A REPORT ON
THE USE AND TRANSFER OF PASSENGER NAME RECORDS BETWEEN THE EUROPEAN UNION AND THE UNITED STATES

U.S. Department of Homeland Security
Privacy Office

June 26, 2015

LETTER FROM THE CHIEF PRIVACY OFFICER

In December 2011, the U.S. Department of Homeland Security (DHS) and the Council of the European Union signed an *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security* regarding the transfer of PNR to DHS by air carriers operating flights between the U.S. and the European Union (2011 Agreement). After parliamentary ratification, the Agreement entered into force on July 1, 2012. 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 programs and operations. This report fulfills my office's statutory duty and satisfies the 2011 Agreement's provision for independent review and oversight of the Department's implementation by my office.[1]

It is my pleasure to report, along with my staff, that DHS continues to comply with the 2011 Agreement and with representations made in the Privacy Impact Assessment and System of Records Notice for the Automated Targeting System, the DHS system that maintains PNR. This report also recommends areas for continued improvement to protect travelers' privacy while enhancing the value of PNR as a critical tool in protecting our homeland.

U.S. Customs and Border Protection (CBP) staff deserve recognition for their diligent work with the DHS Privacy Office preceding and during our review, for producing all documents and information requested, and for implementing recommendations from previous DHS Privacy Office reports on the Department's use of PNR. I would also like to personally recognize CBP Commissioner R. Gil Kerlikowske for his partnership.

We look forward to the upcoming Joint Review with the European Commission and to continuing our cooperative efforts to integrate privacy protections into the means through which countries on both sides of the Atlantic carry out our important security missions.

Karen L. Neuman
Chief Privacy Officer
U.S. Department of Homeland Security

[1] 2011 Agreement, Article 14 (Oversight), available at http://www.dhs.gov/sites/default/files/publications/dhsprivacy_PNR%20Agreement_12_14_2011.pdf.

TABLE OF CONTENTS

I. OVERVIEW

The DHS Privacy Office conducted this Privacy Compliance Review (PCR) pursuant to the Chief Privacy Officer's authority under Section 222 of the Homeland Security Act of 2002 to determine whether the Department of Homeland Security (DHS), in particular, U.S. Customs and Border Protection (CBP), is operating in compliance with the standards and representations in (1) the Automated Targeting System (ATS) System of Records Notice[2] (SORN), (2) the ATS Privacy Impact Assessment[3] (PIA), and (3) the *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security* dated December 14, 2011 (2011 Agreement).[4] The review also evaluated the Department's implementation of recommendations from the 2008,[5] 2010,[6] and 2013[7] PCRs *Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union* (2008, 2010, and 2013 DHS Privacy Office Reports, respectively).

A PNR is a record of travel information created by commercial air carriers that could include each passenger's name, destination, method of payment, flight details, and a summary of communications with airline representatives. PNR is stored in ATS, a custom-designed system used at locations at which CBP maintains a presence, and at the CBP National Targeting Center (NTC).[8] The ATS-Passenger (ATS-P) module facilitates the CBP officer's decision-making about whether a passenger or crew member should receive additional inspection prior to entry into, or departure from, the United States. The officer uses PNR within ATS-P to help decide if that person poses a greater risk for terrorism and related crimes or other serious transnational crimes, to identify individuals for further examination upon arrival/departure, or to protect the vital interests of the individual. A select number of other DHS personnel have access to ATS-P and the PNR held by DHS to fight serious crime and terrorism. The CBP PNR Directive[9] and auditing functions mentioned throughout this report apply to all users of ATS-P.

The DHS Privacy Office reviewed ongoing PNR policies and practices from June 1, 2013 to February 1, 2015 (unless otherwise indicated), including the details of PNR received and reviewed by DHS and information sharing practices with non-DHS entities. The DHS Privacy Office found PNR policies and practices, including how PNR is received, used, and disseminated by CBP, to be substantially compliant with the 2011 Agreement and related provisions in the ATS SORN and ATS PIA.

The DHS Privacy Office found that steps taken by DHS in response to recommendations from the 2008 and 2010 DHS Privacy Office reports remain in place. Almost all of the recommendations from the 2013 DHS Privacy Office report and the European Commission's

[2] http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm, May 22, 2012.
[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf, June 1, 2012.
[4] http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf.
[5] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.
[6] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_review2010update_2010-02-05.pdf.
[7] http://www.dhs.gov/sites/default/files/publications/dhs-pnr-privacy-review-20130703.pdf.
[8] NTC is a division of CBP responsible for national security targeting operations.
[9] The CBP PNR Directive outlines the appropriate use, handling, storage, and disclosure of PNR information.

November 2013 report have been fully implemented. CBP policies and procedures to review user access to PNR, receive timely alerts regarding any access to sensitive PNR, and provide managers notice of user access to depersonalized data or to PNR lacking a U.S. nexus remain effectively in place. CBP is in the process of developing procedures to implement the dormant PNR database required by Article 8 of the 2011 Agreement. CPB will be fully compliant with this requirement before PNR becomes subject to retention in the dormant database on July 1, 2017.

CBP continues to employ automated filters in ATS that block access to PNR collected pursuant to its regulations that do not have a clear nexus to the United States and continues to automatically mask sensitive PNR fields. The DHS Privacy Office found disclosures of PNR to DHS users, non-DHS users, and foreign authorities to be authorized and compliant with the ATS SORN, ATS PIA, and the 2011 Agreement. CBP updated its disclosure forms to better audit the purpose for the disclosure and appropriately logged the PNR disclosures electronically to make review and reporting readily auditable. There have been no reports to either the DHS Privacy Office or CBP of PNR use that was inconsistent with Article 4 of the 2011 Agreement since the Agreement's entry into force on July 1, 2012. Furthermore, CBP has made significant progress in encouraging airlines to "push" PNR to CBP. As of May 18, 2015, 93 percent of air carriers[10] affected by the 2011 Agreement (50 of 54[11]) had transitioned to the "push" system, an increase of 25 percent since the 2013 DHS Privacy Office Report.

A. 2015 Recommendations

- *Transparency*

The DHS Privacy Office found that there are numerous mechanisms by which the Department provides information on its use of PNR and opportunities for individuals to seek access to information and to seek redress.

- *Recommendation: Due to organizational changes within CBP, public facing documents should be updated with correct addresses and points of contact.*
- *Recommendation: To increase awareness in the EU, CBP and the Office of Policy should work with EU-based U.S. embassies to add additional PNR and redress related information on the travel portion of their websites.*
- *Recommendation: To increase awareness in the EU, the Office of Policy should provide the European Commission with similar information for Member State distribution.*

- *Use Limitation*

The DHS Privacy Office found that CBP's use and sharing of PNR, both domestically and internationally, is compliant with the ATS SORN, ATS PIA, and the 2011 Agreement.

- *Recommendation: While the DHS Privacy Office recognizes that the process to depersonalize PNRs after six months is working effectively, CBP should promptly*

[10] "Affected air carriers" includes carriers that operate passenger flights between the U.S. and the EU as well as those incorporated or storing data in the EU and operating passenger flights to or from the U.S.
[11] Note that this number can change given that commercial air carriers alter routes offered to/from the U.S. over time.

review its process for linking PNR to a law enforcement event to ensure adherence to the depersonalization requirements of the 2011 Agreement.

- *Recommendation: CBP and the Office of Policy should finalize the draft protocol to notify EU Member States, as appropriate, of any sharing of EU PNR with third countries.*
- *Recommendation: CBP, together with the DHS Office of Policy, the CBP Privacy Office, and the DHS Privacy Office, should continue to review existing and future domestic and international information sharing arrangements to ensure that all PNR sharing is in accordance with the ATS SORN, ATS PIA, and the 2011 Agreement. CBP should maintain a repository of such arrangements for easy reference to confirm sharing of PNR is appropriate and protected.*

- *Data Minimization*

The DHS Privacy Office found that CBP's PNR retention schedule is compliant with the ATS SORN, ATS PIA, and the 2011 Agreement.

- *Recommendation: CBP should begin to develop implementing documents for the dormant database in preparation for the July 1, 2017 start date.*

- *Individual Participation*

The DHS Privacy Office had to make assumptions about EU-related PNR access and redress requests during the course of its review.

- *Recommendation: CBP should create a means to determine if/how requests for access to or redress involving PNR were received from EU citizens or residents to enable the DHS Privacy Office to better report on categories of people resorting to DHS TRIP.*

- *Accountability/Auditing*

The 2013 CBP PNR Directive specifies procedures regarding access, use, dissemination, and oversight of PNR.

