5) - Atty Client & Delib

CBP uses PNR related to flights between the U.S. and EU to facilitate legitimate travel into and out of the United States and to target more effectively individuals or groups related to terrorism or transnational crimes. PNR provides one of the first indications that a high risk individual may be trying to enter or leave the United States. Members of Passenger Analytic Units (PAUs) and CBP's National

Targeting Center (NTC) are trained to look for individuals of high risk, using PNR in conjunction with technological tools such as CBP's automated systems in conjunction with a variety of different law enforcement databases.

PNR is not used to make a final determination about an individual entering or leaving the United States because the information in the PNR is not sufficiently complete or accurate. PNR data is associated with Advance Passenger Information System (APIS) data, which provides the biographical information that is used for verification of a traveler's identity prior to arrival in the U.S. [REDACTED] at the primary inspection point will also verify and generally determine whether an individual warrants additional scrutiny.

(b)(5) - Atty Client & Delib

Lifecycle of the EU PNR from May 13, 2005 forward

The lifecycle as described below is the lifecycle that exists as of May 13, 2005 with the full implementation of the IT User Requirements.

Step 1: CBP pulls the 34 approved data elements of PNR no earlier than 72 hours prior to scheduled flight departure. If an appropriate push system exists, CBP will support the system from a technical standpoint to receive pushed data 72 hours before scheduled flight time and to receive all subsequent changes to PNR before flight time or to receive pushed data at a pre-specified times depending on a joint agreement with the airline.

Step 2: If data is pulled, unformatted PNR with all information, including "sensitive" data, is accessed and then filtered for "sensitive" terms and codes. "Sensitive" terms and codes are deleted and cannot be re-created. Symbols are put in the location where "sensitive" terms and codes have been removed and original PNR is filtered.

Step 3: PNR is filtered for the 32 data elements and OSI and SSI/SSR fields specified in the Undertakings. The remaining elements of the PNR are deleted by CBP and not accessed.

Step 4: The raw PNR is parsed into a screen that provides consistent display across all reservation systems. The PNR without "sensitive" terms and codes in an unformatted format along with the full information in the OSI and SSI/SSR fields is locked behind the parsed PNR and can only be accessed by a restricted set of users with approval of a supervisor for appropriate purposes.

Step 5: At seven days after the end of travel specified in the itinerary of the PNR, the PNR data will be made available to fewer individuals, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.

Step 6: At 3.5 years from receipt date/time given in the record, PNR that has not been manually accessed will be destroyed and manually accessed PNR will be archived with access only allowed for auditing and to correct technical errors.

Step 7: At 11.5 years from first receipt date/time given in the record, manually accessed PNR will be destroyed. PNR related to a specific enforcement action will be available until the enforcement action is archived.

#3

A REPORT
CONCERNING PASSENGER NAME RECORD INFORMATION
DERIVED FROM FLIGHTS BETWEEN
THE U.S. AND THE EUROPEAN UNION

Privacy Office
U.S. Department of Homeland Security

September 6, 2005

002800

TABLE OF CONTENTS

- I. Letter from the Chief Privacy Officer**
- II. Executive Summary**
- III. History of the PNR Arrangement**
- IV. DHS Privacy Review: A Chronology**
- V. Findings**
 - A. CBP Implementation Practices**
 - B. Undertakings: Section by Section Review**
 - C. Recommendations**
- VI. Conclusion**

APPENDICES

APPENDIX 1: PNR Agreement

APPENDIX 2: PNR Undertakings

APPENDIX 3: Lifecycle of PNR in CBP Operations

I. LETTER FROM THE CHIEF PRIVACY OFFICER

Both the United States and Europe have acknowledged that the exchange of information is an essential tool to fight the global terrorist threat. As we have thought more about current needs and how best to appropriately share information for homeland security purposes, we also have recognized the necessity to take on hard questions concerning the proper limitations on collection and use of data and safeguards for personal information received and shared by government. Democracies worry about such questions because it is an imperative to maintaining the fundamental freedoms and rights we enjoy – the values and way of life we seek to protect from the tyranny of terrorism.

Privacy is recognized in Europe and the United States as an essential right and fundamental value that is well developed in law and custom. We look forward to continuing to work together with European countries and the European Union to honor and integrate privacy protections into the means and practices through which we carry out our homeland security missions.

Both appropriate information sharing and privacy protection are important and the two principles must work together in tandem. This is recognized by senior government leaders on both sides of the Atlantic. These principles also were recognized by the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), in its Undertakings of May 11, 2004, concerning Passenger Name Record (PNR) information sharing, and within the U.S.-EU PNR Agreement of May 28, 2004.

The intent of the framework information sharing arrangement is to allow appropriate information sharing to facilitate safe, transatlantic travel and to fight terrorism and other serious crimes. Both sides recognize, however, that access to personal information

should not be unlimited and should be appropriately tailored, both in use and in the treatment of information received. That is why privacy is mentioned throughout the Undertakings and why both sides spent significant amounts of time working to build in operational privacy protections that would allow for necessary and appropriate sharing of individuals' personal data for public safety.

While this paper and the Joint Review must not lose sight of the fundamental and shared security purposes behind the PNR Undertakings, it is my duty as Chief Privacy Officer for the Department to carry out the mandates of Section 222 of the Homeland Security Act. Our enabling statute directs the Department and my role, in particular, to ensure that privacy attentiveness and privacy protections are integrated into the way the Department carries out our Homeland Security mission. I am pleased, along with my staff, to take on this policy and operational oversight role, both as an inside counselor to the Directorates, component agencies and offices within the Department, and in a necessary external role in reporting on progress and areas for continuing effort.

During the course of this past year, the Privacy Office has reviewed efforts by U.S. Customs and Border Protection to fully implement the Undertakings, as contemplated by the information sharing framework for PNR between the Department and the European Union. CBP has worked diligently with the Privacy Office during the review, including providing documents and information as needed. The efforts of CBP are applauded. I would like to personally thank Commissioner Robert Bonner, Deputy Commissioner Deborah Spero, and Executive Director for Border Security and Facilitation, Robert Jacksta and the CBP team he leads, for their efforts and partnership.

Based upon the Privacy Office review, I can report that CBP has achieved compliance with the representations made in the

Undertakings. While the overall report is positive, we believe that certain policy and operational elements took longer than anticipated to implement. As a result, in addition to guidance on necessary compliance measures, the Privacy Office also required certain remediation steps. CBP agreed to accept both the guidance and remediation required and has fully implemented both.

CBP has shown a willingness to go beyond the requirements of the Undertakings in many cases and to invest on the front end in an information architecture that addresses privacy protections. Additionally, where compliance was not complete during the development of the information system architecture, CBP has taken steps to fully remediate at the request of the Privacy Office. These actions demonstrate the integrity of the Agency and its commitment to integrating appropriate privacy protections into its policies, business processes and technical procedures.

This report summarizes the Privacy Office's review, issues that were raised, guidance shared, and the progress that was achieved during the course of this year.

Signed.....

II. EXECUTIVE SUMMARY

The fundamental purpose of the Joint Review is to serve as a constructive exercise that contributes to the effective operation of U.S. Customs and Border Protection's Undertakings of May 11, 2004, concerning PNR information derived from flights between the European Union and the U.S. The review conducted by the Department of Homeland Security Privacy Office regarding CBP's implementation of the Undertakings, from November 2004 through September 2005, also was conducted in this spirit.

