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

Privacy Office
U.S. Department of Homeland Security

July 3, 2013

LETTER FROM THE DHS ACTING 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 Acting 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, along with that of my staff, to report that with one minor exception as noted below, DHS fully complies 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 identifies 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 Privacy Office during the review, for producing all documents and information requested, and for implementing recommendations from previous Privacy Office reports on the Department's use of PNR. I would like to personally recognize Mr. Thomas Winkowski, Deputy Commissioner of CBP, who is performing the duties of the Commissioner of CBP, for his efforts and partnership.

We look forward to the 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.

Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security

[1] 2011 Agreement, Article 14 (Oversight).

TABLE OF CONTENTS

I. OVERVIEW

II. BRIEF HISTORY OF THE PNR AGREEMENT

III. FINDINGS AND RECOMMENDATIONS

IV. CONCLUSION

APPENDICES

APPENDIX 1: **Lifecycle of PNR in CBP Operations**

APPENDIX 2: **Roles and Responsibilities for PNR under the Privacy Act, E-Government Act, and the 2011 U.S. – EU PNR Agreement**

APPENDIX 3: **2011 PNR Agreement between the U.S. and the European Union, December 14, 2011 (2011 Agreement)**

APPENDIX 4: **Automated Targeting System (ATS) System of Records Notice DHS/CBP-006 May 22, 2012, 77 FR 30297**

APPENDIX 5: **Automated Targeting System (ATS) Privacy Impact Assessment DHS/CBP/PIA-006(b) June 1, 2012**

I. OVERVIEW

The DHS Privacy Office conducted this review 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) and, in particular, U.S. Customs and Border Protection (CBP), is operating in compliance with the standards and representations in the Automated Targeting System (ATS) System of Records Notice[2] (SORN) and Privacy Impact Assessment[3] (PIA), and 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] CBP updated the PIA and SORN for ATS in 2012 to reflect the 2011 Agreement. The Privacy Office's review also measured the Department's implementation of recommendations from the 2008[5] and 2010[6] DHS Privacy Office reports *Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union* (2008 and 2010 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, and 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). 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 because that person may pose a greater risk for terrorism and related crimes or other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature. A select number of other DHS personnel also have access to ATS-P and the PNR held by DHS to fight serious crime and terrorism. The CBP Directive[7] and auditing functions mentioned throughout the report apply to all users of ATS-P.

The Privacy Office reviewed ongoing program policies and practices from July 1, 2012, to May 1, 2013 (unless otherwise indicated), including the details of PNR received and reviewed by DHS and information sharing practices with non-DHS entities. The Privacy Office found those program policies and practices, including how PNR is received, used, and disseminated by CBP, to be generally compliant with the 2011 Agreement and related provisions in the ATS PIA and SORN. During the course of the review, however, the Privacy Office found an instance where the notification to the EU Member States was not taking place after sharing with one of our international partners and has made a recommendation to close this gap in the near term.

The Privacy Office found that steps taken by DHS in response to recommendations in previous Privacy Office reports remain in place. CBP has put in place measures to review user access to PNR, to receive daily alerts regarding any access to sensitive PNR, and to provide managers

---

[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] The CBP PNR Directive outlines the appropriate use, handling, storage, and disclosure of PNR information.

notice of user access to depersonalized data or to PNR lacking a U.S. nexus. CBP is in the process of developing procedures to implement the dormant PNR database required by Article 8 of the 2011 Agreement, and 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 Privacy Office found disclosures of PNR to DHS users, non-DHS users, and foreign authorities to be authorized and compliant with the ATS PIA and SORN, and the 2011 Agreement. CBP 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 April 22, 2013, 68 percent of air carriers[8] affected by the 2011 Agreement (32 of 47) had transitioned to the "push" system, an increase of 20 carriers since the 2010 Privacy Office Report.

A. 2013 Remediation and Recommendations

- *Transparency*

The Privacy Office found that CBP's PNR Frequently Asked Questions (FAQ) and PNR Privacy Policy reflected the 2007 PNR Agreement rather than the 2011 Agreement.