- *Recommendation: Given office restructuring and reorganizing within CBP, the DHS Office of Policy, the DHS Privacy Office, and DHS TRIP, the 2013 CBP PNR Directive should be promptly updated to reflect responsibilities for each office.*
- *Recommendation: To enhance all authorized users' awareness of the responsibilities laid out in the CBP PNR Directive, CBP should redistribute the Directive following its biannual user verification audits to all users.*
- *Recommendation: In conjunction with TECS and NTC privacy training, and before new users are authorized to access PNR, new users should confirm receipt of and be required to read the CBP PNR Directive.*
- *Recommendation: CBP, the Office of Intelligence and Analysis, the Office of the Chief Information Officer, and the DHS Privacy Office should continue to monitor implementation of the Data Framework to ensure PNR retains all protections outlined in the CBP PNR Directive.*

B. Structure of the Review

Beginning in February 2014, the DHS Privacy Office met monthly with a team of DHS officials that included CBP operational and oversight offices to oversee implementation of recommendations from the 2013 review and ensure compliance with the ATS SORN, ATS PIA, and the 2011 Agreement. In February 2015, Chief Privacy Officer Karen Neuman contacted CBP Commissioner R. Gil Kerlikowske to initiate this, the fourth PCR of DHS use and protection of PNR, to outline how the review would be conducted, and to present the criteria that would be used for evaluating compliance with the ATS SORN, ATS PIA, and the 2011 Agreement.

1. The DHS Privacy Office PNR Review Team

The DHS Privacy Office PNR review team was led by Shannon Ballard, Director of International Privacy Programs, with assistance from Kellie Cosgrove Riley, Senior Director for Privacy Policy and Oversight; W. Ken Hunt, Senior Director for Information Sharing, Security, and Safeguarding; Jennifer Murray, Senior Policy Analyst; Kathleen Claffie, former Associate Director Privacy Oversight; Laurence Castelli, Senior Privacy Analyst (Detailee); and Christopher Graff and Margaret Armstrong, Privacy Interns, who provided assistance and guidance. The review team has extensive compliance, privacy policy, legal, and technical expertise.

2. DHS Privacy Office PNR Review

The DHS Privacy Office conducted this PCR of the 2011 Agreement in coordination with CBP leadership and staff for the period of June 1, 2013 – February 1, 2015 (unless otherwise noted). This review consisted of an analysis of existing policies and procedures related to PNR; interviews with key managers, officers, and analysts who handle PNR; and a technical review of CBP systems and documentation. The DHS Privacy Office carried out the following activities:

- Developed and administered a questionnaire for PNR managers and users that included questions on reporting statistics for the review period;
- Reviewed public notices provided to travelers, including the 2012 ATS SORN and ATS PIA, CBP's *Frequently Asked Questions related to PNR*, CBP's PNR Privacy Policy, and *DHS Procedures for Access, Correction or Rectification, and Redress for PNR;*
- Reviewed procedures relating to access, collection, use, sharing, retention, depersonalization, repersonalization, and masking of PNR (including procedures to authorize overrides of the blocking of PNR lacking a U.S. nexus and to authorize access to sensitive data);
- Reviewed select disclosure reports as well as written documentation such as Memoranda of Agreement, Memoranda of Understanding, or other written correspondence that govern the sharing of PNR information with domestic or international partners;

- Reviewed raw PNR collected; case studies falling under each permitted use under Article 4 of the 2011 Agreement; instances of sharing with non-DHS entities; and all redress requests involving PNR;
- Interviewed select authorized non-CBP users of PNR;
- Reviewed documented procedures to conduct searches to respond to FOIA requests for PNR and results of any requests for administrative redress;
- Reviewed internal audit reports and logs;
- Reviewed applicable training materials; and
- Reviewed pertinent technical logs, including records of data repersonalization and data disclosures.

Interviews and consultations included:

- U.S. Customs and Border Protection
    - Office of the Commissioner
    - National Targeting Center (NTC)
    - Privacy and Diversity Office, Office of the Commissioner
    - Office of Field Operations (OFO)
    - Office of Information and Technology (OIT)
    - Customer Service Center (CSC)
    - Office of Internal Affairs
    - Office of Chief Counsel (OCC)
- DHS Policy
    - Threat Prevention and Security Policy, Office of Policy
- Immigration and Customs Enforcement (ICE)
    - Privacy Office
    - Homeland Security Investigations (HSI)
    - Enforcement and Removal Operations (ERO)
- Transportation Security Administration (TSA)
    - Privacy Office
    - DHS Traveler Redress Inquiry Program (DHS TRIP)
- U.S. Citizenship and Immigration Services (USCIS)
    - Privacy Office
    - Fraud Detection and National Security Directorate (FDNS)
- U.S. Coast Guard
    - Privacy Office
- DHS Office of the General Counsel

II. BRIEF HISTORY OF THE PNR AGREEMENT[12]

Pursuant to the Aviation and Transportation Security Act of 2001 (ATSA),[13] CBP processes PNR to vet individuals traveling to and from the United States. In 2003, the European Commission contacted the United States about a potential conflict of laws between ATSA and its implementing regulation and European privacy law. On May 28, 2004, DHS and the European Commission signed an agreement regarding the processing of PNR (2004 Agreement), which followed CBP's issuance of a set of Undertakings[14] setting forth how CBP would process and transfer PNR received in connection with flights between the EU and the United States and the Commission's issuance of an "adequacy finding" concerning such transfers pursuant to the EU Data Protection Directive.[15] As part of the Undertakings, DHS and CBP provided for a Joint Review to take place between the United States and EU to examine CBP's implementation of the Undertakings. The Undertakings also created an additional compliance and complaint resolution role for the DHS Chief Privacy Officer. In September 2005, the DHS Privacy Office completed a review of the PNR program and issued a public report that found the Department was in substantial compliance with the Undertakings and included key areas for improvement.[16]

In May 2006, the European Court of Justice (ECJ) found that the 2004 Agreement had been concluded under inappropriate EU legal authority and was therefore invalid. As a result, DHS and the EU negotiated and concluded an Interim Agreement in October 2006.

In July 2007, DHS and the EU signed a new agreement (2007 Agreement) and exchanged Letters describing commitments made with regard to the use of PNR.[17] The 2007 Agreement required that the parties conduct periodic reviews and a Joint Review took place in the Fall of 2008. In advance of the proposed Joint Review and consistent with its statutory authority, the DHS Privacy Office conducted an assessment of the Department's use of EU PNR and issued a new report with findings that CBP was in compliance with the Privacy Act and the 2007 Agreement and providing additional remediation recommendations (2008 Report).[18]

---

[12] The history of the PNR agreements prior to 2011 is more fully set out in the Privacy Office's 2008 Report at pp. 6-8.

[13] 49 U.S.C.§ 44909(c)(3).

[14] The Undertakings of May 11, 2004 were written commitments made by CBP to the EU concerning PNR information sharing.

[15] 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.

[16] *Privacy Office Report Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union (September 2005).* The report is available at http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacy-pnr-privacyofficefinalreport-september2005.pdf.

[17] *Agreement Between the United States of America and the European Union 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)* July 23, 2007), available at http://www.dhs.gov/sites/default/files/publications/privacy/pnr-2007agreement-usversion.pdf. The Letters are also available on the DHS Privacy Office website at http://www.dhs.gov/sites/default/files/publications/privacy/pnr-2007agreement-usltrtoeu.pdf and http://www.dhs.gov/sites/default/files/publications/privacy/pnr-2007agreement-eultrtous.pdf, respectively.

[18] *Report Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union*, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.

The 2008 Report was published on the DHS website and conveyed to the European Commission; however, the European Commission declined to engage in a Joint Review in 2008. DHS and the European Commission subsequently agreed to hold a Joint Review in February 2010. In advance of that Review, the DHS Privacy Office issued an update to its 2008 Report[19] and found that CBP continued to comply with the 2007 Agreement.

Although the 2007 Agreement provisionally went into force upon signature, it was not ratified by all EU Member States prior to the entry into force of the Lisbon Treaty. The European Parliament informed the European Commission that it would not ratify the 2007 Agreement and instructed the European Commission to seek a new agreement. As a matter of good faith and out of respect for the EU and its evolving political structures following enactment of the Lisbon Treaty, DHS Secretary Janet Napolitano subsequently agreed to negotiate a new agreement, provided the new text would not degrade the operational effectiveness of the 2007 Agreement and would permit necessary additional security enhancements.

The 2011 Agreement was signed on December 14, 2011, and ratified by the European Parliament in April 2012.[20] The 2011 Agreement maintains the integrity of the PNR program while providing enhanced privacy protections for travelers. CBP and the DHS Privacy Office issued an updated SORN and PIA for ATS on May 22, 2012, and June 1, 2012, respectively, to reflect the 2011 Agreement. The DHS Privacy Office review of DHS compliance with the ATS SORN, ATS PIA, and the 2011 Agreement culminated in a report published on July 3, 2013.[21] A joint review with the European Commission was held July 9-10, 2013, which found DHS to be substantially in compliance with the 2011 Agreement.