Deleted: |

As of the date of the Joint Review, the Privacy Office finds that CBP is in compliance with representations made in the Undertakings. CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance with the Undertakings. This is a recognizable achievement, particularly considering the state-of-the-art technology solutions that CBP voluntarily undertook to fully implement the Undertakings through the information technology (IT) systems used by CBP offices nation-wide.

During the course of the review this year the Privacy Office found areas for improvement and focus by CBP in order to reach full compliance with the Undertakings. Depending on the nature of the improvement, the Privacy Office made the following determinations: remediation required, recommendations, and areas to monitor closely. While CBP's overall efforts were responsive and the technological solutions are quite sophisticated, some policy and operational measures to meet full compliance took a lengthy period of time to achieve. At this date, however, the Privacy Office can report that all guidance recommended, whether as a remediation requirement, a recommendation, or direction to monitor areas closely, has been accepted by CBP. To that end, both CBP and Border

and Transportation Security leadership and staff are applauded for their partnership in meeting the challenge of being stewards for the Department's privacy and security mandate.

The following is a summary of the DHS Privacy Office review in two parts:

A. Compliance

- As of the date of the Joint Review, CBP is compliant with representations made in the Undertakings.
- We have had no reports of any deliberate misuse of PNR information received. Further, responsible measures have been undertaken to address system deficiencies that were identified by the Privacy Office prior to the full technical solutions implemented to CBP's IT systems to comply with the Undertakings.
- CBP has invested substantial time, capital, and expertise to fully comply with the Undertakings, both through practices and procedures and through the use of its technology systems.
- CBP, with advice and guidance from the DHS Privacy Office, issued privacy notices and implemented suggested improvements for compliance with the representations in the Undertakings, including the development of compliant information system technology architecture.
- CBP instituted specialized training for its officers on handling PNR derived from flights between the U.S. and the EU.

- New procedures were put in place to track and respond to requests from individual travelers for information related to PNR; CBP's systems were modified to reflect the terms of the Undertakings.

B. Remediation and Best Practices Required by Privacy Office

- *Review and Delete Sensitive Terms.* CBP agreed to delete "sensitive" (b)(5) - Atty Client & Delib agreed to in the Undertakings, which were gathered prior to March 14, 2005, when a functioning technological solution was fully implemented to delete all "sensitive" terms and codes. (b)(5) - Atty Client & Delib collected between May 28, 2004 and March 14, 2005, were deleted. The deletion was completed on (b)(5) - Delib and verified by the Privacy Office.
- *Review and Delete Data outside the 34 permitted elements.* CBP agreed to delete data elements beyond the 34 data elements noted in the Undertakings which, in certain cases, were gathered prior to (b)(5) - Delib when a functioning technological solution was fully implemented to assist in complying with the Undertakings. Excess data elements collected between May 28, 2004 and (b)(5) - Delib 2005 were deleted. This deletion was completed on (b)(5) - Delib 2005 and verified by the Privacy Office.
- *Review Audit Logs for PNR Manually Accessed and Plan for Proper Retention Periods.* For the period from May 28, 2004 to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an appropriate retention period for the data

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

when it is unable to determine if PNR was manually accessed. It will implement the shorter retention period of 3.5 years in these cases, as contemplated by the Undertakings. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

- *Plan Required for Scheduling Routine Reviews of the Use of PNR Information.* In response to remediation guidance from the Privacy Office, the Office of Management Inspections and Integrity Assurance (MIIA) has established a proactive plan for reviewing audit logs associated with CBP's automated system ("the automated system") which maintains the relevant personal information covered by the Undertakings and the PNR arrangement. The purpose of their audit function is to review the use of PNR information. Additionally, the Office of Information and Technology, since May 30, 2005, has been auditing the system weekly for unauthorized use of all PNR data.
- *Electronic Tracking of Disclosures.* CBP added additional technical features that will electronically track whether a particular PNR has been disclosed and to what agency. This will lead to greater assurance for data integrity than the previous paper-based process, particularly so that if a correction is noted with respect to any PNR, all appropriate parties are notified. This change was completed on (b)(5) - Delib 2005. Electronic tracking is a best practice, but is not required by the Undertakings.
- *Audit Process for Access to Airline Reservation Data.* CBP added additional auditable mechanisms for confirming that supervisory approval is sought before CBP Officers

are able to manually access airline reservation data. This change was completed (b)(5) - Delib 2005. The IT audit mechanism is a best practice, but is not required by the Undertakings.

- Areas to Continue to Monitor Closely:
 - *Reconcile Guidance.* Upon conclusion of the Joint Review, CBP will update field guidance in order to capture all appropriate procedural changes, including recommendations that may be made by the Joint Review team, so that they may be properly implemented. The updated guidance will be disseminated to CBP Officers in the field.
 - *Data Disposition.* For records that are manually accessed but not associated with a law enforcement action, CBP will be archiving materials after 3.5 years. CBP is working on the technical solution and will have it in place prior to November 28, 2007, when this commitment will go into affect. It also is working on the deletion process that will need to be in place by November 28, 2015, at which time manually accessed PNR received since May 28, 2004 will start to be deleted consistent with the Undertakings.
 - *Approval of Data Retention Schedule.* CBP has drafted for approval a National Archives and Records Administration (NARA) data retention schedule for PNR that is in conformance with the Undertakings, and submitted it to NARA for consideration on March 29, 2005. The process can take up to six months or longer for NARA approval. CBP will inform the Privacy Office of NARA's determination.

CBP continues to refine its privacy program as it relates to PNR, which we are confident will contribute to the effective implementation of the Undertakings and the operations of CBP. CBP has made all recommended changes requested by the Privacy Office. The Privacy Office will continue to work with CBP in order to ensure that as the operational needs of CBP evolve, privacy protections are maintained.

III. HISTORY OF THE PNR ARRANGEMENT

In the aftermath of September 11th, the United States Congress enacted legislation authorizing the United States Department of Homeland Security's Bureau of Customs and Border Protection (CBP) to obtain access to passenger name records (PNR) originally collected by airlines and airline reservation systems for commercial purposes. More recently, in Section 7210 of the Intelligence Reform and Terrorism Prevention Act of 2004, the Congress also indicated that, where practicable, the Federal government should conduct passenger screening before individuals depart on a flight destined for the United States. Following these Congressional mandates, CBP actively uses PNR information as an initial screening tool to determine whether individuals of interest are planning to travel to the United States.

Beginning in 2002, following the publication of CBP's interim regulations implementing the PNR access requirement referenced above, the European Commission (EC) advised DHS that an EU Data Protection Directive generally prohibited cross-border sharing with non-EU countries, absent a demonstration that the receiving entity in a third country has adequate data protection standards.

Notwithstanding possible exceptions from the Data Protection Directive for law enforcement and national security purposes, as a

means to secure CBP's access to PNR and to provide certainty to the airlines and companies operating Global Distribution Systems (GDS), which may be subject to the EU Data Protection Directive, the U.S. and EU governing authorities committed to negotiate an arrangement to share information while maintaining safeguards for PNR data related to flights to and from the EU. An Interim Arrangement was reached in March, 2003, and CBP implemented guidance to ^{(b)(5) - Atty Client & Delib} in the field so that their treatment of PNR data received was consistent with the Interim Arrangement.

On May 28, 2004, an International Agreement regarding the processing of Passenger Name Records (PNR) was signed by the U.S. Department of Homeland Security (DHS) and the European Union (EU). The Agreement followed the issuance by U.S. Customs and Border Protection (CBP) of a set of Undertakings setting forth how CBP would process and transfer PNR data received in connection with flights between the U.S. and the EU and the subsequent issuance of an Adequacy Finding by the EU concerning such transfers. As part of the Undertakings, DHS and CBP provided for a Joint Review to take place between the U.S. and EU to examine CBP's implementation of the Undertakings.