  - *Recommendation: CBP should promptly amend its PNR FAQ and PNR Privacy Policy to provide full transparency.*
  - *Response: CBP has updated the PNR FAQs and PNR Privacy Policy to reflect the 2011 Agreement and the 2012 ATS SORN and PIA, and has posted the new documents to its website at http://www.cbp.gov/xp/cgov/travel/clearing/pnr/.*

- *Use Limitation*

The Privacy Office found that CBP's use and sharing of PNR, both domestically and internationally, is generally compliant with the ATS SORN, ATS PIA, and 2011 Agreement. CBP is assessing whether the current transmission process for a certain international information sharing arrangement is functioning optimally. The Privacy Office has determined that the types of records being shared and the purposes for which they are being shared is compliant with the ATS SORN, ATS PIA, and 2011 Agreements, but that the notification process to EU Member States has not occurred in connection with this one arrangement with our international partner.

  - *Recommendation: CBP should review the process for sharing and the scope of PNR shared with one of its international partners to ensure it is set up optimally.*
  - *Recommendation: Pursuant to existing requirements, CBP should provide the DHS Office of International Affairs (OIA) with notification about disclosures and, in turn, OIA should notify EU Member States, as*

[8] "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.

appropriate, in a timely manner and develop a consistent approach moving forward for notifications.

- *Recommendation: CBP, together with the CBP Privacy Officer and DHS Chief Privacy Officer, should continue to review existing and future information sharing arrangements with non-DHS entities to ensure that PII is protected.*
- *Response: CBP agrees and is reviewing the transmission process for sharing PNR with one of its international partners and will make procedural updates to the program after the assessment is completed. CBP and OIA are working to develop a consistent process for notification to the EU Member States. The assessment, any necessary changes, and the policy with OIA are expected to be completed within 90 days of this report. CBP will work with OIA to notify the EU Member States in a timely fashion, as appropriate.*

- *Individual Participation*

The Privacy Office found an isolated instance in which PII pertaining to a related third party was included in the response to an individual's Freedom of information Act (FOIA) request for his PNR.

- *Recommendation: CBP should take steps to ensure that only PNR pertaining to the individual requesting the information, and no other individual's passenger reservation information, is included in responses to FOIA requests for PII from a PNR.*
- *Response: CBP has instituted an additional supervisory review step to ensure that only the requestor's PNR is included in responses.*

- *Accountability/Auditing*

In 2010, CBP issued a directive (CBP Directive or Directive) and comprehensive field guidance on access, use, and dissemination of PNR, as the Privacy Office recommended in its 2010 Report.

- *Recommendation: CBP should promptly update its Directive and related field guidance to reflect the 2011 Agreement and distribute both documents to all users authorized to access, use, and disseminate PNR, to demonstrate its commitment to accountability for compliance with the 2012 ATS SORN and PIA and the 2011 Agreement.*
- *Response: CBP has finalized the updated Directive reflecting the requirements of the ATS SORN and PIA, and the 2011 Agreement. The Directive is currently available via the Help tab in ATS-P and CBP disseminated it, along with updated field guidance, to all CBP employees and to DHS employees with PNR access.*

The Privacy Office found that DHS has taken significant steps to ensure accountability for complying with the ATS SORN, ATS PIA, and 2011 Agreement; provides appropriate training for authorized users of PNR; and has implemented effective processes for auditing access to, and use and disclosure of, PNR.

- *Recommendation: To enhance accountability and ensure efficient oversight, CBP should consider consolidating the results of its various audits into comprehensive reports for review by the CBP Privacy Office.*
- *Response: CBP agrees.*

B. Structure of the Review

In April 2013, Acting Chief Privacy Officer Jonathan R. Cantor contacted Thomas Winkowski, Deputy Commissioner of CBP, who is performing the duties of the Commissioner of CBP, to initiate this review, to outline how the review would be conducted, and to present the criteria that would be used for measuring compliance with the updated ATS PIA and SORN and 2011 Agreement.