The DHS Privacy Office has prepared this 2015 Report, consistent with its authorities, to re-assess the Department's compliance with the ATS SORN, ATS PIA, and the 2011 Agreement. A joint review with the European Commission is scheduled for July 1-2, 2015.

[19] *Update to The 2008 Report Concerning Passenger Name Record Information Derived from Flights Between The U.S. and The European Union* (Feb. 5, 2010), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_review2010update_2010-02-05.pdf.

[20] *Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*, available at http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf.

[21] *A Report on the Use and Transfer of Passenger Name Records Between the European Union and the United States, available at* http://www.dhs.gov/sites/default/files/publications/dhs-pnr-privacy-review-20130703.pdf.

III. FINDINGS AND RECOMMENDATIONS

In conducting this review, the DHS Privacy Office used the internationally recognized Fair Information Practice Principles (FIPPs)[22] as the analytical framework for evaluating the Department's compliance with the 2012 ATS SORN and ATS PIA and the 2011 Agreement. The following discussion sets forth the DHS Privacy Office's application of the FIPPs and findings. Each section of this report includes a cross-reference to the sections of the ATS SORN, ATS PIA, and the 2011 Agreement that set out the applicable requirements. Links to these resource documents can be found in Appendix 3.

1. TRANSPARENCY

Requirements

The Privacy Act of 1974, 5 U.S.C. § 552a(e)

2012 ATS PIA: Section 4.0 (Notice)

2011 Agreement: Article 10 (Transparency); Article 23 **(**Review and Evaluation)

Discussion: DHS, and particularly CBP, continue to take steps to increase transparency and raise awareness among the traveling public and the affected air carriers about the 2011 Agreement.

For example, the 2012 ATS SORN and ATS PIA are posted on the DHS website. These documents explain the Department's collection, use, dissemination, and maintenance of personally identifiable information (PII), including PNR, held in ATS and specify the particular criteria for the Department's collection, use, dissemination, and maintenance of PNR, which are in alignment with the 2011 Agreement.

In addition, DHS recently published a PIA related to a specific program that uses PNR. In response to the current foreign fighter threat, DHS will temporarily copy[23] data from DHS databases certified to hold unclassified information to a DHS database certified to hold classified information (known as the DHS Data Framework). The privacy protections for this process are documented in a PIA[24] for the DHS Data Framework – Interim Process to Address an Emergent Threat, which was published on April 15, 2015. (More information on PNR in the Data Framework is discussed in the "Purpose Specification" section of this report.)

---

[22] Privacy Policy Guidance Memorandum Number: 2008-01
http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[23] This interim solution will only continue until the standard model of the Data Framework (http://www.dhs.gov/publication/dhs-all-pia-046-b-dhs-data-framework) is capable of meeting the mission need. DHS remains committed to the standard model of the Data Framework for meeting DHS's mission needs in the long-term, and the Department will revert to the standard model once the technical capabilities are available.

[24] http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-dataframework-april2015.pdf.

Additional documents pertaining to the U.S. – EU PNR agreements can be found under the Privacy Investigations and Reviews[25] section of the DHS Privacy Office website. These include the 2011 Agreement, earlier PNR agreements and related documents, and previous reports by the DHS Privacy Office and the European Commission. Additional information for travelers, including the means to seek access to records or redress, can be found on CBP's public facing website and is provided in the following documents: *DHS Procedures for Access, Correction or Rectification, and Redress for Passenger Name Records,*[26] CBP's Privacy Policy,[27] and PNR Frequently Asked Questions (FAQ)[28] reflecting the 2011 Agreement.

During the review period, CBP continued to promote awareness to affected air carriers of the terms of the 2011 Agreement. For example, during Airlines for America (A4A) and PNRGOV meetings, CPB contacted all air carriers that are required by Article 15 of the 2011 Agreement to push[29] PNR to DHS. During this outreach, CBP offered technical guidance to move to "push," and encouraged carriers to provide information at the time of booking to their passengers regarding the Department's collection and use of PNR. Some airlines have incorporated information about the purpose of the collection, processing, and use of PNR by DHS into its public privacy notices on their websites. These notices also include information about how passengers can request access to or correction of their PNR or redress for an action taken that resulted from use of PNR. It is worth noting that while CBP's PNR regulation does not require air carriers to transmit PNR to DHS via the "push" method, 50 of 54[30] impacted carriers (93 percent) currently do so. This reflects a 25 percent increase since the DHS Privacy Office's 2013 Report.

While the DHS Privacy Office recognizes there is significant information available to the traveling public on DHS public facing websites, easy-to-find information on EU-based websites could increase travelers' awareness on DHS collection and use of PNR and travelers' options for access and redress.

Findings: DHS continues to promote a culture of transparency and awareness about its collection and use of PNR. Public notices that meet the notice requirements of the ATS SORN and ATS PIA and the transparency provisions of the 2011 Agreement are current and posted online. Robust information on DHS compliance with the 2011 Agreement and information on redress for travelers is also readily available online. CBP's engagement with the traveling public and affected airlines should be commended.

Recommendations:

- Due to organizational changes within CBP, public facing documents should be updated with correct addresses and points of contact.

---

[25] http://www.dhs.gov/investigations-reviews.
[26] http://www.cbp.gov/sites/default/files/documents/pnr_access_3.pdf.
[27] http://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf.
[28] http://www.cbp.gov/sites/default/files/documents/pnr_faq_3.pdf.
[29] Airlines are required to acquire the technical ability to push PNR to DHS as opposed to DHS directly pulling PNR from an airline's reservation system.
[30] Current as of May 15, 2015.

- To increase awareness in the EU, CBP and the Office of Policy should work with EU-based U.S. embassies to add additional PNR and redress related information on the travel portion of their websites.
- To increase awareness in the EU, the Office of Policy should provide the European Commission with similar information for Member State distribution.

2. PURPOSE SPECIFICATION

Requirements

2012 ATS SORN: Section on Purposes for PNR in ATS

2012 ATS PIA: Section 3.0 (Uses of Information)

2011 Agreement: Article 2 (Scope); Article 4 (Use of PNR); Article 9 (Non-discrimination)

Discussion: CBP collects PNR pursuant to its statutory authority.[31]

Using the criteria in Article 4 of the 2011 Agreement, the DHS Privacy Office analyzed the reasons that individuals are identified for further scrutiny based in part on their PNR, including for counterterrorism cases and serious transnational crimes. For example, the DHS Privacy Office reviewed cases where PNR was used: (1) to successfully identify potential violent extremists that were referred to law enforcement, (2) where an individual was subject to a "no board" recommendation and did not travel to the U.S., and (3) to identify potential victims of human smuggling.

PNR data is an important tool that CBP's uses to identify high-risk travelers. CBP uses PNR data in conjunction with other information, including current intelligence and law enforcement information to process and evaluate travelers against watchlists and other potential risk indicators all of which make up CBP's larger traveler assessment process. In addition to disclosures for terrorism related cases or active investigations of transnational crimes, CBP shared 21 PNR during the review period with the Centers for Disease Control and Prevention (CDC) to coordinate appropriate responses to health concerns associated with international air transportation, such as those surrounding the Ebola outbreak.

The DHS Privacy Office reviewed the purposes for which authorized DHS individuals used PNR and found these purposes to be consistent with the ATS SORN, ATS PIA, and the 2011 Agreement.

DHS component privacy officers interviewed a random sample of authorized users from each component to determine if their use fell under one of the enumerated purposes in Article 4 of the 2011 Agreement. For example, the Fraud Detection and National Security Directorate of the U.S. Citizenship and Immigration Services use PNR to obtain the travel history of individuals applying for immigration benefits (or their beneficiaries) as part of its counterterrorism efforts or

[31] 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d.

to search for potential indicators of fraud. These uses are consistent with the 2011 Agreement's approved uses of PNR to prevent and combat terrorism and related crimes, and/or to prevent and combat other serious crimes, including serious transnational crimes.

As noted, in response to the current foreign fighter threat, DHS will temporarily copy data from DHS databases certified to hold unclassified information to a DHS database certified to hold classified information. This temporary practice is necessary because important intelligence on about known and suspected terrorists traveling to fight with known terrorist groups cannot be declassified to a level low enough to be stored on DHS's unclassified computers. Therefore, the data, including PNR, was moved to the classified network. The movement of PNR to the classified network does not change the uses of the data or the authorized PNR users. Only users who already have access to PNR on the unclassified network will access PNR on the classified network. These users will be using PNR for the same authorized purposes on both networks. PNR stored in the classified system complies with the terms of the 2011 Agreement.

To ensure that the Department does not use PNR to illegally discriminate against individuals, the DHS Privacy Office participates in quarterly reviews of ATS-P targeting rules with the Office for Civil Rights and Civil Liberties and the Office of the General Counsel. These reviews ensure that the targeting rules are tailored to minimize the impact upon bona fide travelers' civil rights, civil liberties, and privacy, and are in compliance with relevant legal authorities, regulations, and DHS policies. The oversight offices also review these rules to ensure that they are based on current intelligence identifying specific potential threats. The rules are deactivated when no longer necessary to address those threats.