The Undertakings sets up a compliance and complaint resolution role for the DHS Chief Privacy Officer. Prior to the upcoming Joint Review, the DHS Privacy Office conducted an internal review of CBP's implementation of the Undertakings' privacy measures. The internal review has been an iterative process of both reviewing the adequacy of CBP implementation efforts and the Privacy Office providing CBP with internal counseling and conformance measures for achieving consistency with the CBP representations in the Undertakings.

The Privacy Office provided constructive criticism and guidance on many aspects of CBP's implementation efforts at

different points along the review and implementation time line. This is entirely consistent with the internal function of the DHS Privacy Office to provide counsel and privacy policy and compliance direction within DHS. The Privacy Office also is facilitating the Joint Review of the implementation of the representations in the Undertakings on (b)(5) - Atty Client & Delib, (b)(6)

As of May 16, 2005, CBP's written policies and procedures, their actual implementation, and the technology solutions adopted for handling PNR received from the EU [REDACTED] substantial consistency with the Undertakings, dated May 11, 2004, as referenced in the U.S.- EU PNR Agreement, signed on May 28, 2004. In addition, as of September 16, 2005, CBP has implemented remediation and best practice enhancements in response to Privacy Office recommendations.

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. CBP staff made improvements to policies and procedures, both unilaterally by December 2004, and further modifications thereafter at the request of the Privacy Office during the course of the review.

For the periods during which CBP's implementation of the Undertakings was not consistent with representations made to the EU, remediation was necessary, as discussed previously in Section II of this report.

IV. DHS PRIVACY REVIEW: A CHRONOLOGY

The fundamental purpose of the Joint Review is a constructive

one. DHS and the EU, as Joint Review partners, share a view, "... to mutually contributing to the effective operation of the ... Undertakings" (Undertakings at paragraph 43), by periodically meeting to discuss implementation progress. The Privacy Office review also has been conducted in this spirit.

As specified in the Undertakings, the compositions of the Joint Review teams are a cross-section of privacy/data protection, law enforcement, and border and aviation security (Undertakings at paragraph 43, fn.13). In keeping with the Undertaking's dual values of law enforcement and privacy, the make-up of the review teams embodies both principles at the Joint Review.

A. The DHS Privacy Office

1. The DHS Privacy Office Mission

The mission of the Privacy Office is a constructive one. It is an independent voice meant to assist, counsel, recommend, and, where necessary, seek remediation to ensure protection of personal data. It serves a necessary self-critical role for DHS, but one that seeks improvement.

The DHS Privacy Office is the first statutorily required, comprehensive privacy operation in any U.S. federal agency. It operates under the direction of the Chief Privacy Officer, Nuala O'Connor Kelly, who is appointed by the Secretary. The Chief Privacy Officer serves as a steward of Section 222 of the Homeland Security Act of 2002, and the Privacy Office has programmatic responsibilities for the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act, and the numerous laws, Executive Orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personal and Departmental information.

The Privacy Office has oversight of privacy policy matters and information disclosure policy. It is also statutorily required to evaluate all new technologies used by the Department for their impact on personal privacy. The Privacy Office is required to report to Congress on these matters, as well as on complaints about possible privacy violations. Further, the Privacy Office is responsible for privacy-related education and training initiatives for DHS's more than 180,000 employees.

The construct of a privacy officer is similar, but not identical, to the construct of a data protection commissioner. The very principles that the two offices espouse are exactly the same: a constant vigilance to limiting intrusion, to questioning processes, to educating our employees, to encouraging reform, and to challenging and pointing out mistakes when necessary. At DHS, the Chief Privacy Officer's role and that of her Office is both inside and outside the agency. On the inside, the Privacy Office works to educate, to inform, to create processes and mandate attention to privacy and fair information principles in every evolution of new programs, new procedures, new policies, even the hiring and training of new personnel. On the outside, the Privacy Office champions DHS programs where appropriate, but criticizes where necessary. Also, the DHS Privacy Office reports directly to Congress on activities of the Department in a fair, if sometimes critical, way.

2. The DHS Privacy Office and the Undertakings

Consistent with the stated purpose of the Undertakings, the Privacy Office undertook its mission to contribute to the protection of privacy interests relative to PNR data. Further, the Privacy Office, along with the Border and Transportation Security Directorate and CBP, is facilitating the Joint Review of the implementation of the representations in the Undertakings on EU PNR.

As essential background to the Joint Review, it is worth reviewing the various duties of the Privacy Office as defined in the Undertakings: a) oversight and investigation of disclosure, retention and disposal issues related to PNR; b) resolution of complaints between individuals and CBP; and c) point of contact for Data Protection Authorities (DPAs) in the EU member states on behalf of an EU resident.

Deleted: serves

- a. First, Oversight and Investigation. Paragraph 31 recognizes that the Privacy Office has authority to investigate and report on failures to respect conditions for transfer of PNR data with Designated Authorities. We may make findings that the designated authority is ineligible to receive further transfers of PNR data. To date the Privacy Office has not found any of the agencies with which PNR was shared to be ineligible. The review of the policies and procedures surrounding sharing indicates consistency with the representations of the Undertakings.
- b. Second, Resolution of Complaints. Paragraph 41 serves as an appellate function to resolve complaints between individuals and CBP. The Chief Privacy Officer is independent of any directorate within DHS and is statutorily obligated to insure that personal information is used in a manner that complies with relevant laws. To date, the Privacy Office has received no complaints regarding the use of PNR and the Privacy Office has found no instances of misuse of PNR derived from flights between the U.S. and EU by CBP.
- c. Third, Point of Contact and Reporting to Congress. Paragraph 42 establishes the Privacy Office as a point of contact for EU data protection authorities when one of its residents does not believe his/her concern has been satisfactorily addressed by

CBP. The Privacy Office will address such complaints on an expedited basis and report back to the member country, as well as to Congress. There have been no requests or complaints received directly by the Privacy Office from any DPA since the Undertakings were issued in May 2004.

B. CBP

1. CBP Mission:

CBP is the unified border agency within DHS. Under the Homeland Security Act, the U.S. Customs Service was renamed CBP and the inspectional and border patrol elements of the former Immigration and Naturalization Service (INS), and the inspectional elements of the Department of Agriculture, were transferred to CBP. As the single, unified border agency, CBP's mission is vital to the protection of the United States. While its priority mission is to prevent terrorists and terrorist weapons from entering the United States, CBP is also responsible with enforcing all import and export laws, while also facilitating the flow of legitimate trade and travel. CBP uses multiple strategies and employs the latest in technology to accomplish its dual goals. CBP's initiatives are designed to protect the U.S. from acts of terrorism, and reduce the vulnerability to the threat of terrorists through a multi-level inspection process.

2. CBP Efforts

In the U.S., we tend to look at technology risks as well as technology solutions that recognize the appropriate use of information and guard against harm and misuse of personal information. To that end, CBP undertook an analysis not only of policies and procedures, but of their technology systems. With assistance and guidance from the Privacy Office, CBP worked to implement the Undertakings representations. CBP also actively

looked for ways they could improve handling PNR received from the EU.

