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

December 18, 2008

LETTER FROM THE DHS CHIEF PRIVACY OFFICER

In July 2007, the U.S. Department of Homeland Security (DHS) and the Council of the European Union (Council) signed an agreement and exchanged letters regarding the transfer of Passenger Name Record (PNR) data to DHS by air carriers operating flights between the U.S. and the European Union (EU). Included was a provision to "periodically review the implementation of this agreement, the DHS letter, and U.S. and EU PNR policies and practices" to assess the "effective operation and privacy protection of their systems."

It is my duty as the DHS Chief Privacy Officer to carry out the mandates of Section 222 of the Homeland Security Act, as amended, ensuring that privacy protections are integrated into DHS operations. This report fulfills both my office's statutory duty as well as the provision in the Agreement for periodic reviews. It is my pleasure, along with that of my staff, to report that DHS complies with the representations made in the Agreement and Letters, as well as those representations made in the System of Records Notice for the Automated Targeting System (ATS SORN) (*published in the Federal Register on August 6, 2007*), the system in which PNR resides. The report also identifies areas for improvement that could increase the value of PNR as a critical tool in protecting our homeland while ensuring individual privacy to travelers.

The Privacy Office has reviewed efforts by U.S. Customs and Border Protection (CBP) and the DHS Office of Policy to implement fully the provisions of the Agreement and Letters and the representations in the ATS SORN. CBP deserves recognition for their diligent work with the Privacy Office during the review, producing all documents and information requested. I would like to personally recognize Mr. Jay Ahern, Deputy Commissioner U.S. Customs and Border Protection, for his efforts and partnership.

We look forward to a reciprocal review of EU PNR policies and practices and to continuing to work together with the EU and its Member States to integrate privacy protections into the means and practices through which countries on both sides of the Atlantic carry out our important security missions.

Hugo Teufel III
Chief Privacy Officer
U.S. Department of Homeland Security

TABLE OF CONTENTS

I. OVERVIEW

II. HISTORY OF PNR ARRANGEMENT

III. ROLES AND RESPONSIBILITIES FOR PNR UNDER THE PRIVACY ACT AND THE 2007 EXCHANGE OF LETTERS

IV. FINDINGS AND RECOMMENDATIONS

V. CONCLUSION

APPENDICES

APPENDIX 1: Lifecycle of PNR in CBP Operations

APPENDIX 2: Automated Targeting System (ATS) System of Records Notice

APPENDIX 3: Agreement Between the United States of America and the European Union on Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)

APPENDIX 4: Letter from the Council of European Union to the United States

APPENDIX 5: Letter from United States to the Council of European Union (2007 Letter)

I. OVERVIEW

The purpose of this review is to determine whether the Department of Homeland Security (DHS) and, in particular, the U.S. Customs and Border Protection (CBP) are operating in compliance with the Automated Targeting System (ATS) System of Records Notice (SORN) published on August 6, 2007 in the *Federal Register*[1] and the 2007 Letter of Agreement between the United States and the Council of the European Union dated July 26, 2007 (2007 Letter).

The Chief Privacy Officer conducted this review under the authority of the Homeland Security Act § 222 (as amended) and the commitments made in the 2007 Letter. The review was measured against the standards of the ATS SORN, the 2007 Letter, and the *2005 Report Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union*.

The following is a summary of the DHS Privacy Office findings:

A. Continued Compliance

- As of the date of this Review, the Department and, in particular, CBP are compliant with the ATS SORN and the representations made in the 2007 Letter.

- The Privacy Office received no reports of misuse of PNR since the last review, conducted in 2005.

- CBP continues extensive training with its analysts and officers who access ATS and The Treasury Enforcement System (TECS), as well as with other officials who have been provided access to or otherwise use PNR.

- CBP analysts and officers take extensive care in the handling and sharing of PNR, and use of PNR for the purposes it was collected. This is reinforced by the training provided to analysts and officers, as well as the approval processes associated with information requests.

B. 2005 Report Areas that Required Continued Monitoring or Follow Up

- *Retention*: NARA approved the proposed records schedule for ATS. DHS has remediated this outstanding 2005 issue.

- *Routine Review of Uses of PNR by Internal Affairs:* In response to a 2005 recommendation from the Privacy Office, the Office of Internal Affairs established a plan to review audit logs associated with CBP's ATS on the use of PNR information. Since May 30, 2005, the Office of Information and Technology (OIT) has conducted

[1] 72 FR 43650

weekly audits of the system for unauthorized use. Further, the Office of the Inspector General at DHS reviewed ATS and published a report which found CBP to be "effectively employing [privacy and security] controls in protecting individuals' personally identifiable information."[2]

C. 2008 Remediation and Recommendations

- *Notice:*
  - During the review period, the Privacy Office found that the PNR Frequently Asked Questions (FAQ) and PNR Privacy Statement reflected the 2004 Agreement rather than the current 2007 Agreement.
    - *Remediation: CBP has updated the FAQs and Privacy Statement to reflect the new Agreement and the ATS SORN and PIA and is working to publish them on the CBP website.*
- *Access: FOIA and Privacy Act*
  - Timeliness of response to a Privacy Act/FOIA request: The Privacy Office found that there were timeliness issues with the CBP responses to Privacy Act/FOIA requests related to PNR. This is in part because the program is not fully staffed and the initial high volume of requests related to PNR.
    - *Recommendation: CBP should fully staff the FOIA/PA program office to reduce any backlog or delay in processing*
    - *Response: CBP is actively working to staff and reduce the backlog.*
  - Inconsistency of processing of Privacy Act/FOIA requests: The Privacy Office reviewed the accuracy of the responses provided to Privacy Act/FOIA requests, and determined exemptions were inconsistently applied.
    - *Recommendation: CBP should provide more comprehensive training to new and existing staff on FOIA, Privacy Act, DHS policy, the relevant CBP System of Records Notices and applicable exemptions, as well as the use of the Information Technology systems that maintain the information. In particular, training is needed on the various search capabilities of the systems involved.*
    - *Response: CBP has put in place updated procedures for handling exemptions under Privacy Act/FOIA requests*
  - Consistency of search for requests for "all information held by CBP": The DHS Privacy Office reviewed responses to Privacy Act/FOIA requests and determined that CBP was not consistent in the types of searches it conducted in response to certain types of requests; in particular where an individual asked generally for "all information held by CBP".
    - *Recommendation: CBP should develop standard operating procedures that outline which systems are searched and how the search is conducted.*
    - *Response: CBP has updated its process for handling such requests and is actively developing standard operating procedures.*
  - Record Retrieval and Release: The DHS Privacy Office found that the Privacy Act/FOIA personnel need to ensure that where a PNR is indexed and retrieved by

[2] http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_08-06_Oct07.pdf

the requester's name or personal identifier and the information contains information pertaining to a third person whose information does not directly pertain to the individual requesting the information, the requestor only receives personally identifiable information about themselves, which they have provided or which was provided on their behalf, consistent with the policy articulated in the ATS SORN. This occurs, for example, in situations when a travel agent books a group of 20 passengers, which results in a single PNR that holds twenty individuals' travel reservations. Assume one of the individuals requests his PNR. The reservation information of the 19 other individuals does not pertain to the requestor's information and so is not part of the "record" under the Privacy Act.

    - *Recommendation: CBP should ensure that only the PNR information pertaining to the individual requesting the information and no other individual's passenger reservation information, consistent with the ATS SORN.*
    - *Response: CBP has implemented this recommendation by ensuring that all FOIA personnel are trained on the policies outlined in the ATS SORN.*

- *Field Guidance Update:* CBP issued field guidance in 2004 and provided an updated memorandum highlighting the major changes between 2004 and 2007. The 2007 memorandum to the field indicates that updated guidance will be forthcoming. The CBP officers are following the 2004 and 2007 guidance and it sufficiently covers the necessary topics.
    - *Recommendation: For ease of use, the Privacy Office recommends DHS, in coordination with CBP, issue a single set of guidance, consistent with the SORN and the 2007 Agreement, for use by all DHS offices and components which have or may obtain access to PNR.*

II. HISTORY OF THE PNR ARRANGEMENT

In the aftermath of September 11th, the United States Congress required the U.S. Customs Service (what would become the United States Department of Homeland Security's Bureau of Customs and Border Protection (CBP) with the creation of the United States Department of Homeland Security (DHS)) to require air carriers to provide Customs with access to passenger name records (PNR) for purposes of screening individuals traveling to and from the United States.[3] PNR is originally collected by airlines and airline reservation systems for commercial purposes and then shared with CBP consistent with the Aviation Transportation Security Act of 2001 (ATSA).

In 2002, following the publication of the U.S. Customs Service interim PNR implementing regulations, the European Commission (EC) advised DHS that an EU Data Protection Directive[4] generally prohibited cross-border sharing with non-EU countries. Transfers outside the EU

[3] Aviation and Transportation Security Act of 2001, Public Law 107–71—Nov. 19, 2001 (codified at 49 U.S.C. 44909(c)(3)).

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31,*

could only be made following a determination that the receiving entity in the third country was deemed to have "adequate" data protection standards.

To avoid a potential conflict of laws between the U.S. and EU, DHS and the EU negotiated an Interim Arrangement on PNR. The Arrangement was concluded in March 2003. CBP then issued implementation guidance to its Officers in the field to ensure that PNR data received from Europe was treated consistent with the Interim Arrangement.

On May 28, 2004, U.S. Department of Homeland Security (DHS) and the European Union (EU) signed an international agreement regarding the processing of PNR, which replaced the Interim Arrangement. The Agreement followed CBP's issuance of a set of Undertakings setting forth how CBP would process and transfer PNR data received in connection with flights between the EU and the U.S. 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 also created a compliance and complaint resolution role for the DHS Chief Privacy Officer and specified that the Privacy Office should lead an annual review of the Arrangements.

In December 2004, the Congress strengthened DHS's authority for collecting PNR by requiring that, where practicable, the Department should conduct passenger screening before individuals depart on a flight destined for the United States.[5]

In September 2005, the Privacy Office completed its review of the PNR program and issued a public report reviewing CBP's policies and practices consistent with the U.S.-EU arrangement. That review resulted in findings of substantial compliance, but included key areas for improvement. The Report was issued in conjunction with the U.S.-EU Joint Review of the Undertakings on EU PNR held September 2005.