ATS-P is programmed to use flight numbers and airport codes to identify flights with a U.S. nexus, automatically filtering out PNR for travelers whose travel ends before a flight arrives at a U.S. airport. CBP has the authority to require air carriers to provide PNR data with a U.S. nexus, and in some cases, when the U.S. nexus is not apparent in the itinerary.

Designated system users may initiate a manual override function to obtain PNR that has been inadvertently blocked or if the U.S. nexus is not immediately clear and that lack of clarity caused the PNR to not be pushed to DHS. When implementing an override, a warning box appears informing the user that he must provide justification for the request, affirm that he is authorized to access the PNR in question, and that he understands CBP policies regarding the override function.

When a user accesses a PNR that has been identified as a non-U.S. nexus PNR, an email is sent to the ATS-P Mailbox in near real time for management review to determine if there was a U.S.-nexus violation. The mailbox is reviewed routinely by a CBP manager to ensure appropriate use of this function, to identify any misuse of PNR, and to recommend remedial training and/or suspension of system access, as appropriate. Use of the manual override function is audited and its use is tracked for compliance with CBP policy.

During the review period, 290 different users implemented 1,571 overrides with almost all of these overrides ultimately having a U.S. nexus.[32] CBP managers reviewing overrides have found that the overwhelming majority of PNR in question did in fact have a U.S. nexus at some point in the PNR history, as, for example, when a particular flight made an emergency landing at a U.S. airport or stopped to refuel at a U.S. location (but these events were not reflected in the flight itinerary). Between June 1, 2013 and February 1, 2015, there were five warnings issued to authorized users for accessing non-U.S. nexus PNRs. These users operated under the incorrect assumption that they were allowed to access these PNRs. The CBP Manager followed up with the user after the email notification to review the PNR for a possible missed U.S.-nexus, telling the officers they were not authorized to access non-U.S. nexus PNR and reminding them of their obligations pursuant to the CBP Directive. The manager has the authority to revoke the officer's access to ATS-P, if appropriate.

Findings: Based on the foregoing, the DHS Privacy Office finds that the purposes for which the Department uses PNR are compliant with the ATS SORN, ATS PIA, and the 2011 Agreement.

3. USE LIMITATION

Requirements

2012 ATS SORN: Sections on Purposes for PNR in ATS and Routine Uses of Records Maintained in ATS.

2012 ATS PIA: Section 3.0 (Uses of the Information); Section 6.0 (Information Sharing)

2011 Agreement: Article 7 (Automated Individual Decisions); Article 8 (Retention of Data); Article 16 (Domestic Sharing); Article 17 (Onward Transfer); Article 18 (Police, Law Enforcement and Judicial Cooperation)

Discussion: The DHS Privacy Office analyzed the use of PNR to identify individuals who warranted further scrutiny due to the threshold targeting rules in ATS-P. This analysis included a review of the number of enforcement actions, inadmissibility decisions, arrests, referrals to other U.S. law enforcement or security agencies, or identifications of likely ties to organizations or individuals with ties to terrorism that resulted, in part, from an individual's PNR. PNR was also found to be used to eliminate individuals who posed no threat to the homeland. PNR is one element of CBP's evaluation of traveler data to identify high-risk travelers. No decisions concerning travelers are based solely on the automated processing and use of PNR. CBP officers use PNR to assist in determining whether an individual should undergo additional inspection, such as to determine whether the individual should be denied admission into the United States.

The CBP Directive, updated in June 2013, provides a framework for granting access to PNR to authorized personnel within DHS and to DHS's domestic and international mission partners, as appropriate. CBP conducts comprehensive reviews of user accounts within ATS-P. Each user's

[32] 192 overrides were reported from July 1, 2012 – May 1, 2013. DHS believes the increased number of overrides from the 2013 report is due to better accountability, a maturing oversight process, and improvements in RESMON (the reservation system) to prevent users from accessing non-U.S. nexus PNR inappropriately.

level of access is validated biannually by supervisory and management review. The determination of whether a DHS employee requires access or continued access to perform his or her official duties is made by the component or office in which the requesting employee works. The basis for the determination is stated in writing and provided to CBP. The DHS Privacy Office asked component privacy officers to interview a random sample of authorized users from their component to gauge the users' understanding of requirements laid out in the CBP Directive regarding the use of PNR and to review nomination procedures for non-CBP officers to gain access to PNR. The results of these interviews confirmed the employees' "need to know" the information based on their job responsibilities and confirmed their awareness of the CBP Directive and privacy protections surrounding PNR data. In the course of CBP's biannual access validation process, non-CBP users re-receive the CBP Directive and are reminded of their obligations on the use and protection of PNR.

The DHS Privacy Office reviewed biannual reports of CBP's ATS-P User Access Verification audits from April 2013, October 2013, March 2014, and September 2014. These reports demonstrate that CBP continues to make appropriate modifications to access depending on the results of field and headquarters review. Based on the results of these audits, CBP has removed all ATS access and locked the accounts of users whose TECS[33] accounts were found to be in "inactive" status (please see additional information on TECS privacy training under Accountability/Auditing); removed all ATS access from users who resigned, transferred, retired or are deceased; reduced or removed the ATS-P roles of users due to changes in job assignments; and modified and corrected port codes, agency codes, names, job titles, and e-mail addresses as appropriate.

Depersonalization/Repersonalization

Article 8 of the 2011 Agreement addresses Use Limitation, in part, by requiring depersonalization of PNR after six months' retention in the active database. As described below under Data Minimization, CBP demonstrated to the DHS Privacy Office that the process to depersonalize PNR not linked to a law enforcement event works and that any requests to repersonalize PNR is with supervisory approval and only in connection with law enforcement operations that include an identifiable case, threat, or risk, consistent with the CBP Directive. If authorized, the individual user is granted access to depersonalized PNR for 24-hours (however, this PNR remains depersonalized for everyone else). PNR that has been repersonalized is only accessible to that user for 24-hours after which time that user is no longer able to access that repersonalized PNR. If an individual has a need for the repersonalized PNR after 24 hours, he or she must make a new request for the PNR to be repersonalized.

During the course of this review, the DHS Privacy Office found that there may be a high percentage of PNRs that are inaccurately linked to a law enforcement event and therefore not

[33] TECS is both an information-sharing platform that allows users to access different databases that may be maintained on the platform or accessed through the platform and the name of a system of records that includes temporary and permanent enforcement, inspection, and operational records relevant to the anti-terrorism and law enforcement mission of CBP and numerous other federal agencies that it supports. See TECS PIA http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf and SORN http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

depersonalized after six months. CBP is reviewing the process to link PNR to a law enforcement event and assessing its law enforcement functionality and controls.

Using PNR within DHS

CBP acts pursuant to legal authorities[34] and consistent with DHS Policy[35] to grant PNR access to DHS personnel who, in the course of performing their official duties, require such access for the authorized purposes enumerated in the ATS SORN and the 2011 Agreement. CBP receives written confirmation from the DHS component that a DHS employee requires access to PNR to perform his or her official duties and interviews conducted by Component privacy officers confirmed users understand the safeguards surrounding the use of PNR.

The DHS Privacy Office reviewed PNR sharing and use within DHS and confirmed it is on a need-to-know basis and only for purposes specified in Article 4 of the 2011 Agreement.

Sharing PNR Domestically

Consistent with DHS's information sharing mission, information stored in ATS may be shared with appropriate federal, state, or local government agencies. DHS shares information on high-risk travelers of interest who are under investigation for crimes including for terrorism or if the sharing relates to health concerns that could affect vital interests. This sharing is consistent with Article 4 of the 2011 Agreement and only occurs for specific cases after DHS determines that the recipient has a need to know the information to carry out functions consistent with the routine uses set forth in the ATS SORN. CBP personnel must review the request to ensure that the requestor has a law enforcement, public security, or counterterrorism function and the purpose of the request falls within the scope of Article 4 of the 2011 Agreement. The CBP Directive, updated in June 2013, remains in place to ensure the appropriate use, handling, and disclosure of PNR data that is maintained in ATS-P and provides a framework for sharing with DHS's domestic mission partners, as appropriate.

Domestic sharing proceeds according to written confirmation that the recipient will handle the PNR with safeguards equivalent or comparable to those required by the 2011 Agreement and that sharing the PNR is consistent with U.S. law on the exchange of information between domestic government authorities. A completed PNR Disclosure Form identifies the requestor and the purpose for the disclosure request. Any receipt of PNR data is contingent upon an express understanding that the non-DHS authority will treat PNR as sensitive and confidential and will not provide PNR to any other third party without the prior written authorization of DHS. The DHS Privacy Office reviewed select PNR disclosure forms documenting that CBP receives the requisite confirmations.