DHS and the EU were aware from the start that many of the representations in the Undertakings would require DHS and CBP in particular, to make substantial technological changes to its systems, as well as changes in policy, the implementation of which would take time. For example, Officers of CBP with access to PNR received specialized training on handling PNR derived from flights between the U.S. and the EU; new procedures were put in place to track and respond to requests for information related to PNR; and CBP's systems were modified to reflect the terms of the Undertakings.

C. Chronology of the Review

In August 2004, the Privacy Office began discussing the internal review process with Customs and Border Protection (CBP). In November 2004, Nuala O'Connor Kelly, Chief Privacy Officer, DHS, contacted Robert Bonner, CBP Commissioner, to recommend an outline of how the internal privacy review would be conducted, and present the criteria that would be used for measuring consistency with the representations in the Undertakings. The internal review described in this report has assessed CBP's effectiveness in acting consistently with those representations.

1. The DHS PNR Review Team

The DHS PNR Review team was led by Rebecca J. Richards, Director of Privacy Compliance, with technical assistance from Peter Sand, Director of Privacy Technology, and Anna Slomovic, Sr. Privacy Analyst. Technical implementation of the Undertakings in the CBP systems has been reviewed by Robert Bollig from the DHS Office of the Chief Information Officer (OCIO). Maureen Cooney, Privacy Office Chief of Staff and Director of International Privacy

Policy, and Elizabeth Withnell, Chief Counsel to the Privacy Officer provided assistance and counsel. The Review team has extensive compliance, privacy policy, legal, and technical expertise.

2. DHS PNR Review

The review consisted of an analysis of existing policies and procedures, interviews with key management and staff that handle PNR, and technical review of CBP systems and documentation.

The Privacy Office has reviewed the following materials:

- Data lifecycle map;
- Privacy notices to travelers;
- Documented procedures for specific areas relating to collection, use, sharing, and retention of personal information;
- Training materials;
- Contacts with third party agencies including information requests that have been honored; and
- Technical logs that may be pertinent.

Interviews included:

- CBP's National Targeting Center (NTC) Management on policies, procedures and use of the system;
- Passenger Analytic Unit (PAU) training team (individuals who handle PNR on a regular basis);
- Office of Information Technology (OIT) regarding:
 - Privacy training;
 - Sensitive filters and associated timelines;
 - IT User and Functional Requirements being developed to comply with the Undertakings;
 - How CBP's automated system operates; and

- The Customer Satisfaction Unit (CSU).

In addition, the Review Team received a written statement from the Office of Management Inspections and Integrity Assurance (MILA) with examples of how they detect internal problems and perform audits.

CBP's OIT worked with Office of Field Operations (OFO) and the Chief Counsel's Office (OCC) to create technical/technological implementation and enforcement of many of the Undertakings.

Technology implementations were developed, tested, and deployed beginning March 14, 2005. This first phase included the implementation of "sensitive" terms and codes filters, and filtering for the 34 data elements noted in the Undertakings. On May 13, 2005, CBP finalized functional changes to its automated system. This included changes to access control requirements and supervisory approval functions.

Based on the results of our review, the Privacy Office has outlined areas of consistency with the representations in the Undertakings, (b)(5) - Delib

V. FINDINGS

During the period of the Privacy Office review, in particular, CBP has worked hard to ensure that its policies, procedures, and information technology conform to the representations in the Undertakings. As stated above, some of the provisions of the Undertakings were covered by existing laws, regulations, policies, and procedures with which CBP complies. Other provisions required the expenditure of extensive time, effort and resources by

CBP's operations, technical and counsel staff to build the strong program that has brought them into full consistency with the representations in the Undertakings, as of September 16, 2005.

A. Areas of Consistency

Below are significant CBP activities that demonstrate consistency with the Undertakings:

- The bi-annual privacy training that is required for all CBP officers with access to CBP's information systems is informative and well-developed. The examination at the end of the training requires a working knowledge of privacy to pass and gain or retain access to CBP systems.
- CBP's field guidance on handling PNR data derived from flights between the U.S. and EU tracks the Undertakings, and provides excellent training to CBP Officers in the field and at CBP's National Targeting Center (NTC).
- The policies and procedures for disclosure of PNR to third parties, both internal to DHS and external to DHS, are well developed.
- The CBP requirement that all individuals who have access to PNR sign off on notice of the field guidance is recorded specifically in the training portion of CBP's personnel tracking system. This tracking demonstrates the seriousness with which CBP is taking the Undertakings and its full implementation of representations made on behalf of the U.S. to the EU.
- The IT User Requirements have been developed in great detail and in collaboration between operations, technical, and counsel staff. Their deployment on May 13, 2005, provides technical

support for consistency with the representations in the Undertakings, as articulated in CBP field guidance.

- The updates to policies regarding the approval process for gaining access to CBP's automated system have decreased the number of individuals overall who have access to PNR.
- The updated access roles for users of CBP's automated system have been well thought out and reduce the number of users with access to PNR seven (7) days after completion of travel by over forty percent (40%).
- The filters for sensitive terms and codes as provided for in the Undertakings have been deployed and have been working successfully since March 14, 2005.
- PNR data derived (b)(5) - Atty Client & Delib between the EU and the U.S. has also been automatically filtered to ensure it has a nexus to the U.S. This update was implemented on March 14, 2005.
- CBP has provided guidance to its Freedom of Information Act (FOIA) personnel on how to handle requests from individuals that either specifically request PNR or who ask for information more generally.
- CBP has implemented regularly scheduled processes to obtain PNR data, thereby decreasing the occurrence of manually accessed PNR data.
- For records that are manually accessed but not associated with a law enforcement action, CBP will be archiving materials after 3.5 years. CBP is working on the technical solution and will have it in place prior to November 28, 2007, when this provision will go into effect.

B. Undertakings: Section by Section Review

This section discusses the policies, procedures, practices, and IT support related to various areas of the Undertakings.

1. Legal Authority to Obtain PNR (Paragraph 1 of the Undertakings)

The Undertakings state that CBP has legal authority to collect the PNR.

CBP collects PNR data as authorized by legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing regulation.

Deleted:

CBP issued field guidance specific to the PNR related to flights between the United States and European Union Countries on December 20, 2004. This guidance reflects the terms of the Undertakings. On March 14, 2005, an automated system was deployed that filters and tags PNR related to flights between the United States and European Union countries, which further strengthened compliance with the Undertakings.

Findings: Based on review of documented procedures, regulations, and applicable U.S. laws, CBP operates in a manner consistent with the representations in the Undertakings document.

2. Use of PNR Data by CBP (Paragraph 2-3 of the Undertakings)

The Undertakings lay out specifically the scope for which PNR data may be used by CBP.

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

(b)(5) - Atty Client & Delib

who work within the PAUs and CBP's NTC are

trained to identify passengers who are considered high risk and have received additional training in the form of written field guidance.

This field guidance is consistent with the scope of purposes identified in the Undertakings. All (b)(5) - Atty Client & Delib with access to PNR data are required to review and sign an acknowledgment of this guidance. This is logged in the training system so that it may be regularly reviewed by Headquarters staff to ensure that the field staff are properly trained on the use and disclosure of the data.

(b)(5) - Atty Client & Delib

Although the mission of CBP is broader than the three purposes specified in the Undertakings, CBP's use of PNR data is fully consistent with the three stated purposes in the Undertakings.

Findings: Based on review of documented procedures, technical measures and, in-person interviews, CBP operates in a manner consistent with the representations in the Undertakings.

3. Data Requirements

(Paragraph 4-8 of the Undertakings)

The Undertakings set forth CBP's specific PNR data requirements and also specify when and how additional information may be obtained by CBP.