PNR information is a critical tool used by CBP in such screening of travelers to identify individuals of interest who are planning to travel to the United States.

In May 2006, the European Court of Justice (ECJ) responded to a complaint filed by the European Parliament that challenged the legal basis for the PNR Agreement. The ECJ found that the Agreement had in fact been concluded under inappropriate EU legal authority and therefore found the Agreement invalid.

As a result, the DHS and the EU negotiated and concluded interim agreement in October 2006. The Agreement responded to the ECJ decision and lessons learned from the implementation of the 2004 Agreement. This Interim Agreement self terminated in 2007.

In July 2007, DHS and the EU signed a superseding Agreement and exchanged Letters describing commitments made with regard to the use of PNR. In August 2007, DHS issued an updated Privacy Act System of Records Notice (SORN) for the Automated Targeting System (ATS), the system in which PNR resides. With the 2007 Agreement, the parties agreed to

[5] Section 4012 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Public Law 108–458—Dec. 17, 2004.

conduct periodic reviews. Compared with the earlier arrangement, this agreement did not specify that any one component of DHS or the European Union was responsible for conducting the review. Instead the agreement deemed the Secretary of Homeland Security and the Commissioner for Justice, Freedom and Security would be responsible for review.

In advance of the second Joint Review with the European Union, the Privacy Office conducted an assessment of the Department's and CBP's policies and uses of EU PNR. The Privacy Office reviewed the requirements of the ATS SORN, the 2007 Agreement, the 2007 Letter and the issues identified in the 2005 *Report Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union*.

III. ROLES AND RESPONSIBILITIES FOR PNR UNDER THE PRIVACY ACT AND 2007 LETTER

A. The DHS Privacy Office

1. The DHS Privacy Office Mission

The mission of the Privacy Office is to sustain privacy protections and transparency of government operations, while achieving the mission of DHS.

The DHS Privacy Office is the first statutorily required, comprehensive privacy policy office in any U.S. federal agency. It currently operates under the direction of the Chief Privacy Officer, Hugo Teufel III, who was appointed by the Secretary. The Chief Privacy Officer serves under the authority of the Secretary and Section 222 of the Homeland Security Act of 2002, as amended.[6] In 2007 Congress expanded Section 222 to include several other responsibilities for the Chief Privacy Officer including but not limited to expanded and explicit investigative authority, the ability to conduct regular reviews of privacy implementation, and greater coordination with the Inspector General.[7]

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 personally identifiable 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 210,000 employees.

[6] 6 U.S.C. § 142, as amended by the Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53).
[7] *Id.*

The construct of a privacy officer shares some similar aspects of, but is not identical to, the constructs of data protection commissioners and European government data protection officers. The very principles that these 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. Internally, the Privacy Office works to educate, to inform, to create processes, and to mandate attention to privacy and fair information principles in new and existing programs, new procedures, new policies, and the hiring and training of new personnel. Externally, the Privacy Office champions DHS programs where appropriate, but criticizes where necessary.

2. The DHS Privacy Office Responsibilities

Consistent with the statutory requirements of the Chief Privacy Officer, the Privacy Office undertook a review of DHS, and in particular CBP, use of EU PNR data. Further, the Privacy Office, the DHS Office of Policy and CBP, are facilitating the Joint Review of the implementation of the statutory requirements of the Privacy Act and the representations in the 2007 Letter on EU PNR.

B. DHS Office of Policy

1. DHS Policy Mission:

The Office of Policy provides a central office to develop and communicate policies across multiple DHS components to strengthen the Department's ability to maintain uniform policy and operational readiness needed to protect the homeland. It provides the foundation and direction for Department-wide strategic and counter-terrorism planning initiatives that drive budget priorities. It liaises with both the international community and private sector to advance homeland security initiatives and develop lasting partnerships. It bridges the different components of the Department by improving communication among DHS entities, eliminating duplication of effort, and translating policies into timely action.

2. DHS Office of Policy Responsibilities:

The Office of Policy was responsible for the negotiation of the 2006 Interim Agreement and the 2007 Agreement with the EU (the 2004 Agreement preceded the creation of the Office). In fulfilling this responsibility, the Office of Policy identified and ensured consistency between DHS's operational, policy, and legal requirements, including those associated with information sharing, data management, and privacy. In this regard it worked closely with CBP, the Privacy Office, and the Office of the General Counsel. The Office of Policy remains the primary point of contact for the EU and other stakeholders for strategic and policy questions associated with the 2007 Agreement. It also oversees the development and implementation of PNR, border management, and information sharing policies within DHS to ensure consistency with the 2007 Agreement and other obligations.

C. U.S. Customs and Border Protection

1. CBP Mission:

CBP, headed by the Commissioner W. Ralph Basham, 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 for enforcing customs, immigration, agriculture and other U.S. laws at the border, 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 Responsibilities

CBP has primary responsibility for collecting PNR records and actively uses such information at the operational level. While DHS is primarily responsible for defining the policies regarding the handling of such data, CBP is charged with implementing such policies, including the ATS SORN and the 2007 Letter, at a technical and operational level. CBP collects, maintains, uses, and disseminates PNR maintained in ATS-P.

D. Structure of the Review

In August of 2008, the Chief Privacy Officer, contacted W. Ralph Basham, the CBP Commissioner, to recommend an outline of how the internal privacy review would be conducted, and presented the criteria that would be used for measuring consistency with the legal requirements of the ATS SORN and the representations in the 2007 Letter. In addition to meeting with CBP which has the operational lead for use of PNR, the Privacy Office worked with Office of Policy and the DHS Traveler Redress Inquiry Program (DHS TRIP). The internal review described in this report has assessed DHS's and CBP's effectiveness in meeting the requirements of the Privacy Act and the representations made in the 2007 Letter, and improvements made since the 2005 Joint Review.

1. The DHS PNR Review Team

The DHS PNR Review team was led by Rebecca J. Richards, Director of Privacy Compliance, with assistance from Nathan Coleman, Associate Director of Privacy Compliance, and Rachel Drucker, Privacy Analyst. William Holzerland, Associate Director, Disclosure Policy and FOIA Program Development; John Kropf, Deputy Chief Privacy Officer and Senior Advisor for International Privacy Policy; and David Palmer, Deputy Associate General Counsel (Legal Counsel) provided assistance and guidance. The Review team has extensive compliance, privacy policy, legal, and technical expertise.

2. **DHS PNR Review**

The Privacy Office review consisted of an analysis of existing policies and procedures, interviews with key management, officers, and analysts who handle PNR, and technical review of CBP systems and documentation.

The Privacy Office reviewed the following materials:

- Public notices provided to travelers, including the ATS SORN, ATS Privacy Impact Assessment (PIA), Frequently Asked Questions related to PNR, and the CBP PNR Privacy Statement;
- Documented procedures relating to collection, use, sharing, and retention of PNR;
- Training materials; and
- Pertinent technical logs.

Interviews included:

- U.S. Customs and Border Protection Personnel
    - National Targeting Center (NTC) Management on policies, procedures, and use of ATS;
    - Two Passenger Analytic Units (PAU) (Washington, Dulles and Baltimore Washington International);
    - Office of Information Technology (OIT);
    - Office of Public Affairs (OPA)
        - Customer Service Center (CSC);
    - Office of International Trade (OT)
        - Office of Rules and Regulations (OR&R) and
        - Commercial Targeting and Enforcement (CT&E);
    - Office of Chief Counsel (OCC);
    - Office of Field Operations (OFO); and
    - Office of Intelligence and Operations Coordination (OIOC).
- DHS Policy
    - Office of International Affairs
    - Office of Strategic Policy
- DHS Traveler Redress Program (DHS TRIP)

IV. FINDINGS and RECOMMENDATIONS

Based on the results of our review, the Privacy Office has outlined areas of compliance with the Privacy Act and in particular the ATS SORN and representations in the 2007 Letter. The Privacy Office has also requested specific remediation for improving the out of date notices to the public, and made recommendations to strengthen CBP's Privacy Act/FOIA program.

A. Relevant Aspects of the ATS SORN and 2007 Letter: Section by Section Review

This section follows the order of the 2007 Letter and discusses the policies, procedures, practices, and IT support related to various areas of the ATS SORN and the 2007 Letter. Each section begins with a quote from the relevant section of the Privacy Act or the ATS SORN and the 2007 Letter, followed by "Discussion" and then "Findings".

1. Purpose for which PNR is used

ATS SORN*: Purpose(s) of PNR in ATS-P are (a) To prevent and combat terrorism and related crimes; (b) To prevent and combat other serious crimes, including organized crime, that are transnational in nature; (c) To prevent flight from warrants or custody for crimes described in (a) and (b) above; (d) Wherever necessary for the protection of the vital interests of a data subject or other persons; (e) In any criminal judicial proceedings; or (f) As otherwise required by law.*

Roman Numeral I of the 2007 Letter*: DHS uses EU PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law.*

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

CBP issued field guidance specific to the PNR related to flights between European Union countries and the United States on December 20, 2004. This guidance was renewed with a memorandum to the field on August 13, 2007, to reflect the System of Records Notice (SORN) for the Automated Targeting System (ATS) published on August 3, 2007, and the 2007 Letter. This memorandum reiterated that all PNR data elements must be used in accordance with the 2007 Agreement and the CBP field guidance, which reflects the terms of the requirements of the SORN, the 2007 Agreement, and the 2007 Letter. DHS, in coordination with CBP, will be issuing a single set of guidance, consistent with the SORN and the 2007 Agreement, for use by all DHS offices and components which have or may obtain access to PNR.

CBP Officers who work within the Passenger Analytical Units (PAUs) and CBP's National Targeting Center (NTC) are trained to identify passengers who are considered high risk and have received additional training in the form of written field guidance. Formal training is also

administered through the Federal Law Enforcement Training Facility (FLETC). This field guidance and training is consistent with the scope of purposes identified in the ATS SORN and the 2007 Letter.

All CBP Officers with access to PNR data are required to review and sign an acknowledgment of the field guidance. This is logged in the training system so that it may be regularly reviewed by Headquarters staff to ensure that the field staff is properly trained on the use and disclosure of the data. The August 13, 2007, CBP Memorandum also clearly states which PNR data elements are allowed to be used and for which purposes. In interviews with the PAUs at both Washington Dulles and Baltimore Washington International Airports, the personnel at the PAUs had the field guidance on hand and were well-versed in the appropriate uses of the information as demonstrated through the interview process.