The DHS Privacy Office reviewed a random sample of PNR disclosure forms that CBP provided to other U.S. government agencies between June 1, 2013 and February 1, 2015. These disclosures were for high-risk travelers of interest who are under investigation for crimes

[34] ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

[35] DHS Information Sharing Strategy https://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf.

consistent with Article 4 of the 2011 Agreement or for terrorism or the sharing related to health concerns that could affect vital interests. For example, CBP shared 21 PNR with the Centers for Disease Control and Prevention (CDC) to coordinate appropriate responses to health concerns associated with international air transportation, such as those surrounding highly infectious diseases including Ebola. The DHS Privacy Office found disclosures outside of DHS to be within the scope of the purposes defined in Article 4 of the 2011 Agreement.

Sharing PNR Internationally

Consistent with DHS's information sharing mission, PNR stored in ATS may be shared with appropriate foreign or international government agencies. This sharing occurs for specific cases and only after DHS determines that the recipient has a need to know the information to carry out functions consistent with the routine uses set forth in the ATS SORN. CBP reviews requests for PNR by non-U.S. authorities to determine whether the intended use is consistent with the purposes identified in the ATS SORN. CBP requires that non-U.S. authorities demonstrate that they can protect the data in a manner consistent with DHS standards and applicable U.S. laws, regulations, and international agreements and arrangements. The non-U.S. authority receiving PNR must affirm that it will treat PNR as sensitive and confidential and will not provide PNR to any other third party without DHS's prior written authorization.

Between June 1, 2013 and February 1, 2015, CBP shared PNR with non-U.S. government entities twice: one for terrorism purposes and one for transnational crime/law enforcement purposes. Neither instance of sharing involved EU PNR. In both instances, the requestor provided justification for their request so CBP could confirm it fell under an allowable use under Article 4 of the 2011 Agreement. In response, CBP provided the recipients with written directions on additional restrictions connected with the recipient's use of PNR and any further sharing of the data. The DHS Privacy Office reviewed each request to disclose PNR and found that in both instances the PNR was shared for an authorized purpose pursuant to written understandings governing the use and protection of the PNR shared.

Although the two instances of international sharing did not include EU PNR and therefore did not call for notification to the appropriate EU authorities as required by the 2011 Agreement, there currently is no final DHS protocol for providing such notification. The DHS Privacy Office reviewed a draft protocol that should be promptly finalized and distributed to all authorized PNR users to clarify the process to share EU PNR with international partners.

Additional sharing with authorized international partners occurs via a CBP Officer posted to Europol Headquarters as a liaison. The officer's role is to exchange law enforcement information with Europol partners, with a focus on disrupting terrorist travel. On a regular basis the liaison officer reviews reports on high risk passengers who were identified through advance targeting, including through PNR. When the liaison officer finds a targeted passenger with a nexus to a Europol member state, he shares the information in the report with the member state's representatives. Since October 2014, the DHS liaison submitted 122 names to Europol of persons suspected of being involved in terrorism.

Findings: The DHS Privacy Office found that CBP's use and sharing of PNR, both domestically and internationally, comply with the ATS SORN, ATS PIA, and the 2011

Agreement. The DHS Privacy Office has determined that the types of records being shared and the purposes for which they are being shared comply with the ATS SORN, ATS PIA, and the 2011 Agreement.

Recommendations:

- While the DHS Privacy Office recognizes that the process to depersonalize PNRs after six months is working effectively, CBP should promptly review its process for linking PNR to a law enforcement event to ensure adherence to the depersonalization requirements of the Agreement.
- CBP and the Office of Policy should finalize the draft protocol to notify EU Member States, as appropriate, of any sharing of EU PNR with third countries.
- CBP, together with the DHS Office of Policy, the CBP Privacy Office, and the DHS Privacy Office, should continue to review existing and future domestic and international information sharing arrangements to ensure that all PNR sharing is in accordance with the ATS SORN, ATS PIA, and the 2011 Agreement. CBP should maintain a repository of such arrangements for easy reference to confirm sharing of PNR is appropriate and protected.

4. DATA MINIMZATION

Requirements

2012 ATS SORN: Section on Categories of Individuals Covered by ATS; Section on Passenger Name Records

2012 ATS PIA: Section 2.0 (Characterization of the Information); Section 5.0 (Data Retention)

2011 Agreement: Article 3 (Provision of PNR); Article 6 (Sensitive Data); Article 8 (Retention of Data)

Discussion: The DHS Privacy Office confirmed that CBP maintains only those data elements outlined in the ATS SORN under "categories of records" and restated in the Annex to the 2011 Agreement. In addition, CBP has demonstrated to the DHS Privacy Office that certain codes and terms that may be in a PNR but that have been identified as "sensitive" are automatically filtered out and blocked by CBP in ATS-P.

Sensitive Data

In exceptional cases, for example, when the life of an individual could be imperiled or seriously impaired, access to sensitive data may be granted. In these exceptional instances, access is tightly controlled and requires supervisory approval by the CBP Deputy Commissioner or designee. Any retrieval of sensitive PNR through ATS-P is recorded by the system and ATS generates a daily email informing CBP management whether or not any sensitive data elements have been accessed.

During the review period, CBP records indicate that no sensitive data was accessed. The DHS Privacy Office reviewed the entire PNR for 10 random individual records from eight randomly

selected dates (total of 80 records) during the review period, searching for sensitive terms and determined that no PNR data elements outside of the 19 allowable PNR types listed in the Annex to the 2011 Agreement were present. The DHS Privacy Office observed markings within the PNR that substituted for sensitive terms, showing blocked data fields where a sensitive term that may have been included in an air carrier's records was hidden from DHS view.

In October 2014, however, CBP's Office of Information and Technology found that users of a DHS mobile application of ATS-P were able to see unblocked sensitive codes and terms in PNR when initiating a query of PNR records linked to persons identified as targets for vetting at Immigration Advisory Program or Joint Security Program locations overseas. Immediate corrective action was taken to filter out sensitive PNR codes and terms from displaying in the mobile application. The DHS Privacy Office reviewed how the mobile application is used by an authorized user at an overseas location and confirmed that the mobile application does not store a copy of the PNR data and notes there is no evidence that sensitive terms played any role in making a passenger referral to an airline.

The process to gain access to sensitive terms remains in place. Users with a Supervisory Access Role can select an ATS user to grant access to sensitive words for a specific case. If selected, a pop-up will appear asking the Supervisor if they have received permission from the Deputy Commissioner to grant/approve access to sensitive information. Once an ATS user has been granted access to sensitive data and views a PNR containing such data, ATS will log the occurrence. A group of CBP managers receive a daily email indicating if a PNR with sensitive data has been accessed. As of March 5, 2015, there were no instances of CBP access to masked sensitive data.

Data Retention

Authorized ATS users have access to PNR in an active database for up to five years. As required by Article 8 of the 2011 Agreement, PNR in the active database and not connected to a law enforcement event is depersonalized after six months. After the initial five-year retention period in the active database, the PNR will be transferred to a dormant database for a period of up to ten years. In 2016, CBP will begin developing protocols for the dormant PNR database, as the first PNR to be moved into dormant status will occur on July 1, 2017.

Depersonalization

To confirm PNR has been depersonalized following its six-month retention, the DHS Privacy Office reviewed both depersonalized records and the process to "repersonalize" consistent with the 2011 Agreement,

The process to depersonalize PNR was updated after the 2013 Joint Review wherein ATS-P is now programmed to automatically depersonalize PNR not connected to a law enforcement event six months from the date of first collection, as opposed to the last load date. The DHS Privacy Office reviewed records older than six months that showed only the record locator, reservation system, date record was created, load and update dates, and the itinerary. An affirmation of depersonalization and the date of depersonalization are also included in the depersonalized record. The DHS Privacy Office reviewed records in the active database stored between June 1, 2013 and February 1, 2015, and confirmed the process to depersonalize PNR not connected to a

law enforcement event occurred. As noted under Use Limitation above, the DHS Privacy Office found that there may be a high percentage of PNRs that are inaccurately linked to a law enforcement event and therefore not depersonalized after six months. CBP is reviewing the process to link PNR to a law enforcement event and assessing its law enforcement functionality and controls.

Repersonalization

If an authorized user believes there is a need to view depersonalized information based on law enforcement operations or in connection with an identifiable case, threat, or risk, that user must obtain prior permission from a supervisor to be granted access to repersonalized PNR. If permission to repersonalize the PNR is granted, the individual user is granted access to depersonalized PNR for 24-hours (however, this PNR remains depersonalized for everyone else). During the review period, there were 3,034 cases where users have accessed and reviewed depersonalized PNR. PNR that has been repersonalized is only accessible for 24-hours after which time that user is no longer able to access that repersonalized PNR. If an authorized user has a need for the repersonalized PNR again after 24-hours, he/she must make a new request for the PNR to be repersonalized. This may be the reason for the increase in cases of represonalization since the last review.