On March 14, 2005, CBP's automated system was updated to capture only the 34 PNR data elements identified in the Undertakings from an air carrier's system and parse it so that the data can be viewed consistently across air carriers. Any elements outside of the 34, for example number of bags, will be filtered so that the information may not be viewed and is not retrievable. At the same time, CBP deployed the sensitive term and code filters, which delete all sensitive terms and codes that were mutually identified between the EU and U.S. on November 3, 2004. The original PNR is filtered and sensitive terms cannot be re-created.

On May 13, 2005, CBP deployed updates to the automated system to reduce the number of users who have access to PNR. The system limits who may access the OSI and SSI/SSR open fields. The user must receive specific approval before viewing these fields. An audit trail is created when the OSI and SSI/SSR fields are accessed.

PAUs and the NTC do not have investigative responsibilities. If, based on the information available to PAU and NTC officers, additional information about an individual must be obtained from sources outside the government, the officers may contact appropriate law enforcement authorities for further investigation. Those law enforcement authorities can then obtain additional data through lawful channels. Officers are trained on these procedures prior to gaining access to PNR.

CBP anticipates working with the EU if it finds that additional data fields are required beyond the 34 data elements identified in the Undertakings.

Due to the cancellation of the CAPPs II program, there was no transfer of PNR data for any purpose related to this program. There have been no bulk transfers to any agency of PNR data which CBP obtains pursuant to its legal authority.

Findings: Based on an extensive technical review of the system as well as a review of the documented policies, procedures, training, interviews, applicable regulations and U.S. law, CBP is in compliance with the representations in the Undertakings for data collected as of May 13, 2005. For data received between May 28, 2004 and March 14, 2005, the Privacy Office required CBP to review and filter data elements that were received beyond the 34 data elements set forth in the Undertakings and to permanently delete these items. CBP agreed, and the deletion process was complete by (b)(5) - Delib 2005 and was verified by the Privacy Office.

4. Treatment of "Sensitive" Data (Paragraph 9-11 of the Undertakings)

The Undertakings specify that "sensitive" data will be filtered and deleted.

(b)(5) - Atty Client, & Delib are trained to follow the Undertakings on the proper use of sensitive personal information such as race, color, age, sexual orientation, religion, sex, national origin, or disability for purposes of identifying persons of concern. The "Standards of Conduct," agency guidance that provides standards of behavior for all CBP employees, specifically states: "Employees will not act or fail to act on an official matter in a manner which improperly takes into consideration an individual's race, color, age, sexual orientation, religion, sex, national origin, or disability." All CBP employees receive a copy of the Standards of Conduct at the start of employment.

(b)(5) - Atty Client & Delib

CBP's "Table of Offenses and Penalties," which provides guidance to CBP managers, supervisors and practitioners on the appropriate penalties to apply in typical cases of employee misconduct, provides for anywhere from a fourteen (14) day suspension to removal from employment for "[a]cting or failing to act on an official matter in a manner which improperly takes into consideration an individual's race, color, age, sexual orientation, religion, sex, national origin, or disability." (Section B(2), Discriminatory Behavior).

In addition to the general training that all (b)(5) - Atty Client & Delib receive, those in the PAUs and CBP's NTC are specifically reminded that the identification of individuals for the purposes of focusing further investigation based on race, religion, or sex is prohibited.

(b)(5) - Atty Client & Delib

Prior to the implementation of the sensitive data filters in March of 2005, CBP field guidance provided that CBP officers were not allowed to use "sensitive" terms and codes, as mutually identified by

the U.S. and EU. The guidance required that for discretionary disclosures outside of CBP, either internally to DHS or externally to other government agencies or foreign countries, sensitive data had to be removed prior to disclosure. For non-discretionary disclosures, field guidance provided that the CBP officer consult with appropriate counsel to determine what must be disclosed. On March 14, 2005, CBP deployed the "sensitive" data filter, which deletes all sensitive terms and codes, as agreed by the U.S. and EU on November 3, 2004. With the implementation of the "sensitive" data filter, no such terms or codes will appear in the PNR. For PNR received between May 28, 2005 and March 14, 2005, CBP has deleted all "sensitive" terms and codes; therefore manual redaction is no longer necessary.

Deleted: a

An item was included in the field guidance issued to CBP supervisors highlighting the key points that must be reviewed prior to further dissemination of the guidance to CBP Officers in the field. This insured that supervisors were providing consistent training across the different ports. After receiving and reviewing field guidance, all CBP Officers were required to sign a statement that they read and understood it.

Findings: Based on an extensive technical review of the system as well as a review of the documented policies, procedures, training, interviews and applicable regulations and U.S. law, CBP is in compliance with the representations in the Undertakings for data received on or following March 14, 2005. For data received between May 28, 2004 and March 14, 2005, the Privacy Office required CBP to review data and filter (b)(5) - Atty Client & Delib terms permanently delete these items. CBP agreed to this remediation course and it was completed by (b)(5) - Delib 2005 and compliance was verified by the Privacy Office.

(b)(5) - Atty Client & Delib

5. Method of Accessing PNR Data (Paragraph 12-14 of the Undertakings)

The Undertakings provide for specifics on when and how often CBP may access PNR from air carrier systems.

Before accessing airline reservation data in the automated system, CBP Officers encounter several system prompts and reminders of field guidance and policies regarding the authorized use of PNR data. Each user must click "I agree" to such statements before he or she is given access to the system.

PNR data derived between the EU and the U.S. has also been automatically filtered to ensure it has a nexus to the U.S. This update was implemented on March 14, 2005.

CBP is working with several air carriers and Global Distribution Systems (GDSs) to develop a "push" system that meets the needs of all parties and has had preliminary conversations with representatives of some of the major reservation systems. Currently, CBP is testing a "push" system with the airlines to modernize reservation data access and dissemination methods.

PNR data is retrieved no earlier than 72 hours prior to scheduled flight departure. Non-routine retrievals are documented both manually and electronically. In addition, field guidance provides specific processes and reporting requirements to be followed in cases where PNR data is manually accessed.

Findings: Based upon a review of the technical system and documented policies and procedures, beginning May 13, 2005, CBP is in compliance with the representations in the Undertakings. For the period from May 28, 2004 to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an

appropriate retention period for data when it is unable to determine if PNR was manually accessed. It will implement the shorter retention period of 3.5 years in these cases, as contemplated by the Undertakings. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

6. Storage of PNR Data (Paragraph 15 Undertakings)

The Undertakings provide for specific requirements regarding who may have access to PNR and for how long different data sets may be maintained by CBP.

Access: CBP has issued guidance requiring supervisory approval for user access to the automated system. Access privileges are also discontinued after a specified period following lack of use of the system by an authorized user.

On May 13, 2005, CBP deployed four new user roles that restrict the number of individuals with access to PNR for set periods of time:

- Group I Users have access to CBP's automated system, but are not able to view PNR;
- Group II Users have access to PNR for 7 days after the last day of travel and must obtain supervisory approval to view OSI and SSI/SSR open fields;
- Group III Users have access to PNR beyond 7 days after the last day of travel and must obtain supervisory approval to view OSI and SSI/SSR open fields;
- Group IV Users have access to PNR beyond 7 days after the last day of travel, are able to access OSI and SSI/SSR open fields as needed, and provide permission to those in the previous group that cannot view the open fields without permission.

The number of users who can access a particular PNR drops by over forty percent seven days after completion of travel.