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

***Findings*:** Based on a review of the documented procedures, regulations, and specific examples of information used and shared by DHS, CBP operates in a manner consistent with the purposes outlined in the ATS SORN and representations in the 2007 Letter. As a matter of best practices, the Privacy Office recommends re-issuing a single set of guidance that consolidates all updates, memoranda, and policies.

2. Sharing of PNR

ATS SORN: *In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3). DHS only discloses information to those authorities who have a legal purpose to use the data, intend to use the information consistent with the purpose for which CBP collects it or for another legally required function, such as GAO oversight and ongoing IT maintenance, and has sufficient capability to protect and safeguard it. Under these limits, data may be disclosed as a routine use…*

Roman Numeral II of the 2007 Letter*:* *DHS shares EU PNR data only for the purposes named in article I.*

Discussion: DHS's and CBP's mandate to share counterterrorism related information both within DHS and with other Federal agencies was strengthened in 2004 with the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), in particular Section 7010[8] and Executive Order 13388.

Pursuant to the Privacy Act, 5 U.S.C. 552a (b)(1), and the "One DHS Policy," CBP may share PNR within DHS, if the component has a "need to know" the information. CBP logs the sharing of PNR with all other components within DHS to provide for additional oversight.

[8] The Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108–458—Dec. 17, 2004.

Pursuant to the IRPTA of 2004 § 7010, sharing of PNR may occur between CBP NTC and the FBI's Terrorist Screening Center in order to determine the appropriate law enforcement response to an possible match to the Terrorist Screening Database (TSDB).

Sharing of PNR occurs at the headquarters, the CBP National Targeting Center – Passenger (NTCP), or field units. All sharing, whether internal or external to CBP, is logged in ATS. The Privacy Office reviewed six specific instances of sharing of PNR from the NTC. Five of these instances were terrorism related in accordance with the purpose of "terrorism and related crimes." One of these instances was law enforcement related due to a warrant for an individual who was arriving or departing the U.S. and was wanted for several serious and violent crimes, which is envisioned by "other serious crimes, including organized crime, that are transnational in nature; and flight from warrants or custody for crimes described above".

The Privacy Office also reviewed a random sampling of ten instances where CBP made disclosures outside of DHS. The log was retrieved from the ATS system. Eight disclosures were terrorism related and two were transnational crimes. All were properly logged and within the scope of the purpose of the ATS SORN and the 2007 Letter.

In addition to the types of terrorism related, flights from warrants related, and transnational crimes related disclosures discussed above, the Privacy Office found that PNR was regularly shared by the NTC-P with the Center for Disease Control (CDC) to properly coordinate appropriate responses to health concerns associated with international air transportation. Sharing for this purpose is clearly envisioned when necessary for the protection of the vital interests of the data subject or other persons. DHS has a Memorandum of Understanding (MOU) in place with the CDC dictating the specific terms and protocols for the sharing of information, including PNR, and the SORN for ATS allows for sharing of information "to appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk." (Routine use D, ATS SORN DHS/CBP-006, August 6, 2007, 72 FR at 43654).

The Privacy Office spoke with a total of 15 officers and analysts from the NTC-P and PAUs at Dulles International Airport and Baltimore International Airport. Based on the personal interviews with analysts at the NTC-P and in the PAUs, most sharing is done either with the Terrorist Screening Center or through DHS's National Operations Center with the CDC. Each analyst stated such requests are formally logged.

***Findings*:** In each instance of sharing of PNR the Privacy Office found that the sharing comported with the purposes of the collection stated in the ATS SORN and the 2007 Letter. In fact, where the issue of information sharing was discussed with analysts at the NTC and officers at the PAUs, it was clear that sharing of PNR was forbidden unless routed through chain of command and logged appropriately.

ATS SORN*: Routine Uses A and B, and general provisions of* the Privacy Act of 1974, 5 U.S.C. § 552a (b)(1), (b)(3), b(8) and (e)(10)
A. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws;
B. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;
(b) Conditions of disclosure
Privacy Act:
No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be
(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties; …
(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;…
(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual…
(e) Agency requirements: (10) establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

Roman numeral II of the 2007 Letter*: DHS treats EU PNR data as sensitive and confidential in accordance with U.S. laws and, at its discretion, provides PNR data only to other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, transnational crime and public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating, according to law, and pursuant to written understandings and U.S. law on the exchange of information between U.S. government authorities. Access shall be strictly and carefully limited to the cases described above in proportion to the nature of the case.*

Discussion: PNR is maintained within a secure information technology system, ATS. CBP has completed the necessary security reviews to receive its certification and accreditation (C&A) under the Federal Information Security Management Act (FISMA) for ATS. When information is transferred or removed from the IT system, ATS logs the external sharing. Internal sharing is logged locally on hard copy, or the individual has an assigned account and ATS tracks the usage by the individual.

The additional safeguard of logging internal sharing increases accountability of the user and increases the ability to audit usage of the system. When a user logs into ATS, he is reminded of the appropriate use of PNR and policies regarding further dissemination of the information outside of the ATS system. When information is logged and shared externally, a notice to the recipient is automatically generated by ATS stating the accepted uses and further disclosure of the information.

As noted above, the examples of the external sharing were compatible with the purposes outlined in the ATS SORN and consistent with the routine uses published in the ATS SORN. In the case of the PNR information shared for health related information, the sharing was conducted pursuant to an MOU between DHS and CDC.

None of those interviewed indicated they had ever needed to access sensitive information within a PNR, but aptly described the process, understanding its importance and significance.

***Findings*:** The Privacy Office finds that CBP is in compliance with this provision of the ATS SORN as required by U.S. law on information sharing. The sharing of information with CDC is done in accordance with a signed MOU between DHS and the CDC, and the ATS SORN. The sharing is done in furtherance of DHS and CDC's statutory missions, to protect the public safety.

ATS SORN*: Routine Uses A, B, and C.*
A. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws;

B. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

C. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a data subject and such disclosure is proper and consistent with the official duties of the person making the disclosure;

Roman Numeral II of the 2007 Letter*: EU PNR data is only exchanged with other government authorities in third countries after consideration of the recipient's intended use(s) and ability to protect the information. Apart from emergency circumstances, any such exchange of data occurs pursuant to express understandings between the parties that incorporate data privacy protections comparable to those applied to EU PNR by DHS, as described in the second paragraph of this article.*

Discussion: Under the Privacy Act, absent the consent of the data subject, CBP may only share PNR with another government in a third country if there is an appropriate routine use or it

adheres to one of the statutory basis for disclosure as outlined in the Privacy Act; the use must be compatible with the purpose of the original collection. This requirement is in place whether there is an emergency or not. CBP provided an example of third country government sharing, a Memorandum of Understanding (MOU) regarding the sharing of certain information, including PNR data related to individuals who are deemed to be a high risk for terrorism or other serious transnational crimes, based on jointly determined criteria. The MOU (which was concluded consistent with the more restrictive 2004 PNR Arrangement with the EU) clearly states the reasons the information will be shared and the constraints on further use or dissemination to or by the third country. This information is shared pursuant to Routine Uses A, B, and C of the ATS SORN.

***Findings*:** The Privacy Office finds CBP to be in compliance with the routine uses published in the ATS SORN and the relevant provision of the 2007 Letter.

3. Types of Information Collected

ATS SORN: *Categories of Records in the System:*

ATS-P, a component of ATS, maintains the PNR information obtained from commercial air carriers and uses that information to assess whether there is a risk associated with any travelers seeking to enter, exit, or pass through the United States. PNR may include some combination of these following categories of information, when available:

1. *PNR record locator code.*
2. *Date of reservation issue of ticket.*
3. *Date(s) of intended travel.*
4. *Name(s).*
5. *Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.).*
6. *Other names on PNR, including number of travelers on PNR.*
7. *All available contact information (including originator of reservation).*
8. *All available payment/billing information (e.g. credit card number).*
9. *Travel itinerary for specific PNR.*
10. *Travel agency/travel agent.*
11. *Code share information (e.g., when one air carrier sells seats on another air carrier's flight).*
12. *Split/divided information (e.g., when one PNR contains a reference to another PNR).*
13. *Travel status of passenger (including confirmations and check-in status).*
14. *Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields.*
15. *Baggage information.*
16. *Seat information, including seat number.*
17. *General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information.*

18. *Any collected APIS information (e.g., Advance Passenger Information (API) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender).*
19. *All historical changes to the PNR listed in numbers 1 to 18.*

Not all air carriers maintain the same sets of information for PNR, and a particular individual's PNR likely will not include information for all possible categories. In addition, PNR does not routinely include information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual. To the extent PNR does include terms that reveal such personal matters, DHS employs an automated system that filters certain of these terms and only uses this information in exceptional circumstances.

Roman Numeral III of the 2007 letter*: Most data elements contained in PNR data can be obtained by DHS upon examining an individual's airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically significantly enhances DHS's ability to focus its resources on high risk concerns, thereby facilitating and safeguarding bona fide travel.*

Types of EU PNR Collected:

1. *PNR record locator code.*
2. *Date of reservation/issue of ticket.*
3. *Date(s) of intended travel.*
4. *Name(s).*
5. *Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.).*
6. *Other names on PNR, including number of travelers on PNR.*
7. *All available contact information (including originator information).*
8. *All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction).*
9. *Travel itinerary for specific PNR.*
10. *Travel agency/travel agent.*
11. *Code share information.*
12. *Split/divided information.*
13. *Travel status of passenger (including confirmations and check-in status).*
14. *Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote.*
15. *All Baggage information.*
16. *Seat information, including seat number.*
17. *General remarks including OSI, SSI and SSR information.*
18. *Any collected APIS information.*
19. *All historical changes to the PNR listed in numbers 1 to 18.*

Discussion: The Privacy Office reviewed the ATS system, and CBP only maintains those elements outlined in the ATS SORN under "categories of records" and similarly restated in the 2007 Letter in the system.

The Privacy Office reviewed the ATS system and the documentation and found that the system and documentation matched the above mentioned categories of records.

The Privacy Office reviewed technical guidance provided to airlines regarding the required categories of data. This guidance mirrors the CBP ATS technical requirements and the 2007 Letter. By providing mirror guidance externally to airlines, which are required to comply with PNR requirements, CBP has publicly committed itself to collecting only those categories of data identified in the ATS SORN and the 2007 Letter.