PNRs held in ATS-P are retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008. The retention period for the majority of official records held in ATS and not connected to a law enforcement event does not exceed 15 years, after which time the records are deleted. CBP's data retention procedures vary based upon whether the data was collected under the 2004 Agreement and Undertakings, the 2007 Agreement, or the 2011 Agreement. EU PNR retained and disposed of in accordance with the 2011 Agreement is subject to the additional access restrictions and masking requirements discussed in this report. To confirm PNR held in ATS has been deleted after 10 years, the DHS Privacy Office reviewed results of audits run on ATS searching for PNR not connected to a law enforcement event dating from January 1, 1998 to May 27, 2004, which found no records.

Findings: The DHS Privacy Office finds that DHS and CBP's data minimization processes are compliant with the ATS SORN, ATS PIA, and the 2011 Agreement. The DHS Privacy Office notes CBP's internal auditing mechanisms prevent access to sensitive terms via its mobile application and finds sensitive terms are automatically hidden from DHS view and the process to request access to sensitive terms is in place. The DHS Privacy Office recognizes the three phases of data retention (active/depersonalized/dormant) and found the processes to gain access to PNR in each phase are generally compliant with the ATS SORN, ATS PIA, and the 2011 Agreement. As noted above, however, CBP should review the process that links PNR to a law enforcement event, which impacts the data retention protocols, to ensure PNR is not being kept in the active database longer than necessary.

Recommendation:

- CBP should begin to develop implementing documents for the dormant database in preparation for the July 1, 2017 start date.

5. DATA QUALITY/INTEGRITY

Requirements

2012 ATS SORN: Section on Safeguards

2012 ATS PIA: Section 2.0 (Characterization of the Information)

2011 Agreement: Article 5 (Data Security); Article 15 (Method of PNR Transmission)

Discussion: DHS has a number of physical and procedural safeguards in place to protect personal privacy and the integrity of PNR data, including physical security, access controls, data separation and encryption, audit capabilities, and accountability measures. Records in ATS are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies.[36] Strict controls have been imposed to minimize the risk of compromising the information that is being stored.

CBP receives PNR directly from the travel reservation systems of commercial carriers. DHS recognizes that information provided from commercial sources does not guarantee data accuracy. Therefore, CBP carefully reviews any requests it receives from individuals to correct PNR. CBP has a process in place to update PNR held in ATS if it becomes aware of any inaccuracies due to correction, rectification, or redress procedures available to travelers.

To promote data integrity in ATS, DHS provides individuals with the means to seek access to and correction or rectification of their PNR. During the reporting period, the DHS Traveler Redress Inquiry Program (DHS TRIP) received 31,509 inquiries of which 7,062 applicants checked the "privacy box" in their inquiry and 11 inquiries included references to a traveler's PNR. When DHS receives an application and appropriate documentation that includes references to PNR, DHS TRIP begins to process the request through CBP's TRIP office. None of these 11 inquiries requested modification to or correction of PNR data.

To support the accuracy, timeliness, and completeness of PNR, airlines are required to push PNR to CBP at intervals beginning 96-hours before departure. As noted, currently 50 of 54 (93 percent) air carriers affected by the 2011 Agreement "push" PNR to DHS while CBP uses the "pull" method with four carriers. Carriers pushing PNR to DHS are complying with the technical requirements to do so. CBP has had to "pull" PNRs in instances when no PNRs were loaded from carriers, including "push" carriers. In these cases, the failure to push PNR was due to a flight schedule change, carrier hardware or software issue, or carrier connection issues, thus CBP pulled the information it is legally authorized to collect. In calendar years 2013 and 2014, the number of ad hoc PNR retrievals prior to, between, or after regularly scheduled transmissions amounted to 0.19 percent and 0.34 percent respectively of total PNR received.

Findings: The DHS Privacy Office finds that DHS efforts to ensure data integrity and accuracy comply with the ATS SORN, ATS PIA, and the 2011 Agreement.

[36] At a minimum, DHS Sensitive Systems Policy Directive 4300A: https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

6. INDIVIDUAL PARTICIPATION

Requirements

2012 ATS SORN: Section on Public Record Access/Redress Procedures; Contesting Record Procedures

2012 ATS PIA: Section 7.0 (Redress)

2011 Agreement: Article 11 (Access for Individuals); Article 12 (Correction or Rectification for Individuals); Article 13 (Redress for Individuals)

Discussion: The DHS Privacy Office reviewed the activities of the CBP Customer Service Center, the CBP FOIA/Privacy Act Program, and DHS TRIP. All three programs accept requests for access to PNR or for redress from individuals regardless of their status within the United States. All three programs post information on submitting requests on their websites.[37]

If a passenger has concerns or questions upon entry into or exit from the United States, the first recourse is to speak with a supervisor at the Port of Entry. If the passenger's questions or concerns cannot be addressed at the Port of Entry, the passenger will be given a general fact sheet that directs individuals to contact the CBP Customer Service Center or DHS TRIP. Between June 1, 2013 and February 1, 2015, the CBP Customer Service Center did not receive any questions or complaints related to PNR. In the event of such a request, the Center would direct the requestor to submit a FOIA or Privacy Act request or submit a DHS TRIP inquiry.

Several options are available for individuals seeking correction of PII held by DHS:

- The Freedom of Information Act (FOIA)[38] allows individuals, regardless of citizenship, to request access to their own records held by a U.S. executive branch agency and is enforceable in U.S. federal court. A requester may challenge a refusal to disclose data or a lack of a response to a FOIA request first through an administrative appeals process and then in federal court.
- Under DHS policy,[39] individuals who are not U.S. citizens or lawful permanent residents may request amendment of their records, including PNR, by filing a Privacy Act Amendment Request through the CBP FOIA Headquarters Office. Individuals may contact CBP FOIA Headquarters either online[40] or by mail.[41] An individual may file a

[37] This information is available at http://www.cbp.gov/travel/customer-service/handle-complaints, http://www.cbp.gov/site-policy-notices/foia, and http://www.dhs.gov/dhs-trip respectively.
[38] 5 U.S.C. sect. 552, As Amended.
[39] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf. The policy, referred to as the "mixed systems" policy, gives non-U.S. persons whose data are held in systems that also contain the personal data of U.S. persons the same administrative opportunities to request correction of their data that are available to U.S. persons. The "mixed systems" policy applies to PNR in ATS-P; but it does not extend or create a right of judicial review for non-U.S. persons.
[40] http://www.cbp.gov/site-policy-notices/foia.
[41] CBP FOIA Headquarters Office, U.S. Customs and Border Protection, FOIA Division, 1300 Pennsylvania Avenue, NW, Room 3.3D, Washington, DC 20229, Fax Number: (202) 325-1476.

concern, complaint, or request for correction with regard to accessing his or her PNR by contacting the Assistant Commissioner, CBP Office of Field Operations.[42]

- DHS TRIP provides a means for all individuals, regardless of citizenship, to seek correction of erroneous information that may result in travel screening delays or misidentification. DHS TRIP does not provide individual access to one's records, but rather provides a structured method of review and rectification.
- An individual has the additional option of submitting a request for correction directly to the DHS Chief Privacy Officer via email at privacy@hq.dhs.gov or in writing at: DHS Chief Privacy Officer, Washington, D.C. 20528.

Between June 1, 2013 and May 5, 2015, CBP received 42,028 FOIA requests for "travel records," an almost 150 percent increase from the 2013 report. Of these, there were 342 specific requests for PNR. The DHS Privacy Office reviewed all 342 PNR FOIA requests, and found that of those properly submitted, 24 percent were EU-related.[43] PNR-specific FOIA requests were processed on average within six months, a significant increase from the 2013 Privacy Report. (Note that the increase in FOIA processing time from 2013 is due to the increase in the overall number of FOIA requests CBP receives year after year. CBP policy is to process requests is on a "first in, first out" basis.) The average response time for PNR-specific requests was comparable to the average response time for all CBP FOIA requests.

Any person can file a FOIA request, including U.S. citizens, foreign nationals, organizations, associations, and universities. Records obtainable under the FOIA include all "agency records" that were created or obtained by a Federal agency and are, at the time the request is filed, in that agency's possession and control. Upon receipt of a FOIA request, CBP acknowledges receipt of the request by issuing a letter or email to the requestor. The request is then placed in the queue and will be processed in its turn. Under FOIA and DHS regulation and policies, CBP is allowed to process requests on a first-come, first-served basis, and may also process requests in separate queues depending on their complexity. If CBP has a backlog of requests (which it currently does) the requester may have to wait some time before receiving the requested materials.