The system restricts users in the appropriate groups to reviewing data only for the appropriate time periods. The system is also able to flag what PNR has been accessed manually and what PNR is related to a law enforcement action so that the information is maintained for the appropriate retention periods.

To ensure that the system is being accessed and used appropriately, audit logs are being created for all access to PNR data.

Retention: CBP continues to work on its National Archived Records Administration (NARA) retention period. A NARA retention schedule has been drafted and submitted to NARA. The process takes roughly six months from March 29, 2005. CBP will notify the Privacy Office of NARA's determination.

CBP is unable to differentiate manually accessed PNR data from other data that was received between the period of May 28, 2004 and May 14, 2005. After the implementation of the access controls on May 14, 2005, CBP obtained the ability to differentiate PNR connected to a law enforcement action. CBP anticipates the development of a mechanism, well in advance of the November 28, 2007 deadline, that will determine when these records will need to be deleted or archived.

Findings: Based upon review of documented policies and review of the technical system, CBP is substantially compliant with the representations in the Undertakings. For the period from May 28, 2004 to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an appropriate retention period

for data when it is unable to determine if PNR was manually accessed. It will implement the shorter retention period of 3.5 years in these cases, as contemplated by the Undertakings document. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

7. CBP Computer System Security (Paragraphs 16-23 of the Undertakings)

The Undertakings require that specific technical and training requirements are met to ensure the security and privacy of the system, and that appropriate disciplinary actions can be taken if a problem arises.

CBP's automated system is Certified and Accredited (C&A) under the Federal Information Security Management Act (FISMA). Formal accreditation was issued in February 2003. The C&A is performed every three years.

The automated system is only accessible through the CBP intranet. All information is read only. No other foreign, federal, state, or local agency has direct electronic access to the PNR data.

Access to PNR is controlled through the automated system. Multiple layers of approval are needed for PNR access. Individuals must have a favorable background check, local supervisory approval, Headquarters approval, and approval from the Office of Information Technology.

All (b)(5) - Atty Client & Delib with access to systems containing PNR data must (b)(5) - Atty Client & Delib take privacy awareness training and pass an exam every two years. User access is denied if an individual does not take the online class and pass the exam. Supervisory approvals are necessary to regain access to the system. In accordance with CBP policy, failure to complete privacy and security training may be documented in the

individual's file.

Training covers the appropriate use and disclosure of personal information by (b)(5) - Atty Client & Delib. It gives an excellent overview of the Privacy Act requirements and application of the third agency rule that are being fully implemented for PNR data. Training also covers Freedom of Information Act (FOIA) and overall required privacy practices. The training includes a test that requires a working knowledge of privacy to pass and gain or retain access to the system.

(b)(5) - Atty Client & Delib

CBP's "Table of Offenses and Penalties" guidance provides for an appropriate penalty for using government property, property under government custody, or the property of others, for other than official purposes, which includes querying confidential or sensitive databases for other than official purposes. A first offense leads to anywhere from a written reprimand to a fourteen (14) day suspension, and a second offense, anywhere from a fourteen (14) day suspension to removal, depending on the nature of the infraction. (Section J(3), Misuse of Property).

Office of Management Inspections and Integrity Assurance (MIIA) tracks all access to and activities on CBP's automated system. Users are reminded of this every time they log on. MIIA does not have an automated alert system at this time, but has been discussing such an option for several CBP systems, including the automated systems used for PNR. The Integrity Programs Division of MIIA conducts proactive periodic general data queries. MIIA will begin a program of scheduled audits of access to CBP's automated system. (b)(5) - Atty Client & Delib

As a law enforcement agency, CBP (and its predecessor, U.S. Customs Service) has a long history of ensuring compliance. (b)(5) - Atty Client & Delib have a legal obligation to ensure compliance with laws, regulations, and agency policies and take their duties seriously. They

are required to, and regularly do, report issues and concerns to the CBP Joint Intake Center in the MIIA or DHS, Office of Inspector General (OIG). If the allegation might have a criminal predicate, it is investigated by the OIG or referred to the Immigration and Customs Enforcement (ICE), Office of Professional Responsibility. If the allegation is not considered to have a criminal predicate, MIIA will routinely refer the matter to CBP management for administrative inquiry and action.

Findings: Based upon review of training materials, documented policies, and procedures and the technical system, CBP is in compliance with the Undertakings. OIT conducts routine audits of the system weekly for unauthorized use of all PNR data. Additionally, MIIA will begin a program of scheduled audits of access to CBP's automated system (b)(5) - Atty Client & Delib

8. CBP Treatment and Protection of PNR Data (Paragraphs 24 – 27 of the Undertaking)

The Undertakings require that PNR data be afforded appropriate protection when requests for disclosures are made.

When users enter CBP's automated system, a notice reminds them that the system contains trade secrets and information protected by the Privacy Act. They are also reminded about the fines associated with inappropriate use. The log-in page also carries a reminder that the information in the system is law-enforcement sensitive.

CBP has existing policies and procedures for handling of FOIA and Privacy Act requests in compliance with the law. PNR requests received are handled in accordance with these policies. CBP's field guidance on PNR specifically describes how requests for information and correction should be handled relative to PNR.

On May 16, 2005, at the request of the Privacy Office, additional guidance was issued to all FOIA and Customer Satisfaction Unit (CSU) staff directing them to send all FOIA requests related to PNR, whether specifically requesting PNR or that may be read to include PNR, to the PNR Program Officer for further research and response. This memo directs the staff to log EU PNR requests separately and to forward any requests for amendment to PNR to the PNR Program Officer.

Findings: Based on review of documented policies and procedures and the system that handles the disclosures, CBP is in compliance with the representations in the Undertakings.

9. Transfer of PNR Data to Other Government Authorities
(Paragraphs 28-35 of the Undertakings)

The Undertakings lay out how PNR may be transferred to other government authorities outside of CBP.

DHS components are not treated as "third agencies" for Privacy Act purposes and no special "routine use" legal requirements for data transfer typically apply, other than a need for the specific information. CBP field guidance provides specific requirements for how information related to PNR derived from flights between the EU and U.S. is to be transferred outside CBP. The guidance states that DHS and its components are to be treated as "third agencies" for the purposes of data transfer. CBP maintains a file of all disclosures that have been made to other parts of DHS and a file of all disclosures made to outside agencies. There have been no disclosures to foreign agencies as of September 16, 2005.

Through the privacy awareness training required for all officers of CBP with access to systems containing PNR and other sensitive data, CBP trains officers repeatedly that information should only be

disclosed for specific purposes with prior approval and written documentation. The documentation must include why information was disclosed, to whom, and under what circumstances. There are specific questions on the privacy awareness training test regarding proper and improper disclosure of information. Officers must pass this test in order to gain and maintain access to the information systems at CBP and then on a biannual basis to maintain their access to the system.

CBP field guidance provides specifics regarding how and when PNR derived from flights between the U.S. and EU may be released. All disclosures must be requested in writing and only under exigent circumstances may such PNR data be disclosed based on a verbal request. In the instance of verbal requests, a written request must be submitted as soon as possible. The written request must indicate

who is requesting the information and for what purposes. The [REDACTED] (b)(5) - Atty Client & Delib

[REDACTED] must review and ensure that the government authority requesting the information has law enforcement or counterterrorism functions and that the subject PNR is being requested for the scope defined in the Undertakings. PNR may also be disclosed to relevant government authorities where necessary to protect the vital interests of a data subject or others. [REDACTED] (b)(5) - Atty Client & Delib

[REDACTED] pursuant to paragraph 34 of the Undertakings. All responses with the PNR must have the following disclosure:
"Property of U.S. Customs and Border Protection. This document is provided to your agency for its official use only and remains the PROPERTY OF U.S. CUSTOMS AND BORDER PROTECTION (CBP). This document contains confidential personal information of the data subject ("Official Use Only") and confidential commercial information and may not be disclosed to any third party without the express prior written authorization of CBP." In addition, CBP has provided field officers with routine language that must be used for all disclosures in addition to the information noted above.