On October 1, 2007, ATS was updated to capture only the categories of PNR data identified in the 2007 Letter, from an air carrier's system and to parse it so that the data can be displayed in a uniform manner for analysis purposes (as opposed to the raw form which would differ from air carrier to air carrier). Any data outside of the identified data categories are filtered so that the information may not be viewed and is not retrievable thirty days after CBP receives the information. The first deletion took place on October 30, 2007.

The Privacy Office reviewed ten random sets of individuals' PNR from ten random dates. This review demonstrated that the data sets included in the random PNRs matched the data sets allowable under the ATS SORN and the 2007 Letter.

***Findings*:** The Privacy Office found the ATS system documentation, technical guidance provided to airlines, and the random sampling of PNR matched the data collection requirements of the ATS SORN and the 2007 Letter.

ATS SORN*: Section (e)(7) of the Privacy Act:*
(e) Agency requirements
(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

Roman Numeral III of the 2007 letter*: To the extent that sensitive EU PNR data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual), as specified by the PNR codes and terms which DHS has identified in consultation with the European Commission, are included in the above types of EU PNR data, DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information. Unless the data is accessed for an exceptional case, as described in the next paragraph, DHS promptly deletes the sensitive EU PNR data.*

Discussion: CBP deploys 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.

CBP Officers are trained to follow the ATS SORN and the 2007 Letter on the proper use of sensitive personal information which may be contained in a PNR, 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 CBP Officers 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.

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 field guidance was issued in 2004 and updated with additional guidance in 2007. DHS, in coordination with CBP, will be developing a uniform set of guidance which governs the handling of PNR, consistent with the ATS SORN and 2007 Agreement, by all offices and components of DHS.

Internal Notice: 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.

***Findings*:** Based on the technical review of the system as well as a review of the documented policies, procedures, training, interviews, applicable regulations and U.S. law, the Privacy Office finds that CBP is in compliance with the ATS SORN and the representations in the 2007 Letter. The Privacy Office verified as of August 20, 2008, that the sensitive filters are currently operating in an identical manner to the last review. As a matter of best practices, the Privacy Office recommends DHS, in coordination with CBP, issue a single set of guidance, consistent with the ATS SORN and 2007 Agreement, to be used by all DHS offices and components that have or may obtain access to PNR.

ATS SORN: *ATS SORN Routine Use D: D. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable*

disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk);

Roman Numeral III of the 2007 letter*: If necessary in an exceptional case where the life of a data subject or of others could be imperiled or seriously impaired DHS officials may require and use information in the EU PNR other than those listed above, including sensitive data. In that event DHS will maintain a log access to any sensitive data in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law.*

Discussion: CBP made no requests for additional information due to exceptional circumstances referenced in the 2007 Letter.

None of the officers interviewed had ever sought access to sensitive data from a PNR, but aptly described the process to be employed if it was necessary.

***Findings*:** The Privacy Office finds CBP is in compliance with this provision of the Privacy Act and the 2007 Letter.

4. Access and Redress

ATS SORN*: Public Record Access/Redress Procedures*

DHS policy allows persons (including foreign nationals) to access and seek redress under the Privacy Act to raw PNR data maintained in ATS-P. The PNR data, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record. This access does not extend to other information in ATS obtained from official sources (which are covered under separate SORNs) or that is created by CBP, such as the targeting rules and screening results, which are law enforcement sensitive information and are exempt from certain provisions of the Privacy Act. For other information in this system of records, individuals generally may not seek access for purposes of determining if the system contains records pertaining to a particular individual or person. (See 5 U.S.C. 552a (e)(4)(G) and (f)(1)).

Individuals, regardless of nationality, may seek access to records about themselves in accordance with the Freedom of Information Act. In addition, DHS policy allows persons, including foreign nationals, to seek access under the Privacy Act to raw PNR data submitted to ATS-P. Requests for access to personally identifiable information contained in PNR that was provided by the requestor or by someone else on behalf of the requestor, regarding the requestor, may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.50C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791). Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked ``Privacy Act Access Request.'' The request should include a general description of the records sought and must

include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

CBP notes that ATS is a decision-support tool that compares various databases, but does not actively collect the information in those respective databases, except for PNR. When an individual is seeking redress for other information analyzed in ATS, such redress is properly accomplished by referring to the databases that directly collect that information. If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program (``TRIP''). See 72 FR 2294, dated January 18, 2007. Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through TRIP.

TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs--like airports and train stations or crossing U.S. borders. Through TRIP, a traveler can request correction of erroneous PNR data stored in ATS-P and other data stored in other DHS databases through one application. Additionally, for further information on ATS and the redress options please see the accompanying PIA for ATS published on the DHS website at http://www.dhs.gov/privacy. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at http://www.dhs.gov/trip and at http://www.dhs.gov. Additionally, a traveler may seek redress from CBP at the time of the border crossing.

Contesting Record Procedures

Individuals may seek redress and/or contest a record through several different means, all of which will be handled in the same fashion. If the individual is aware the information is specifically handled by CBP, requests may be sent directly to CBP at the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791). If the individual is uncertain what agency is responsible for maintaining the information, redress requests may be sent to DHS TRIP at DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at http://www.dhs.gov/trip.

Roman Numeral IV of the 2007 letter*: DHS has made a policy decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with U.S. law, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR. These policies are accessible on the DHS website, www.dhs.gov.*
Furthermore, PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U.S. Privacy Act and the U.S. Freedom of Information Act (FOIA). FOIA permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from disclosure by an applicable exemption under the FOIA. DHS does not disclose PNR data to the

public, except to the data subjects or their agents in accordance with U.S. law. Requests for access to personally identifiable information contained in PNR that was provided by the requestor may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: (202) 344-1 850 and fax: (202) 344-2791).

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

Discussion: The Privacy Office reviewed the activities of the DHS Traveler Redress Inquiry Program (DHS TRIP), the CBP Customer Service Center, and the CBP Freedom of Information Act/Privacy Act Program. All three programs accept requests for redress or requests for access to information from individuals no matter their status within the U.S.

Information on accessing individual's information can be found at:

- www.dhs.gov/trip,
- www.dhs.gov/foia, and
- http://www.cbp.gov/xp/cgov/travel/customerservice/.

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 that cannot be addressed at the Port of Entry, the passenger will be given a general fact sheet that directs individuals to contact the Customer Service Center or DHS TRIP with any further questions.

Requests from individuals who have an issue upon entry into or exit from the country can be received in one of three ways: the DHS Traveler Redress Inquiry Program (TRIP); the CBP Customer Service Center; or a Freedom of Information Act/Privacy Act request.

DHS TRIP: The Department of Homeland Security's Travel Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs--like airports and train stations--or crossing U.S. borders, including:

- denied or delayed airline boarding
- denied or delayed entry into and exit from the U.S. at a port of entry or border checkpoint
- continuously referred to additional (secondary) screening

To file a complaint with the DHS Traveler Redress Inquiry Program, or TRIP, the process starts at the http://www.dhs.gov/trip webpage. This website has a PDF form which may be emailed or mailed and an electronic form that can be submitted over the internet. When the form and supporting documentation are submitted by mail or email, a confirmation letter is sent, notifying the submitter that their request has been received.

When the form is submitted online, a case number is returned at the end of the request, and directions for providing supporting documentation to TRIP is given. After the request is submitted, the case is assigned to TRIP analyst for review. Once the TRIP analyst determines that all of the correct documentation is present, he reviews the submitted complaint form to determine which component participating in TRIP should address the complaint. The component then reviews the complaint to determine which division within the component is best equipped to answer the complaint. Occasionally, the component determines that the complaint was misidentified, and should be handled by another component, and reassigns it to them in TRIP. The assigned division takes action to remediate the complaint if applicable, and create a letter to be returned to the submitter. The letter and remediation action are entered into TRIP. TRIP then sends the letter to the person who filed the complaint.

TRIP has liaisons from CBP to handle CBP-related issues. The CBP Liaison reviews the CBP assigned complaints and works directly with individuals in the Office of Field Operations (OFO) to identify and resolve the issues as quickly as possible. PNR is rarely involved in any of the research surrounding why an individual is seeking redress.

Customer Service Center: At the CBP Customer Service Center (CSC), CBP employees field calls and other forms of correspondence from persons who have an issue upon entry into or exit from the country. If the CSC can resolve the issue over the phone, they will strive to do so. To close out the case, the CSC sends a letter to the person notifying them that their issue has been resolved. For issues that are out of the prevue of the CSC, a referral letter is sent to the person directing him to contact the agency that can assist them with a resolution. CSC does not have access to PNR and must seek further information from personnel in OFO. In interviews with CSC personnel, CSC personnel stated that they rarely have seen PNR be the subject of a complaint and could not provide a single example.

Office of International Trade, Commercial Targeting and Enforcement (CT&E), Freedom of Information Act Division: CBP reorganized its Freedom of Information Act (FOIA) Division and centralized processing of Privacy Act or Freedom of Information Act requests (FOIA/PA requests) at Headquarters in the Office of International Trade in September 2007.

CBP handles all FOIA/PA requests received by CBP in accordance with Title 19, Code of Federal Regulations (C.F.R.), Part 103, 6 C.F.R Part 5, DHS directives, and CBP directives. Field guidance on EU PNR references existing general statutory restrictions 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 existing CBP and DHS policy, and the law.

The FOIA/PA requests are first reviewed to ensure that CBP is the correct agency to handle the request. If the request should be directed elsewhere, CBP sends a letter to the requestor with information regarding who to contact to gain access to the information sought.

Once it has been determined that the request is indeed a CBP FOIA/PA request, it is given to a FOIA officer for research. The FOIA officer searches the systems available to him to gather the requested information; for PNR the FOIA officer searches ATS-P. For broader requests for all information that CBP has, the FOIA officer will search the CBP TECS information technology system using different query functions, but will generally not search ATS-P unless an individual specifically requests her PNR.

Upon identifying the responsive records, the FOIA officer then reviews the collected information for any exemptions applicable under the Privacy Act of 1974 or the Freedom of Information Act and redacts any information that is exempt. A letter is then drafted to go back to the requestor, which includes a copy of any of the information found in the search for the records.