Although CBP has not limited disclosure of PNR to requestors seeking access to their own PNR data,[44] it may have to notify requesters that their requests for PNR have been insufficient due to failures to provide required information to process the FOIA request. During the reporting period, there were no inadvertent disclosures to persons other than the requesting individual or a third-party authorized by that individual. Thirty-eight FOIA requests for PNR data were from an authorized third party, but none of the third-party requestors were specified as an EU Member State Data Protection Authority. DHS has not received any requests from individuals to correct or rectify (including the possibility of erasure or blocking) their PNR data.

[42] Assistant Commissioner, CBP Office of Field Operations, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Washington, DC 20229.
[43] The DHS Privacy Office deems a FOIA request to be "EU related" if the requester claims citizenship, a mailing address, or place of birth in the EU.
[44] Under the terms of the System of Records Notice for ATS and the DHS Privacy Policy Guidance Memorandum 2008-01, CBP provides access to all persons requesting their own PNR.

DHS TRIP does not request the citizenship of individuals seeking redress. Therefore, DHS Privacy Office statistics are based on assumptions around information provided by the DHS TRIP filers in its inquiry. Between July 3, 2013 and March 14, 2015, there were a total of 31,509 DHS TRIP inquiries of which 7,062 applicants checked the "privacy box" in their inquiry. During this period, DHS TRIP received 4,933 inquiries from individuals with an identified place of birth in the EU (compared to 5,729 inquiries from those with a place of birth in the United States) including 182 inquiries from individuals with an identified EU address (compared to 1,128 inquiries from those with a U.S. address) for a range of travel related concerns, not specifically PNR. The average time to process any type of DHS TRIP inquiry is 54 days so far in Fiscal Year 2015.

Recommendation: CBP should create a means to determine if/how requests for access to or redress involving PNR were received from EU citizens or residents to enable the DHS Privacy Office to better report on categories of people resorting to DHS TRIP.

Findings: The DHS Privacy Office finds that DHS mechanisms for individuals to obtain appropriate access, correction, and redress comply with the ATS SORN, ATS PIA, and the 2011 Agreement.

7. SECURITY

Requirements

2012 ATS SORN: Section on Safeguards; Section on Storage; and general provisions of the Privacy Act of 1974, 5 U.S.C. § 552a (e)(10)

2012 ATS PIA: Section 8.0 (Auditing and Accountability)

2011 Agreement: Article 5 (Data Security); Article 15 (Method of PNR Transmission)

Discussion: DHS and CBP have authority to seek administrative, civil, or criminal penalties against individuals for unauthorized use or disclosure of PNR and other CBP data. As noted below, all PNR users must undergo privacy training and obtain approval from their supervisor and the ATS system owner before gaining role-based access to ATS. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Notices at sign-on remind users that they are accessing a law enforcement sensitive database for official use only, and that an improper disclosure of PII contained in the system may constitute a violation of the Privacy Act. The notice also states that information contained in the system is subject to the third party rule, meaning that the information may not be disclosed outside DHS without the express permission of CBP.

The CBP Directive remains in place to ensure the appropriate use, handling, and disclosure of PNR data that is maintained in ATS-P. The Directive provides a framework for granting access to PNR to authorized personnel within DHS and to DHS's domestic and international mission partners, as appropriate. Technical and organizational oversight is implemented by user access controls, biannual user access audits, log in and user warning banners, automated email alerts for

overrides or use of sensitive data, automated masking and depersonalization, and data retention limits.

When allegations of TECS/ATS misuse are investigated or as part of other larger investigations where TECS/ATS misuse might have occurred, CBP's Office of Internal Affairs performs audits of ATS use. To guard against the risk of unauthorized access or use of PNR, CBP's Office of Field Operations, along with DHS Component points of contact, verify that users with PNR access are authorized to retain that access. To guard against unintended or inappropriate disclosure of PNR data, the Office of Field Operations conducts audits of all disclosures within and outside of DHS. The CBP Privacy Office oversees the results of these audits and takes appropriate corrective action if warranted.

CBP's Office of Field Operations and Office of Information and Technology are responsible for maintaining updated technical/security procedures by which PNR is accessed by DHS and non-DHS users.

CBP completed a system security plan for ATS and received its Authority to Operate ATS on January 31, 2014. Records in ATS are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. CBP has a number of physical and procedural safeguards to protect personal privacy and ensure data integrity, which include physical security, access controls, data separation and encryption, audit capabilities, and accountability measures. 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.

Between June 1, 2013 – February 1, 2015, the DHS Privacy Office received no reports of the loss or compromise of EU PNR.

Findings: The DHS Privacy Office finds that DHS complies with the ATS SORN, ATS PIA, and the 2011 Agreement and protects PNR through appropriate security safeguards against risk of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. ACCOUNTABILITY/AUDITING

Requirements

2012 ATS SORN: Section on Routine Use

2012 ATS PIA: Section 8.0 (Auditing and Accountability)

2011 Agreement: Article 14 (Oversight)

Discussion: Section 222 of the Homeland Security Act of 2002, as amended, gives the DHS Chief Privacy Officer independent oversight of privacy policy matters and information

disclosure policy within the Department. This includes the authority to investigate and review all programs, such as ATS, and policies for their privacy impact. The DHS Privacy Office conducts ongoing oversight of ATS and has conducted formal reviews of the system many times, including PIA and SORN updates and previous PNR PCRs.[45] CBP has implemented recommendations from previous DHS Privacy Office reviews. During the reporting period, the DHS Privacy Office received no complaints relating to non-compliance with the 2011 Agreement or any complaints regarding misuse of PNR.

CBP's PNR Directive is the core framework for establishing user accountability for protecting PNR data and management responsibilities for access, training and certification, security, disclosures, and corrections and complaints, which is reinforced through field guidance and mandatory training. The Directive provides the framework for auditing and oversight by CBP to ensure privacy-protective measures remain in place. The 2013 CBP Directive ensures that access to, and use and disclosures of, PNR comply with the ATS SORN, ATS PIA, and the 2011 Agreement.

User Awareness

In June 2013, CBP updated its PNR Directive, which together with a management memorandum and field guidance, was distributed to all PNR users. For easy reference, the June 2013 PNR Directive is available under the Help tab in ATS-P and outlines the appropriate use, handling, and disclosure of PNR data and provides a framework for granting access to PNR to authorized personnel within DHS and for sharing PNR with DHS's domestic and international mission partners, as appropriate. As part of the bi-yearly user access verification audits, DHS Component points of contact redistribute the Directive to authorized PNR users within their Component and remind them that the Directive is located in ATS-P under the Help menu.

Auditing Functions

CBP maintains a record of all sharing of PNR within DHS. When a user logs into ATS, notice is provided about the appropriate use of PNR and policies regarding further dissemination of the information outside of the ATS system. Users must affirmatively acknowledge these notices before gaining access to the system.

All disclosures to non-DHS users are recorded by the CBP office sharing the information, in accordance with the CBP Directive. A copy of all requests for PNR from non-DHS users, and the corresponding responses regarding PNR disclosures, are retained by the CBP Privacy Officer for audit purposes. When information is shared externally, an automatically generated notice is sent along with the information to the recipient stating the permissible uses of PNR and the parameters for further disclosure of the information.

As discussed above, the DHS Privacy Office reviewed disclosure documents recording instances of sharing PNR with U.S. domestic partners. For oversight purposes, these records include the name of the CBP action officer and supervisor, the requesting official, the reason for the request and how it complies with DHS/CBP policy and Article 4 of the 2011 Agreement (if applicable), the information disclosed, and how the information was disclosed. Each disclosure includes a notice that PNR information is confidential information (both personal and commercial), that use

[45] See previous PCRs here: http://www.dhs.gov/investigations-reviews.

of this information must meet the purposes defined in Article 4 of the 2011 Agreement, and that the information cannot be released to any third party without CBP's express written consent.

CBP and DHS employ a multi-faceted approach to oversight. CBP's oversight of user access to sensitive data and depersonalized PNR, and to acquiring PNR lacking an obvious U.S. nexus, is detailed above under Data Minimization and Purpose Specification, respectively. The Use Limitation section of this report discusses CBP's process for verifying that user access to PNR is warranted and for withdrawing user access as needed. These reports are also maintained by the CBP Privacy Office for oversight purposes. In addition to these activities, CBP's Office of Field Operations audits the use of ATS-P to guard against unauthorized use and CBP's Office of Internal Affairs audits ATS when allegations of TECS/ATS misuse are investigated, as noted in the Security section above. The CBP Directive and notices within the system define strict disciplinary action in response to unauthorized access or disclosure by DHS personnel that may include termination of employment and/or result in the imposition of criminal sanctions (fines, imprisonment, or both). Unauthorized access to or disclosure of PNR by a non-DHS user will result in revocation of that user's access and may result in criminal sanctions.