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

Prior to the implementation of automated filters to remove sensitive data, CBP Officers manually removed sensitive data in cases of discretionary disclosure outside of CBP, either internally to DHS or externally to other government agencies or foreign countries. For non-discretionary disclosures, field guidance required that (b)(5) - Atty Client & Delib [REDACTED] consult with appropriate counsel to determine what would be disclosed.

Disclosures of PNR must be recorded and reported to CBP Headquarters on a monthly basis. Headquarters maintains a log of all disclosures that occur both within DHS and externally to other agencies. At the request of the Privacy Office, CBP is implementing a set of technical fixes to allow it to more efficiently monitor the disclosures of information that may be subsequently changed because of a request for correction by a data subject. This update (b)(5) - Atty Client & Delib [REDACTED] although it is not a requirement under the Undertakings. As of September 16, 2005, PNR has been shared in a small number of cases with other Department of Homeland Security component agencies or other [REDACTED] government law enforcement (b)(5) - Atty Client & Delib [REDACTED] authorities that have a need to know to carry out their official duties. All were consistent with the scope of the Undertakings and had the notice above attached to the data.

Findings: Based upon available information and documented policies and procedures, training materials, and the system handling disclosures, the Privacy Office assessment is that CBP is complying with the representations in the Undertakings.

10. Notice, Access, and Opportunities for Redress for PNR Data Subjects
(Paragraphs 36-44 of the Undertakings)

The Undertakings reflect that CBP will provide individuals with notice,

access to their records, and opportunities for redress.

CBP has developed the Customs and Border Protection Passenger Name Record Privacy Statement for PNR Data Received in Connection with Flights Between the U.S. and the European Union. The statement discusses why CBP receives [REDACTED] data, who has access to it, how long data is retained, and how questions and complaints may be filed and appealed.

CBP has a Customer Satisfaction Unit and Freedom of Information Action Officers who respond to requests from the public and handle all requests related to PNR. If a passenger has an issue upon entry into or exit from the country, the first recourse is to speak with a supervisor at the Port of Entry and handle the issue. If the passenger has questions or concerns, the passenger will be given a general fact sheet that directs individuals to contact the FOIA/Customer Satisfaction Unit with any further questions if the issue cannot be resolved while the individual is still at the port.

On May 16, 2005, additional guidance was issued to all FOIA and Customer Satisfaction Unit (CSU) staff directing them to send all FOIA requests related to PNR, whether specifically requesting PNR or potentially related to PNR, to the PNR Program Officer for further research and response. This memo directs the staff to log requests for [REDACTED] separately and to forward any requests for amendment to PNR to the PNR Program Officer.

FOIA requests received by CBP are handled in accordance with Title 19, Code of Federal Regulations, Section 103.5 and CBP directives. Field guidance on EU PNR reiterates existing statutory provisions and states that first party requests for personal information shall be processed without asserting any exemption based on the fact that the data is confidential personal information of that data subject (5 U.S.C. 552(b)(6)) or that it is confidential commercial information of the air

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

carrier (5 U.S.C. 552(b)(4)). Other exemptions, however, may be applied as appropriate. Requests by persons other than the data subject will result in the assertion of these exemptions (5 U.S. C. 552 (b) (4) and (6)), as well as other applicable exemptions, and information will not be disclosed. This is consistent with the existing Customs Directive, DHS policy and the law.

Requests for corrections related to PNR data will be handled through both policies and procedures, and technical means. Field guidance states that if there is request made in the field, the (b)(5) - Atty Client & Delib should follow normal procedures for FOIA requests or amendment of records. If designated personnel in the NTC and the Security Office determine, whether through a request by the individual or on their own, that information in a PNR is inaccurate, a separate record in CBP's automated system will be created and linked from the PNR. This record will indicate the inaccuracy. The technical implementation will enable those who are authorized to make corrections to PNR records, to enter a FOIA tracking number into the correction record.

All corrections will be forwarded to the PNR Program Officer to determine whether the relevant information in the subject PNR has been disclosed to "third agencies." If disclosures of that information have been made, corrections will be forwarded to the appropriate parties.

If an individual has a concern, issue, or appeal after working with CBP, the matter may come to the attention of the Chief Privacy Officer. Customs and Border Protection Passenger Name Record Privacy Statement for PNR Data Received in Connection with Flights Between the U.S. and the European Union specifies that the DHS Chief Privacy Officer may review CBP decisions resolving inquiries and complaints.

Findings: Based on review of documented policies and procedures, as well as the system handling disclosures, interviews, and technical capabilities, CBP is in compliance with the representations in the Undertakings. At the request of the Privacy Office, CBP is implementing additional technical means to track the information that is shared to ensure that agencies that have received PNR information receive appropriate corrected information, including improvements to the data's integrity. This is a best practice measure and was not required by the Undertakings.

11. Usage Compliance Issues

(Paragraphs 43-44 of the Undertakings)

On July 22, 2003, CBP issued interim field guidance to provide (b)(5) - Atty Client & Delib with specifics on the handling of PNR consistent with the interim arrangement with the EU. On December 20, 2004, the Office of Field Operations issued guidance to all field offices and CBP's National Targeting Center to provide further guidance on (b)(5) - Atty Client & Delib specific to the Undertakings. During weekly musters at that time, CBP supervisors highlighted the high level issues that needed to be addressed as the guidance was distributed. Anyone with access to PNR signed an acknowledgment that they had received and understood the field guidance. This was tracked in the training system.

Findings: Based on review of documented policies and procedures, training materials and interviews, CBP is complying with the representations in the Undertakings.

C. AREAS FOR IMPROVEMENT

The DHS Privacy Office found areas for improvement during this review process. CBP has made all the recommended changes or provided a timeline for when the recommended changes will be

made. While CBP's overall efforts are good and the technological solutions are quite sophisticated, some efforts took longer than expected or should have. With the exception of language regarding the sensitive data elements that said "with the least possible delay," there was no provision in the Undertakings for a phased in approach to implementation (although arguably there should have been, as demonstrated by the fact that even after the issuance of the Undertakings and signing of the agreement, the list of "sensitive" data terms and codes were not settled by the parties until the fall of 2004). But, in any case, the reasonable expectation was for a speedier implementation.

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

1. Remediation

Efforts to remediate CBP treatment of PNR derived from flights between the U.S. and EU since issuance of the Undertakings and signing of the PNR Agreement were necessary to the extent that actual treatment had been inconsistent with formal representations to the EU and to citizens and other individuals whose data has been transferred since May of 2004.