Requests for Corrections: 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 CBP Officer should follow normal procedures for FOIA requests or amendment of records. Designated personnel in the Office of Field Operations 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 enables those who are authorized to make corrections to PNR records, to enter a tracking number into the correction record. To date, CBP has received no requests to amend or correct PNR.

The process for all corrections is they are 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. As noted above, this process has not been requested to date.

Appeals: 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. The *U.S. 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: In reviewing the DHS TRIP process, the Privacy Office found that the liaison process between CBP and DHS TRIP is working well and, while traveler complaints may take time to resolve, that the overall process appears to be working. Generally, the basis for concern is something other than information in the PNR and, as such, PNR has not been accessed in resolving redress issues.

In reviewing the Customer Service Center's process for issues outside of DHS TRIP, PNR is rarely involved in the review process.

The majority of PNR related requests are sent to Commercial Targeting & Enforcement Freedom of Information Act Division. The Privacy Office reviewed the overall process for handling PNR requests as well as reviewing the Privacy Act request process for "all information held by CBP".

The Privacy Office reviewed seven requests for PNR and three other requests related to searches for "all information held by CBP". The unredacted PNR information provided from ATS-P were consistent and accurate with the information maintained in ATS-P. The requests for PNR took more than one year to process and were inconsistent in what information was redacted.

In discussing the process with the FOIA personnel, management noted that they have been understaffed and are bringing on new staff to reduce the backlog and period of time it takes to respond to requests. Additionally, management stated that part of the delayed response was due to the large number of requests initially submitted for PNR.

CBP provides basic FOIA/Privacy Act training both in house and through outside groups. Additional on the job training is provided including guidance based on recent court cases. The PNR specific requests are a small percentage of the total requests based on the statistics provided to the Privacy Office, but if ATS-P were searched in all cases in which an individual asks for "all information held by CBP," the percentage would increase more than seven

Two specific issues arose with the discussion of requests and redaction. First, if an individual requests "all information held by CBP" the FOIA specialist generally does not search ATS because PNR was not specifically requested.

Second, the DHS Privacy Office found that the Privacy Act/FOIA personnel need to ensure that where a PNR is indexed and retrieved by the requester's name or personal identifier and the information contains information pertaining to a third person whose information does not directly pertain to the individual requesting the information, the requestor only receives personally identifiable information about themselves, which they have provided or which was provided on their behalf, consistent with the policy articulated in the ATS SORN. This occurs, for example, in situations when a travel agent books a group of 20 passengers, which results in a single PNR that holds twenty individuals' travel reservations. Assume one of the individuals requests his PNR. The reservation information of the 19 other individuals does not pertain to the requestor's information and so is not part of the "record" under the Privacy Act.

The ATS SORN (72 FR at 43655) makes clear that an individual may only access personally identifiable information from ATS-P (PNR) to the extent such information is about that individual and was provided by or on behalf of that individual.

The FOIA/PA request process needs to be strengthened to improve response time, improve the quality of the responses and the redaction, and sufficiency of searches. DHS Privacy Office recommends CBP develop standard operating procedures related to how and which CBP systems are searched will strengthen the program and increase consistency. CBP should ensure that only the PNR information pertaining to the individual requesting the information and no other individual's passenger reservation information, consistent with the ATS SORN.

Based on the above recommendations, CBP has updated its process for handling requests and is actively developing standard operating procedures. Additionally, CBP has implemented this recommendation by ensuring that all FOIA personnel are trained on the policies outlined in the ATS SORN.

5. Enforcement

ATS SORN*:* *Privacy Act Section 5 U.S.C. 552a (g) and (i) provide for civil remedies and criminal penalties.*

(g)(1) Civil remedies

Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which

was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of--

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(i)(1) Criminal penalties
Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

Roman Numeral V of the 2007 Letter*: Administrative, civil, and criminal enforcement measures are available under U.S. law for violations of U.S. privacy rules and unauthorized disclosure of U.S. records. Relevant provisions include but are not limited to Title 18, United States Code, Sections 64 1 and 1030 and Title 19, Code of Federal Regulations, Section 103.34.*

Discussion: DHS and CBP have clear authority under the Privacy Act, Title 18, and Title 19 to enforce any security, privacy, or other administrative, civil, or criminal penalties against individuals for unauthorized use or disclosure of PNR and other CBP data.

Findings: DHS's and CBP's authority have not changed since the publication of the ATS SORN or the signing of the 2007 Letter.

6. Notice

ATS SORN*: DHS issued the ATS SORN on August 6, 2007, in the Federal Register at 72 FR 43650, an associated notice of proposed rulemaking related to exempting the SORN from certain provisions of the Privacy Act as seen at 72 FR 43567, and a Privacy Impact Assessment at www.dhs.gov/privacy.*

Roman Numeral VI of the 2007 letter*:* *DHS has provided information to the traveling public about its processing of PNR data through publications in the Federal Register and on its website. DHS further will provide to airlines a form of notice concerning PNR collection and redress practices to be available for public display. DHS and the EU will work with interested parties in the aviation industry to promote greater visibility of this notice.*

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

- System of Records Notice re-published on August 6, 2007, 72 FR 43650 in response to significant public comment.
- Notice of Proposed Rulemaking re-published on August 6, 2007, 72 FR 43567.
- Privacy Impact Assessment Update for the Automated Targeting System, published August 3, 2007.
- System of Records Notice published on November 2, 2006, 71 FR 64543.
- Privacy Impact Assessment for the Automated Targeting System, published November 22, 2006.

Additionally, CBP has published on its web site at http://www.dhs.gov/xlibrary/assets/privacy/privacy_faq_pnr_cbp.pdf FAQs, but these FAQs need to be updated.

CBP 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 after the 2004 Agreement. The statement discusses why CBP receives data, who has access to it, how long data is retained, and how questions and complaints may be filed and appealed. See http://www.dhs.gov/xlibrary/assets/privacy/privacy_stmt_pnr.pdf.

The Privacy Statement and Frequently Asked Questions need to be updated to reflect the 2007 Letter, ATS SORN and PIA.

After the conclusion of the 2007 PNR agreement, DHS coordinated with the Air Transport Association and International Air Transportation Association on the development of revised carrier notices to ensure passengers were well informed about how their data would be handled.

Findings: The ATS SORN and PIA remain accurate. CBP has updated the FAQs and Privacy Statement related to the PNR arrangement and is working to post them on the web site.

7. Data Retention

ATS SORN*:* *Records in this system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration. ATS both collects information directly, and derives other information from various systems. To the extent information is collected from other systems, data is retained in accordance with the record retention requirements of those systems.*

The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be deleted, except as noted below. The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions: ATS-P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers. Notwithstanding the foregoing, information maintained only in ATS that is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

Roman Numeral VII of the 2007 Letter*:* *DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status. Data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. We expect that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions. Data that is related to a specific case or investigation may be retained in an active database until the case or investigation is archived. It is DHS' intention to review the effect of these retention rules on operations and investigations based on its experience over the next seven years. DHS will discuss the results of this review with the EU.*

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

Discussion: The retention schedule for ATS-P was officially approved by the National Archives and Records Administration (NARA) on August 14, 2007. The schedule makes specific reference to EU PNR data, stating the following:

- EU PNR data will remain in an analytical active database for a period of seven years.
- After seven years, the data is moved to a dormant, non-operational status. Data in dormant status will be retained for eight years and may be accessed only with approval from a senior DHS official designated by the Secretary of Homeland Security.
- Data related to a specific case or investigation may be retained in an active database until the case or investigation is archived.

CBP has also provided the Privacy Office with logs of purged data tables demonstrating their compliance with the retention schedule.

Findings: The Privacy Office has verified the NARA retention schedule and the purge logs provided by CBP. CBP is in compliance with the ATS retention schedule consistent with the SORN and the 2007 Letter.

8. Transmission

ATS SORN: This topic is outside the scope of the ATS SORN.

Roman Numeral VIII of the 2007 Letter*: Given our recent negotiations, you understand that DHS is prepared to move as expeditiously as possible to a "push" system of transmitting PNR from airlines operating flights between the EU and the U.S. to DHS. Thirteen airlines have already adopted this approach. The responsibility for initiating a transition to "push" rests with the carriers, who must make resources available to migrate their systems and work with DHS to comply with DHS's technical requirements. DHS will immediately transition to such a system for the transmission of data by such air carriers no later than January 1, 2008 for all such air carriers that have implemented a system that complies with all DHS technical requirements. For those air carriers that do not implement such a system the current system shall remain in effect until the air carriers have implemented a system that is compatible with DHS technical requirements for the transmission of PNR data. The transition to a "push" system, however, does not confer on airlines any discretion to decide when, how or what-data to push. That decision is conferred on DHS by U.S. law.*

Discussion: Under the 2007 Letter, DHS stated that it would move as expeditiously as possible to a "push" system of transmitting PNR, to accommodate airlines no later than January 1, 2008, and to provide technical guidance as necessary. CBP reached out extensively to the carriers regarding the need to move to a "push" system and provided the Privacy Office with a list of every carrier that is currently operating a "push" system and those continuing to operate a "pull" system. CBP made every effort to meet the January 1, 2008, deadline for those carriers capable or nearing capability of operating a "push" system.

For those airlines that were continuing to operate "pull" systems, CBP has provided extensive technical guidance on how to implement a "push" system and how best to interface with CBP once that system is established, but CBP does not currently have authority to force carriers to implement such a "push" system. CBP stated to the Privacy Office that airlines that are capable

of implementing or capable of progressing to implementation of a "push" system have been responsive to CBP's guidance.

For those airlines not capable of implementing a "push" system by January 1, 2008, CBP provided technical guidelines to enable that implementation as expeditiously as possible and continues to work closely with them to move the airlines to the "push" system.

Findings: The Privacy Office finds that CBP is in compliance with representations made in the 2007 Letter. CBP has done and continues to do the necessary outreach to, and education of the carriers, but the carriers are in control of whether their system can adopt a "push" system and absent a regulatory requirement mandating "push", there is currently no way to ensure 100% transition.