Privacy Training

The CBP Directive requires that all users of ATS-P receive training on the use of PNR, including training in privacy, civil rights, and civil liberties protections, in order to have access to that information. Before obtaining access to PNR through ATS-P, CBP employees are first required to meet all privacy and security training requirements necessary to obtain access to TECS. The Privacy and Security Awareness course addresses information integrity, protecting your personal computer, Rules of Behavior, the Privacy Act, the Trade Secrets Act,[46] and how to avoid accidentally giving away sensitive personnel or commercial information. To retain access to TECS (and, thus, ATS), all system users are required to complete this training annually and must answer 90 percent of questions correctly in order to pass an examination. If an individual does not successfully complete the training and examination, he or she loses access to all computer systems, including ATS.

NTC requires additional training that provides greater understanding of the restricted nature of PNR information, particularly EU PNR, and demonstrates how to properly use ATS-P to identify a U.S. nexus. All DHS and non-DHS users with direct access to PNR must certify their receipt of the CBP Directive and their full awareness of its content. Specific topics within the Directive have been shared during monthly Passenger Analysis Unit conference calls and PNR training is also included in threat briefings at specific ports. As noted above, users of ATS-P also have ready access to the Directive via the Help tab in ATS-P.

FOIA Training

As noted in the 2013 PCR, the CBP FOIA Office's *Processing Instructions for PNR* provide staff a comprehensive review of FOIA procedures that includes instructions on conducting searches in ATS in response to FOIA requests for PNR. There are typically four types of FOIA requests received by travelers: all records; entry/exit records; I-94 records; and border crossing/incident records. PNR requests are handled specifically by the NTC, which researches

[46] 18 U.S.C. 1905.

the PNR records and provides them to the CBP FOIA Office due to ATS-P access restrictions. All other requests for traveler data are handled by the CBP FOIA office.

Findings: The DHS Privacy Office finds that DHS has taken steps to ensure accountability for complying with the ATS SORN, ATS PIA, and the 2011 Agreement and has implemented an effective process for auditing access to, and use and disclosure of, PNR. Privacy awareness training is provided to all authorized PNR users and the CBP Directive is readily available as a reference.

Recommendations:

- Given office restructuring and reorganizing within CBP, the DHS Office of Policy, the DHS Privacy Office, and DHS TRIP, the June 2013 PNR Directive should be promptly updated to reflect responsibilities for each office.
- To enhance all authorized users' awareness of the responsibilities laid out in the 2013 PNR Directive, CBP should redistribute the Directive following its biannual user verification audits to all users.
- In conjunction with TECS and NTC privacy training, and before new users are authorized to access PNR, new users should confirm receipt of and be required to read the CBP Directive.
- CBP, the Office of Intelligence and Analysis, the Office of the Chief Information Officer, and the DHS Privacy Office should continue to monitor implementation of the Data Framework to ensure PNR retains all protections outlined in the CBP PNR Directive.

IV. CONCLUSION

Based on the above comprehensive review, the DHS Privacy Office finds that DHS and CBP comply with the ATS SORN, ATS PIA, and the 2011 Agreement.

APPENDIX I: Lifecycle of PNR in CBP Operations

What is PNR?

Anyone traveling on a commercial air carrier can have a reservation known as a 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 the following 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 authorized users 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 identify more effectively individuals or groups related to terrorism or transnational crimes. PNR provides one of the earliest indications that a high-risk individual may be trying to enter or leave the United States. CBP officers in the field[47] and at the 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 may not be sufficiently complete and may contain inaccuracies. PNR data may be used in conjunction with Advance Passenger Information System (APIS) data,[48] 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.

[47] CBP field officers include those at the Passenger Analysis Unit [who conduct local targeting of high-risk travelers for all of CBP's border security missions (including customs, immigration, and agriculture) at the CBP ports of entry], in the Immigration Advisory Program (a partnership between DHS/CBP, foreign governments, and commercial air carriers to identify and prevent high-risk travelers who are likely to be inadmissible into the United States from boarding U.S.-bound flights), and in the Regional Carrier Liaison Group (who work closely with carriers to provide information prior to passenger travel to prevent passengers who may be inadmissible, or who possess fraudulent documents, from traveling to the U.S.).

[48] See APIS PIA and SORN at http://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Lifecycle of PNR

Step 1: CBP's systems are programmed to accept PNR pushed from an air carrier up to 96 hours before a flight's departure and all subsequent changes to the PNR before flight time or to receive pushed updates at scheduled times. If CBP must pull data, it does so no earlier than 96 hours prior to scheduled departure.

Step 2: 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. Sensitive terms and codes are deleted and cannot be re-created after 30 days.

Step 4: After six months, PNR data is depersonalized, and specific fields may only be repersonalized by designated users upon receiving permission from a supervisor through the system. PNR related to a specific enforcement action will not be depersonalized for the life of the enforcement record.

Step 5: At five years from the initial load date 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 6: At 15 years from receipt date/time given in the record, PNR will be fully anonymized without the possibility of repersonalization, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.

APPENDIX II: Roles and Responsibilities for PNR Under the Privacy Act, E-Government Act, and the 2011 U.S. – EU PNR Agreement

A. The DHS Privacy Office

1. The DHS Privacy Office Mission

The mission of the DHS Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities.

2. DHS Privacy Office Responsibilities

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, Karen L. Neuman. The Chief Privacy Officer serves under the authority of the Secretary and Section 222 of the Homeland Security Act of 2002, as amended.[49] 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 and greater coordination with the Inspector General.[50]

The DHS 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 DHS 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 DHS Privacy Office is required to report to Congress on these matters, as well as on complaints about possible privacy violations. Further, the DHS Privacy Office is responsible for privacy-related education and training initiatives for DHS's more than 240,000 employees.

The DHS Privacy Office Privacy Oversight Team was established in February 2012, and the team's objectives were strengthened in the 2015-2018 Strategic Plan. The team is responsible for conducting robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DHS activities.

The DHS Privacy Office contributed a senior member to the U.S. negotiating team for the 2011 Agreement. The role of a U.S. government privacy officer is similar to, but not identical to, the role of European data protection commissioners and officers. The very principles that these officers 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 DHS Privacy Office works to educate, to inform, to create privacy-protective processes, and to mandate attention to privacy and fair information practice principles in new and existing programs, new procedures, new policies, and the hiring

[49] 6 U.S.C. § 142, as amended by the Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53).
[50] *Id.*

and training of new personnel. Externally, the DHS Privacy Office champions DHS programs as appropriate, but criticizes when necessary.

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 bridges the different components of the Department by improving communication among DHS entities, eliminating duplication of effort, and translating policies into timely action.

The Office of Policy also serves as the principal international advisor to the Office of the Secretary and other DHS senior leadership and as such coordinates DHS multilateral and bilateral engagement. It reviews, monitors and, as appropriate, negotiates international agreements and arrangements for consistency with the DHS international engagement plan and strategies.

2. DHS Office of Policy Responsibilities

The Office of Policy contributed two members to the U.S. negotiating team for the 2011 Agreement and supported the Office of the Deputy Secretary in managing the negotiations. It is the primary point of contact for the EU and other stakeholders for strategic and policy questions associated with the 2011 Agreement. It also oversees the development and implementation of PNR, border management, and information sharing policies within DHS to ensure consistency with the 2011 Agreement and other obligations. In this regard it works closely with CBP, the DHS Privacy Office, and the Office of the General Counsel.

C. U.S. Customs and Border Protection

1. CBP Mission

CBP, led by Commissioner R. Gil Kerlikowske, is the unified border agency within DHS. As the single, unified border agency of the United States, including customs, border patrol and inspection, and immigration functions, 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 United States from acts of terrorism and reduce the Nation's vulnerability to the threat of terrorists through a multi-level inspection process.

2. CBP Responsibilities

CBP contributed a senior member to the U.S. negotiating team for the 2011 Agreement. 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, the ATS PIA, and the 2011 Agreement, at a technical and operational level. CBP collects, maintains, uses, and disseminates PNR maintained in ATS-P.

APPENDIX III: Resources

- **2011 PNR Agreement between the U.S. and the European Union, December 14, 2011 (2011 Agreement)**

http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf

- **Automated Targeting System (ATS) System of Records Notice DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297**

http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm

- **Privacy Impact Assessment for the Automated Targeting System DHS/CBP/PIA-006(b) June 1, 2012**

http://www.dhs.gov/publication/automated-targeting-system-ats-update

- **DHS/CBP Procedures for Access, Correction or Rectification, and Redress for Passenger Name Records (PNR)1**

http://www.cbp.gov/sites/default/files/documents/pnr_access_3.pdf

- **DHS/CBP Frequently Asked Questions on the Receipt of Passenger Name Record Information, June 21, 2013**

http://www.cbp.gov/sites/default/files/documents/pnr_faq_3.pdf

- **DHS/CBP Passenger Name Record Privacy Policy, June 21, 2013**

http://www.cbp.gov/sites/default/files/documents/pnr_privacy_3.pdf

- **Past U.S.-EU PNR Joint Review Documentation**

http://www.dhs.gov/investigations-reviews