- *Review and Delete "Sensitive" Terms.* CBP agreed to delete sensitive terms [REDACTED] in the Undertakings, which were gathered between May 28, 2004 and March 14, 2005, when a functioning technological solution was fully implemented to delete all "sensitive" terms and codes. The time period for the deletion was May 28, 2004 to March 14, 2005. The deletion was completed on (b)(5) - Delib 2005 and verified by the Privacy Office.
- *Review and Delete Data Outside the 34 Agreed upon Fields.* CBP has agreed to delete data elements beyond the 34 noted in the Undertakings which in certain cases were gathered between May 28, 2004 and March 14, 2005, when a functioning

(b)(5) - Atty Client & Delib

technological solution was implemented. The time period for the deletion was from May 28, 2004 to March 14, 2005. This deletion (b)(5) - Atty Client & Delib [REDACTED] 2005 and verified by the Privacy Office.

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

- *Review Audit Logs for Retention Periods.* For the period prior to May 14, 2005, CBP reviewed its audit logs and determined it was unable to differentiate accessing PNR for automated purposes and accessing PNR for manual purposes. CBP has undertaken the effort of determining and applying an appropriate retention period for data when it is unable to determine if PNR was manually accessed. It will implement the shorter retention period of 3.5 years, as contemplated by the Undertakings. PNR linked to an enforcement record will be retained for such time as the enforcement record is archived.

3. Recommendations

The following recommendations were made to strengthen consistency with the representations in the Undertakings and to generally enhance privacy interests. CBP has made all of these changes effective (b)(5) Delib [REDACTED]

- *Electronic Tracking of Disclosures.* CBP [REDACTED] additional technical features that will electronically track whether a particular PNR has been disclosed and to what agency. This [REDACTED] lead to greater assurance for data integrity than the [REDACTED] paper-based process, particularly so that if a correction is noted with respect to any PNR, all appropriate parties are notified
- *Website Contact Information.* CBP and the Privacy Office have updated their websites to include a phone number to receive

(b)(5) - Atty Client & Delib

comments, complaints, and concerns and to reflect the implementation of the "sensitive" data filters.

4. Areas to Continue to Monitor Closely

In some instances, the representations in the Undertakings will take effect over time and so the Privacy Office will continue to monitor the implementation over time. These activities include:

- *Update CBP guidance to the field.* Throughout the review process, CBP has refined its approach to protecting privacy to ensure that it is fully consistent with the Undertakings. At the conclusion of the Joint Review, CBP will make a single set of changes to field guidance to incorporate the minor changes that have been made operationally over the last year.
- For records that are manually accessed but not associated with a law enforcement action, CBP will be archiving PNR after 3.5 years. CBP is working on the technical solution and will have it in place prior to November 28, 2007, when this provision will go into affect. CBP is also working on the deletion process that will need to be in place by November 28, 2015, at which time manually accessed PNR received starting on May 28, 2004 will start to be deleted in accordance with the Undertakings.
- CBP has drafted for approval a National Archives and Records Administration (NARA) data retention schedule for PNR that is in conformance with the Undertakings. The schedule was submitted on March 29, 2005, to NARA and takes about six months to be approved.

E. Conclusion

During the course of the Privacy Review this year, CBP has

worked to make the changes required to bring it into full compliance with representation made in the Undertakings. The review helped to clarify the efforts required to fully actualize the framework for information sharing, including the necessity to build a technology system that integrated the Undertakings privacy provisions into the online operational screening process. This required a significant effort by CBP. While the discussions (b)(5) - Atty Client & Delib

Undertakings anticipated that it would take time to phase in the policies and operational measures to meet full compliance, the view of the Privacy Office is that it took too long on the part of our component agency CBP. For this reason, the Privacy Office made recommendations to CBP that would further enhance privacy protections above and beyond the obligations of the Undertakings. These recommendations were acknowledged, undertaken, and have been completed by CBP. The Privacy Office will continue to work closely with CBP to ensure that privacy protections are a part of any new operational policies and procedures implemented by CBP.

APPENDIX 1: PNR Agreement

[insert Agreement]

APPENDIX 2: PNR Undertakings

[insert Undertakings]

APPENDIX 3: Lifecycle ██████████ in CBP Operations

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



What is PNR?

Anyone traveling on a commercial air carrier into or out of the United States has a reservation known as the Passenger Name Record (PNR). PNRs are generally created within air carriers' reservation and/or departure control systems ("reservation systems") to fill seats and collect revenue. There are five basic air carrier reservation systems, although each air carrier has made changes to their system tailored to their specific needs. As a result, very few of the air carriers' systems are exactly the same or provide CBP with the same information in the same format. Thirty-four (34) different air carriers with twenty-four (24) different systems engage in flights which are covered by the Undertakings.

PNR has three primary sections: *Active Portion*, which contains the name(s) of the passenger(s), the itinerary, and *Supplemental Information* (such as baggage, frequent flier information, special requests, or other information related to the reservation); and *Historical Portion*, which contains changes made to the active component. When CBP receives PNR from an air carrier it may have all this information or, more likely, it will have some portions of this information. CBP takes the PNR in unformatted form and parses it so that no matter which air carrier system is involved, the PNR is displayed in a common format for CBP Officers who are reviewing it to identify high-risk passengers.

CBP uses PNR related to flights between the U.S. and EU to facilitate legitimate travel into and out of the United States and to target more

effectively individuals or groups related to terrorism or transnational crimes. PNR provides one of the first indications that a high risk individual may be trying to enter or leave the United States.

Members of Passenger Analytic Units (PAUs) and CBP's National Targeting Center (NTC) are trained to look for individuals of high risk, using PNR in conjunction with technological tools such as CBP's automated systems in conjunction with a variety of different law enforcement databases.

PNR is not used to make a final determination about an individual entering or leaving the United States because the information in the PNR is not sufficiently complete or accurate. PNR data is associated with Advance Passenger Information System (APIS) data, which provides the biographical information that is used for verification of a traveler's identity prior to arrival in the U.S. CBP Officers at the primary inspection point will also verify and generally determine whether an individual warrants additional scrutiny.

Lifecycle of the EU PNR from May 13, 2005 forward

The lifecycle as described below is the lifecycle that exists as of May 13, 2005 with the full implementation of the IT User Requirements.

Step 1: CBP pulls the 34 approved data elements of PNR no earlier than 72 hours prior to scheduled flight departure . If an appropriate push system exists, CBP will support the system from a technical standpoint to receive pushed data 72 hours before scheduled flight time and to receive all subsequent changes to PNR before flight time or to receive pushed data at a pre-specified times depending on a joint agreement with the airline.

Step 2: If data is pulled, unformatted PNR with all information, including "sensitive" data, is accessed and then filtered for "sensitive" terms and codes. "Sensitive" terms and codes are deleted

and cannot be re-created. Symbols are put in the location where "sensitive" terms and codes have been removed and original PNR is filtered.

Step 3: PNR is filtered for the 32 data elements and OSI and SSI/SSR fields specified in the Undertakings. The remaining elements of the PNR are deleted by CBP and not accessed.

Step 4: The raw PNR is parsed into a screen that provides consistent display across all reservation systems. The PNR without "sensitive" terms and codes in an unformatted format along with the full information in the OSI and SSI/SSR fields is locked behind the parsed PNR and can only be accessed by a restricted set of users with approval of a supervisor for appropriate purposes.

Step 5: At seven days after the end of travel specified in the itinerary of the PNR, the PNR data will be made available to fewer individuals, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.

Step 6: At 3.5 years from receipt date/time given in the record, PNR that has not been manually accessed will be destroyed and [REDACTED] PNR will be archived with access only allowed for auditing and to correct technical errors.

Step 7: At 11.5 years from first receipt date/time given in the record, manually accessed PNR will be destroyed. PNR related to a specific enforcement action will be available until the enforcement action is archived.

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

Deleted: M

Deleted: A

09/23/18