Roman Numeral VIII of the 2007 Letter*: Under normal circumstances DHS will receive an initial transmission of PNR data 72 hours before a scheduled departure and afterwards will receive updates as necessary to ensure data accuracy. Ensuring that decisions are made based on timely and complete data is among the most essential safeguards for personal data protection and DHS works with individual carriers to build this concept into their push systems. DHS may require PNR prior to 72 hours before the scheduled departure of the flight, when there is an indication that early access is necessary to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with the purposes defined in article I. In exercising this discretion, DHS will act judiciously and with proportionality.*

Discussion: DHS obligations under this provision are twofold: to ensure that PNR is received from carriers 72 hours before a scheduled departure, and when early access is required, DHS act in accordance with its stated purposes in the 2007 Letter and with judiciousness and proportionality.

In interviews conducted with NTC analysts and PAU officers, no analysts or officers had accessed PNR data prior to 72 hours using the exceptional circumstances rationale. Generally, the information is reviewed within 72 hours of a particular flight.

Findings: CBP has not sought PNR ahead of the standard 72 hours based on exceptional circumstances. The Privacy Office finds CBP in compliance with the stated requirements.

9. Reciprocity

ATS SORN: This topic is outside the scope of the ATS SORN.

Roman Numeral IX of the 2007 Letter*: During our recent negotiations we agreed that DHS expects that it is not being asked to undertake data protection measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems. DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of the DHS letter while conducting consultations with the EU with a view to reaching a prompt and satisfactory resolution. In the*

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

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

Findings: Privacy Office finds that DHS and CBP are in compliance with the 2007 Letter. While some European authorities have welcomed discussions with DHS about their PNR and similar systems, DHS has not been afforded any detailed assessment of how these systems are operated on a European scale. DHS has not exercised its authority to suspend provisions of the letter and request consultations. Greater transparency on the part of many European authorities would allow for a more effective implementation of this provision.

10. Review

ATS SORN: This topic is outside the scope of the ATS SORN.

Roman Numeral X of the 2007 Letter: *DHS and the EU will periodically review the implementation of the agreement, this letter, U.S. and EU PNR policies and practices and any instances in which sensitive data was accessed, for the purpose of contributing to the effective operation and privacy protection of how practices for processing PNR. In the review, the EU will be represented by the Commissioner for Justice, Freedom and Security, and DHS will be represented by the Secretary of Homeland Security, or by such mutually acceptable official as each may agree to designate. The EU and DHS will mutually determine the detailed modalities of the reviews.*

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

Discussion: This review has been completed in order to comply with this portion of the 2007 Letter and the U.S.-EU Agreement.

Findings: Through this review and ongoing discussion with the EU, DHS has complied with this portion of the 2007 Letter.

V. Conclusion

Based on the above comprehensive review, the Privacy Office finds that DHS and CBP are in compliance with ATS SORN and the 2007 Letter.

APPENDIX 1: Lifecycle of 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 is a wide spectrum of air carrier reservation systems; 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.

PNR has three primary sections: *Active Portion*, which contains the name(s) of the passenger(s), the itinerary; *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, as in other regions of the world, 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 includes 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 PNR forward

Step 1: CBP pulls the approved categories of data from 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 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. 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 approved categories of data stated in the ATS SORN. The remaining elements of the PNR are deleted by CBP and are not accessible through the system. Categories outside those in the ATS SORN are deleted and cannot be re-created after 30 days.

Step 4: At seven years after the end of travel specified in the itinerary of the PNR, the PNR data will be moved to a dormant, non operational status, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.

Step 5: At 15 years from receipt date/time given in the record, PNR will be deleted, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.

APPENDIX 2: Automated Targeting System (ATS) System of Records Notice

[Federal Register: August 6, 2007 (Volume 72, Number 150)]
[Notices]
[Page 43650-43656]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr06au07-61]

==========

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[DHS-2007-0042]

Privacy Act of 1974; U.S. Customs and Border Protection, Automated Targeting System, System of Records

AGENCY: Privacy Office; Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: This document is a new System of Records Notice (SORN) for the Automated Targeting System (ATS) and is subject to the Privacy Act of 1974, as amended. ATS is an enforcement screening tool consisting of six separate components, all of which rely substantially on information in the Treasury Enforcement Communications System (TECS). ATS historically was covered by the SORN for TECS. The Department of Homeland Security, U.S. Customs and Border Protection (CBP) published a separate SORN for ATS in the Federal Register on November 2, 2006. This SORN did not describe any new collection of information and was intended solely to provide increased notice and transparency to the public about ATS. Based on comments received in response to the November 2, 2006 notice, CBP issues this revised SORN, which responds to those comments, makes certain amendments with regard to the retention period and access provisions of the prior notice, and provides further notice and transparency to the public about the functionality of ATS.

TECS is an overarching law enforcement information collection, risk assessment, and information sharing environment. It is also a repository for law enforcement and investigative information. TECS is comprised of several modules that collect, maintain, and evaluate screening data, conduct targeting, and make information available to appropriate officers of the U.S. government. ATS is one of those modules. It is a decision support tool that compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. As such, ATS allows DHS officers charged with enforcing U.S. law and preventing terrorism and other crimes to effectively and efficiently manage information collected when travelers or goods seek to enter,

exit, or transit through the United States.

Within ATS there are six separate and distinct components that perform screening of inbound and outbound cargo, conveyances, or travelers. These modules compare information received against CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts using law enforcement data, intelligence, and past case experience. The modules also facilitate analysis of the screening results of these comparisons. In the case of cargo and conveyances, this screening results in a risk assessment score. In the case of travelers, however, it does not result in a risk assessment score.

DATES: The new system of records will be effective September 5, 2007.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-572-8790), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of

[[Page 43651]]

International Trade, Mint Annex, 1300 Pennsylvania Ave., NW., Washington, DC 20229. For privacy issues please contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The System

The priority mission of CBP is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. ATS uses CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts to assess and identify high-risk cargo, conveyances, and travelers that may pose a greater risk of terrorist or criminal activity and therefore should be subject to further scrutiny or examination. These rules are based on investigatory and law enforcement data, intelligence, and past case experience. Historically, the SORN for the Treasury Enforcement Communications System (TECS) covered ATS. As part of DHS's updating of its system of records notices and in an effort to provide more detailed information to the traveling public and trade community, DHS has decided to notice ATS as a separate Privacy Act system of records, giving greater visibility into its targeting and screening efforts.

TECS is an overarching law enforcement information collection, risk assessment, and information sharing environment. It is also a repository for law enforcement and investigative information. TECS is comprised of several modules that collect, maintain, and evaluate screening data, conduct targeting analysis, and make information available to appropriate officers of the U.S. government. ATS is one of those modules. It is a decision-support tool that compares traveler,

cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. As such, ATS allows DHS officers charged with enforcing U.S. law and preventing terrorism and other crime to effectively and efficiently manage information collected when travelers or goods seek to enter, exit, or transit through the United States. Within ATS there are six separate and distinct components that perform screening of inbound and outbound cargo, conveyances, or travelers by comparing information received against CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts based on law enforcement data, intelligence, and past case experience. The modules also facilitate analysis of the screening results of these comparisons.

As a legacy organization of CBP, the U.S. Customs Service traditionally employed computerized screening tools to target potentially high-risk cargo entering, exiting, and transiting the United States. ATS originally was designed as a rules-based program to identify such cargo; it did not apply to travelers. Today, ATS includes the following separate components: ATS-N, for screening inbound or imported cargo; ATS-AT, for outbound or exported cargo; ATS-L, for screening private passenger vehicles crossing at land border ports of entry using license plate data; ATS-I, for cooperating with international customs partners in shared cargo screening and supply chain security; ATS-TAP, for assisting tactical units in identifying anomalous trade activity and performing trend analysis; and ATS-P, for screening travelers and conveyances entering the United States in the air, sea, and rail environments. The Privacy Impact Assessment (PIA)--which DHS will publish on its Web site (http://www.dhs.gov/privacy)

concurrently with the publication of the SORN in the Federal Register--provides a full discussion of the functional capabilities of ATS and its components. It is worth clarifying here, however, that only the ATS components pertaining to cargo rely on rules-based ``scoring'' to identify cargo shipments of interest. Travelers identified by risk-based targeting scenarios identified through the ATS-P are not assigned scores.

ATS-P became operational in 1999 and is critically important to CBP's mission. ATS-P allows CBP officers to determine whether a variety of potential risk indicators exist for travelers and/or their itineraries that may warrant additional scrutiny. ATS-P maintains Passenger Name Record (PNR) data, which is data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. CBP began receiving PNR data voluntarily from air carriers in 1997. Currently, CBP collects this information as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).

ATS-P's screening relies upon information from the following databases: TECS, the Advanced Passenger Information System (APIS), the Non Immigrant Information System (NIIS), the Suspect and Violator Indices (SAVI), and the Department of State visa databases, as well as the PNR information that it maintains. As stated above, unlike in the cargo environment, ATS-P does not use a score to determine an individual's risk level; instead, ATS-P compares PNR and information in the above-mentioned databases against lookouts and patterns of suspicious activity identified by analysts based upon past

investigations and intelligence. This risk assessment is an analysis of the threat-based scenario(s) that a traveler matched when traveling on a given flight. These scenarios are drawn from previous and current law enforcement and intelligence information. This analysis is done in advance of a traveler's arrival in or departure from the United States and becomes one tool available to DHS officers in identifying illegal activity. In lieu of manual reviews of traveler information and intensive interviews with every traveler arriving in or departing from the United States, ATS-P allows CBP personnel to focus their efforts on potentially high-risk passengers.

The Legal Requirements

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a ``system of records.'' A system of records is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. ATS involves the collection and creation of information that is maintained in a system of records. ATS also stores information on individuals other than U.S. citizens and lawful permanent residents (LPRs). As a matter of administrative policy, where the PII of individuals other than U.S. citizens and LPRs is held in mixed systems (i.e., a system also including U.S. citizen or LPR), DHS will accord

[[Page 43652]]

such PII the fair information principles set forth the Privacy Act.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system to make agency recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, to assist the individual to more easily find such files within the agency, and to inform the public if any applicable Privacy Act exemptions will be claimed for the system.

Access to information in ATS may be provided. However, as discussed further later in this notice, certain records within ATS are exempt from certain provisions of the Privacy Act (specifically, those provisions contained at 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g)) pursuant to 5 U.S.C. 552a(j)(2) and (k)(2)). Notwithstanding the listed exemptions for the system, individuals, regardless of their citizenship, may make a written request to review and access personal data provided by and regarding the requester, or provided by a booking agent, brokers, or other person on the requester's behalf, that is collected by CBP and contained in the PNR database stored in the ATS-P, and correct any inaccuracies. Data collected and maintained from air carriers as PNR are listed later in this notice in the ``Categories of Records in the System'' section of this notice; the listed categories are not specific data elements because each carrier varies its

configuration of PNR to meet its business needs. In an effort to provide some consistency in the description of PNR data for the traveling public, CBP has categorized the various data that generally comprise PNR for air carriers into the 19 categories listed in the SORN. The PNR data, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record, such as use and application of frequent flier miles, internal annotations to the air fare, etc.

To obtain access to a requestor's own PNR, contact the FOIA/PA Branch, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791). Additionally, regardless of their citizenship, individuals who believe they have been erroneously denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through DHS Traveler Redress Inquiry Program (``TRIP''). (See 72 FR 2294, January 18, 2007). For further information on the Automated Targeting System and the redress options, please see the accompanying Privacy Impact Assessment for the Automated Targeting System at http://www.dhs.gov/privacy under ``Privacy Impact Assessment.'' Redress requests should be sent to: Systems Manager, DHS TRIP, U.S. Department of Homeland Security, Washington, DC.

DHS is hereby publishing a description of the system of records referred to as the Automated Targeting System. In accordance with 5 U.S.C. 552a(r), a report concerning this record system has been sent to the Office of Management and Budget and to the Congress.

Discussion of Revisions Arising From Public Comments:

On November 2, 2006, CBP issued a Privacy Act System of Records Notice for ATS (71 FR 64543). DHS received a number of comments and decided to extend the comment period until December 29, 2006, by Federal Register Notice dated December 8, 2006 (71 FR 71182). A total of 641 comments were received in response to the SORN. After considering these comments, CBP has made the following substantive changes to the previously issued SORN. First, the general retention period for data maintained in ATS is reduced from 40 years to a total of 15 years. CBP has determined that it can continue to uncover and use information relating to terrorism and other serious crimes within this shorter retention period.

This retention period is consistent with the retention period currently contained in international agreements entered into by the Department. Furthermore, CBP has limited access to the last eight years of the retention period for PNR data to those users who first obtain supervisory approval to access the archive where the data is maintained. CBP, however, has created an exception to this general retention period such that PNR data, as well as any other data that may be stored in ATS, which becomes associated with active law enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

Second, persons whose PNR data has been collected and maintained in ATS-P will have administrative access to that data under the Privacy Act. This data will be available in the same format that it was

obtained by CBP (with the exception of business confidential information that may be contained in the record). These individuals will also be able to seek to correct factual inaccuracies contained in their PNR data, as it is maintained by CBP. CBP believes that permitting persons to access and to seek to amend their PNR data will reduce the incidence of potential misidentifications and improve the accuracy of the data within ATS-P.

Third, CBP has added the following category to the categories of persons from whom information is obtained: ``Persons who serve as booking agents.'' Several commenters correctly noted that many in the traveling public utilize the services of booking agents and that booking agents' identities are included in itinerary information.

Fourth, to be consistent with the forthcoming SORN for the Advanced Passenger Information System (APIS), CBP has amended category A to include persons whose international itineraries cause their flight to stop in the United States, either to refuel or to permit a transfer, and crewmembers on flights that overfly or transit through U.S. airspace.

Fifth, as stated above, CBP has clarified the categories of PNR data collected and maintained in ATS-P to more accurately reflect the type of data collected from air carriers. Consistent with its particular business needs, each air carrier determines the specific configuration of data elements that ultimately constitute PNR. By providing increased notice of the types of data that may be contained within PNR, CBP seeks to provide the public with a greater understanding of the personal information being maintained in ATS-P. Examples of these categories of PNR, as listed below under ``Categories of Records'' include: Name, date of issuance ticket, date(s) of travel, PNR locator number, payment information, such as credit card information, and travel agent or travel agency that may have made the reservations for the individual.

Lastly, two of the routine uses included in the earlier version of the SORN-those pertaining to using ATS in background checks--are removed. This is necessary because the revised SORN contains a more narrow definition of the purposes for which certain data--

[[Page 43653]]

specifically, PNR data maintained in ATS-P--will be used. The deleted routine uses did not fit within the scope of these purposes.

This discussion of comments addresses revisions made to the SORN published on November 2, 2006. The full comments received address additional issues, such as mission creep, potential economic impact, appropriate applicability of the Privacy Act, constitutionality, and information quality. For a discussion of the full comments received from the November 2, 2006, publication and DHS' response, please see ``Discussion of Public Comments Received on the Automated Targeting System Privacy Act System of Records Notice'' on the DHS Web site at http://www.dhs.gov/privacy.

SYSTEM NAME:

Automated Targeting System (ATS)--CBP.

SYSTEM LOCATION:

This computer database is located at the CBP National Data Center in Washington, D.C. Computer terminals are located at customhouses, border ports of entry, airport inspection facilities under the

jurisdiction of DHS, and other locations at which DHS authorized personnel may be posted to facilitate DHS's mission. Terminals may also be located at appropriate facilities for other participating government agencies pursuant to agreement.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

ATS includes the following separate components: ATS-N, for screening inbound or imported cargo; ATS-AT, for outbound or exported cargo; ATS-L, for screening private passenger vehicles crossing at land border ports of entry by license plate data; ATS-I, for cooperating with international customs partners in shared cargo screening and supply chain security; ATS-TAP, for assisting tactical units in identifying anomalous trade activity and performing trend analysis; and ATS-P, for screening travelers and conveyances entering the United States in the air, sea and rail environments.

Collectively, these components handle information relating to the following individuals:

A. Persons seeking to enter, exit, or transit through the United States by land, air, or sea. This includes passengers who arrive and depart the United States by air or sea, including those in transit through the United States on route to a foreign destination and crew members who arrive and depart the United States by air or sea, including those in transit through the United States on route to a foreign destination, and crew members on aircraft that over fly the United States.

B. Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise.

C. Persons who are employed in any capacity related to the transit of merchandise intended to cross the United States border.

D. Persons who serve as operators, crew, or passengers on any vessel, vehicle, aircraft, train, or other conveyance that arrives in or departs the United States.

E. Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter, exit, or transit through the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

ATS uses CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts to assess and identify high-risk cargo, conveyances, or travelers that should be subject to further scrutiny or examination. ATS maintains these assessments together with a record of which rules were used to develop the assessment. With the exception of PNR information, discussed below, ATS maintains a pointer or reference to the underlying records from other systems that resulted in a particular assessment.

ATS-P, a component of ATS, maintains the PNR information obtained from commercial air carriers and uses that information to assess whether there is a risk associated with any travelers seeking to enter, exit, or pass through the United States. PNR may include some combination of these following categories of information, when available:

1. PNR record locator code.
2. Date of reservation/ issue of ticket.
3. Date(s) of intended travel.

4. Name(s) .
5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.).
6. Other names on PNR, including number of travelers on PNR.
7. All available contact information (including originator of reservation).
8. All available payment/billing information (e.g. credit card number).
9. Travel itinerary for specific PNR.
10. Travel agency/travel agent.
11. Code share information (e.g., when one air carrier sells seats on another air carrier's flight).
12. Split/divided information (e.g., when one PNR contains a reference to another PNR).
13. Travel status of passenger (including confirmations and check-in status).
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields.
15. Baggage information.
16. Seat information, including seat number.
17. General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information.
18. Any collected APIS information (e.g., Advance Passenger Information (API) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender).
19. All historical changes to the PNR listed in numbers 1 to 18.

Not all air carriers maintain the same sets of information for PNR, and a particular individual's PNR likely will not include information for all possible categories. In addition, PNR does not routinely include information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual. To the extent PNR does include terms that reveal such personal matters, DHS employs an automated system that filters certain of these terms and only uses this information in exceptional circumstances.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

19 U.S.C. 482, 1461, 1496, and 1581-82, 8 U.S.C 1357, Title VII of Public Law 104-208, 49 U.S.C. 44909, and the ``Security and Accountability for Every Port Act of 2006'' (SAFE Port Act) (Pub. L. 109-347).

PURPOSES FOR PNR IN ATS-P:

(a) To prevent and combat terrorism and related crimes;
(b) To prevent and combat other serious crimes, including organized crime, that are transnational in nature;
(c) To prevent flight from warrants or custody for crimes described in (a) and (b) above;
(d) Wherever necessary for the protection of the vital interests of a data subject or other persons;
(e) In any criminal judicial proceedings; or
(f) As otherwise required by law.

[[Page 43654]]

PURPOSES OF ATS (EXCEPT PNR IN ATS-P):

In addition to those purposes listed above for PNR in ATS-P:

(a) To perform targeting of individuals, including passengers and crew, focusing CBP resources by identifying persons who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law.

(b) To perform a risk-based assessment of conveyances and cargo to focus CBP's resources for inspection and examination and enhance CBP's ability to identify potential violations of U.S. law, possible terrorist threats, and other threats to border security; and

(c) To otherwise assist in the enforcement of the laws enforced or administered by DHS, including those related to counterterrorism.

ROUTINE USES OF RECORDS MAINTAINED IN THE VARIOUS COMPONENTS OF ATS, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3). DHS only discloses information to those authorities who have a legal purpose to use the data, intend to use the information consistent with the purpose for which CBP collects it or for another legally required function, such as GAO oversight and ongoing IT maintenance, and has sufficient capability to protect and safeguard it. Under these limits, data may be disclosed as a routine use in the following manner:

A. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws;

B. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

C. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a data subject and such disclosure is proper and consistent with the official duties of the person making the disclosure;

D. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk;

E. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in response to a subpoena, or in connection with criminal law proceedings;

F. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate in the proper performance of the official duties of the officer making the disclosure.

G. To an agency, organization, or individual for the purposes of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function;

H. To a Congressional office, for the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains;

I. To contractors, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records, in compliance with the Privacy Act of 1974, as amended;

J. To the U.S. Department of Justice (including U.S. Attorney offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent said employee, or (d) the United States or any agency thereof;

K. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. Sections 2904 and 2906;

L. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations where CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance ATS;

M. To appropriate agencies, entities, and persons when (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons when reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM

STORAGE:

The data is stored electronically at the National Data Center for current data and offsite at an alternative data storage facility for historical logs and system backups.

RETRIEVABILITY:

The data is retrievable by name or personal identifier from an

electronic database.

SAFEGUARDS:
    All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include all of the following: restricting access to those with a ``need to know''; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications.
    ATS also monitors source systems for changes to the source data. The system

[[Page 43655]]

manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. ATS information is secured in full compliance with the requirements of the Federal Information Security Management Act (FISMA) and the DHS IT Security Program Handbook. This handbook establishes a comprehensive information security program.

USE AND CONTROL:
    CBP maintains full access for a limited number of authorized personnel to all information contained within ATS. Authorized personnel receive thorough background investigations and extensive training on CBP security and privacy policies on the appropriate use of ATS information. These individuals are trained to review the risk assessments and background information to identify individuals who may likely pose a risk. To ensure that ATS is being accessed and used appropriately, audit logs are also created and reviewed routinely by CBP's Office of Internal Affairs to ensure integrity of the system and process.
    Access to the risk assessment results and related rules is restricted to a limited number of authorized government personnel who have gone through extensive training on the appropriate use of this information and CBP policies, including for security and privacy. These All individuals are specifically trained to review the risk assessments and background information to identify individuals who may likely pose a risk.

RETENTION AND DISPOSAL:
    Records in this system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration. ATS both collects information directly, and derives other information from various systems. To the extent information is collected from other systems, data is retained in accordance with the record retention requirements of those systems.
    The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be deleted, except as noted below. The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions: ATS-P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary

of Homeland Security and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers. Notwithstanding the foregoing, information maintained only in ATS that is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

It is important to note that the justification for a fifteen year retention period is based on CBP's law enforcement and security functions at the border. This retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Passenger records including historical records are essential in assisting CBP Officers with their risk-based screening of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing these records for these purposes allows CBP to continue to effectively identify suspect travel patterns and irregularities.

SYSTEM MANAGER(S) AND ADDRESS:

Executive Director, National Targeting and Security, Office of Field Operations, U.S. Customs and Border Protection, Ronald Reagan Building and Director, Targeting and Analysis, Systems Program Office, Office of Information Technology, U.S. Customs and Border Protection.

PUBLIC RECORD ACCESS/REDRESS PROCEDURES:

DHS policy allows persons (including foreign nationals) to access and redress under the Privacy Act to raw PNR data maintained in ATS-P. The PNR data, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record, such as . This access does not extend to other information in ATS obtained from official sources (which are covered under separate SORNs) or that is created by CBP, such as the targeting rules and screening results, which are law enforcement sensitive information and are exempt from certain provisions of the Privacy Act. For other information in this system of records, individuals generally may not seek access for purposes of determining if the system contains records pertaining to a particular individual or person. (See 5 U.S.C. 552a (e)(4)(G) and (f)(1)).

Individuals, regardless of nationality, may seek access to records about themselves in accordance with the Freedom of Information Act. In addition, DHS policy allows persons, including foreign nationals, to seek access under the Privacy Act to raw PNR data submitted to ATS-P. Requests for access to personally identifiable information contained in PNR that was provided by the requestor or by someone else on behalf of the requestor, regarding the requestor, may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.50C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791). Requests should conform to the

requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked ``Privacy Act Access Request.'' The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

CBP notes that ATS is a decision-support tool that compares various databases, but does not actively collect the information in those respective databases, except for PNR. When an individual is seeking redress for other information analyzed in ATS, such redress is properly accomplished by referring to the databases that directly collect that information. If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program (``TRIP''). See 72 FR 2294, dated January 18, 2007. Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for

[[Page 43656]]

additional screening by CBP may submit a redress request through TRIP. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs--like airports and train stations or crossing U.S. borders. Through TRIP, a traveler can request correction of erroneous PNR data stored in ATS-P and other data stored in other DHS databases through one application. Additionally, for further information on ATS and the redress options please see the accompanying PIA for ATS published on the DHS website at http://www.dhs.gov/privacy.

Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at http://www.dhs.gov/trip and at http://www.dhs.gov.

Additionally, a traveler may seek redress from CBP at the time of the border crossing.

CONTESTING RECORD PROCEDURES:

Individuals may seek redress and/or contest a record through several different means, all of which will be handled in the same fashion. If the individual is aware the information is specifically handled by CBP, requests may be sent directly to CBP at the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791). If the individual is uncertain what agency is responsible for maintaining the information, redress requests may be sent to DHS TRIP at DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at http://www.dhs.gov/trip.

RECORD SOURCE CATEGORIES:

The system contains information derived from other law enforcement systems operated by DHS and federal, state, local, tribal, or foreign government agencies, which collected the underlying data from individuals and public entities directly.

The system also contains information collected from carriers that operate vessels, vehicles, aircraft, and/or trains that enter or exit the United States. In addition, the cargo modules (ATS-Inbound and Outbound) employ information collected from third party data aggregators.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to 6 CFR Part 5, Appendix C, certain records and information in this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2)). With respect to ATS-P module, exempt records are the risk assessment analyses and business confidential information received in the PNR from the air and vessel carriers. No exemption shall be asserted regarding PNR data about the requester, obtained from either the requester or by a booking agent, brokers, or another person on the requester's behalf. This information, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record. For other ATS modules the only information maintained in ATS is the risk assessment analyses and a pointer to the data from the source system of records.

Dated: July 31, 2007.
Hugo Teufel III,
Chief Privacy Officer.
[FR Doc. E7-15197 Filed 8-1-07; 11:51 am]

BILLING CODE 4410-10-P

APPENDIX 3: Agreement Between the United States of America and the European Union on Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)

DECLARATION ON BEHALF OF THE EUROPEAN UNION TO THE AGREEMENT BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA ON THE PROCESSING AND TRANSFER OF PASSENGER NAME RECORD (PNR) DATA BY AIR CARRIERS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY (DHS) (2007 PNR AGREEMENT)

"This Agreement, while not derogating from or amending legislation of the EU or its Member States, will, pending its entry into force, be implemented provisionally by Member States in good faith, in the framework of their existing national laws."

APPENDIX 4: Letter from the Council of European Union to the United States

COUNCIL OF THE EUROPEAN UNION

Brussels, 23 July 2007

FULL POWERS

THE PRESIDENT OF THE COUNCIL OF THE EUROPEAN UNION

has decided by these presents to confer full powers on

Luis AMADO

Minister of State
Minister for Foreign Affairs of the Portuguese Republic,
President of the Council of the European Union,

to sign and provisionally apply, on behalf of the European Union, the 2007 Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS).

The Council, upon completion of the internal procedures necessary for the conclusion of the Agreement, reserves the right to approve the instruments signed by its Plenipotentiary in pursuance of the full powers conferred by these presents.

The President of the Council

of the European Union

COUNCIL OF
THE EUROPEAN UNION

The Presidency

Brussels, 23 July 2007

Secretary Michael Chertoff

U.S. Department for Homeland Security

Washington DC 20528

Dear Secretary,

Thank you very much for your letter to the Council Presidency and the Commission explaining how DHS handles PNR data.

The assurances explained in your letter provided to the European Union allow the European Union to deem, for the purposes of the international agreement signed between the United States and European Union on the processing and transfer of PNR in July 2007 that DHS ensures an adequate level of data protection.

Based on this finding, the EU will take all necessary steps to discourage international organisations or third countries from interfering with any transfers of EU PNR to the United States. The EU and its Member States will also encourage their competent authorities to provide analytical information flowing from PNR data to DHS and other US authorities concerned.

We look forward to working with you and the aviation industry to ensure that passengers are informed about how governments may use their information.

Yours sincerely,

Luis Amado
President of the Council

APPENDIX 5: Letter from United States to the Council of European Union (2007 Letter)

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 26, 2007

Mr. Luis Amado
President of the Council of the European Union
175 Rue de la Loi
1048 Brussels Belgium

Dear President of the Council of the European Union,

In response to the inquiry of the European Union and to reiterate the importance that the United States government places on the protection of individual privacy, this letter is intended to explain how the United States Department of Homeland Security (DHS) handles the collection, use and storage of Passenger Name Records (PNR). None of the policies articulated herein create or confer any right or benefit on any person or party, private or public, nor any remedy other than that specified in the Agreement between the EU and the U.S. on the processing and transfer of PNR by air carriers to DHS signed in July 2007 (the "Agreement"). Instead, this letter provides the assurances and reflects the policies which DHS applies to PNR data derived from flights between the U.S. and European Union (EU PNR) under U.S. law.

I. Purpose for which PNR is used: DHS uses EU PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law. DHS will advise the EU regarding the passage of any U.S. legislation which materially affects the statements made in this letter.

II. Sharing of PNR:

DHS shares EU PNR data only for the purposes named in article I.

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

proportion to the nature of the case.

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

III. Types of Information Collected:

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

Types of EU PNR Collected:

1. PNR record locator code,
2. Date of reservation/ issue of ticket
3. Date(s) of intended travel
4. Name(s)
5 Available frequent flier and benefit information (i.e., free tickets, upgrades, etc)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator information)
8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote
15. All Baggage information
16. Seat information, including seat number
17. General remarks including OSI, SSI and SSR information
18. Any collected APIS information
19. All historical changes to the PNR listed in numbers 1 to 18

To the extent that sensitive EU PNR data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual), as specified by the PNR codes and terms which DHS has identified in consultation with the European Commission, are included in the above types of EU PNR data, DHS employs an automated system which filters those sensitive

PNR codes and terms and does not use this information. Unless the data is accessed for an exceptional case, as described in the next paragraph, DHS promptly deletes the sensitive EU PNR data.

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

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

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

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

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

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

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

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

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

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

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

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

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

X. Review: DHS and the EU will periodically review the implementation of the agreement, this letter, U.S. and EU PNR policies and practices and any instances in which sensitive data was accessed, for the purpose of contributing to the effective operation and privacy protection of our practices for processing PNR. In the review, the EU will be represented by the Commissioner for Justice, Freedom and Security, and DHS will be represented by the Secretary of Homeland Security, or by such mutually acceptable official as each may agree to designate. The EU and DHS will mutually determine the detailed modalities of the reviews.

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

We trust that this explanation has been helpful to you in understanding how we handle EU PNR data.

Sincerely,

Michael Chertoff

Secretary of Homeland Security