1. The DHS Privacy Office Privacy PNR Review Team

The Privacy Office PNR review team was led by Shannon Ballard, Director of International Privacy Programs, with assistance from Martha Landesberg, Senior Director Privacy Oversight; Rebecca Richards, Senior Director Compliance; James Holzer, Senior Director, FOIA Operations; Kellie Riley, Attorney Advisor; Kathleen Claffie, Associate Director Privacy Oversight; Nicole Sanchez, International Privacy Analyst; Jimmy Wolfrey, FOIA Program Specialist; and Liz Lyons, Compliance Specialist, who provided assistance and guidance. The review team has extensive compliance, privacy policy, legal, and technical expertise.

2. DHS Privacy Office PNR Review

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 Privacy Office reviewed the following materials:

- Public notices provided to travelers, including the 2012 ATS SORN and PIA, CBP's *Frequently Asked Questions related to PNR*, CBP's PNR Privacy Policy,[9] and *DHS Procedures for Access, Correction, or Rectification, and Redress for PNR;*[10]
- Documented 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), as well as Memoranda of Agreement /Memoranda of Understanding governing the sharing of PNR information with domestic or international partners;
- Documented procedures to conduct searches to respond to FOIA requests for PNR;
- Internal audit reports and logs;
- Training materials; and

[9] The 2013 FAQ and Privacy Policy are available at http://www.cbp.gov/xp/cgov/travel/clearing/pnr/.
[10] http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_DHS%20Procedures%20for%20PNR%20Access%20Correction%20and%20Redress%20FINAL%2020120727%20docx.pdf

- Pertinent technical logs, including records of data repersonalization and data disclosures.

Interviews and consultations included:

- U.S. Customs and Border Protection
  - National Targeting Center (NTC)
  - Office of Diversity and Civil Rights, Office of Privacy
  - Office of Information and Technology (OIT)
  - Office of Intelligence and Investigative Liaison (OIIL)
  - Customer Service Center (CSC)
  - Office of Regulations and Rulings (OR&R)
  - Office of Chief Counsel (OCC)
  - Office of Field Operations (OFO)
- DHS Policy
  - Office of Policy
  - Office of International Affairs
- Immigration and Customs Enforcement (ICE)
  - Office of Homeland Security Investigations (HSI)
- U.S. Citizenship and Immigration Services (USCIS)
  - Fraud Detection and National Security Directorate (FDNS)
- DHS Office of the General Counsel
- DHS Traveler Redress Inquiry Program (DHS TRIP)

II. BRIEF HISTORY OF THE PNR AGREEMENT[11]

CBP processes passenger name records (PNR) for purposes of screening individuals traveling to and from the United States pursuant to the relevant section of the Aviation and Transportation Security Act of 2001 (ATSA).[12] 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 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.[13] 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 a 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

[11] The history of the Agreement prior to 2011 is more fully set out in the Privacy Office's 2008 Report at pp. 6-8.
[12] 49 U.S.C.§ 44909(c)(3).
[13] 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.

and issued a public report finding that the Department was in substantial compliance with the Undertakings and including key areas for improvement.[14]

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.[15] The 2007 Agreement required that the parties conduct periodic reviews, and a Joint Review was to take 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 finding CBP to be in compliance with the Privacy Act and the 2007 Agreement and providing additional remediation recommendations (2008 Report).[16]

The 2008 Report was published on the DHS website and conveyed to the Commission; however, the Commission declined to engage in a Joint Review in 2008. DHS and the 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[17] and found that CBP continued to comply with the 2007 Agreement.

Although the 2007 PNR 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 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 additional security enhancements where necessary.

The 2011 U.S.-EU PNR Agreement (2011 Agreement) was signed on December 14, 2011, and ratified by the European Parliament in April 2012.[18] The 2011 Agreement maintains the

---

[14] *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.

[15] *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.

[16] *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.

[17] *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.

[18] *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

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 has prepared this 2013 Report, consistent with its authorities, to re-assess the Department's compliance with the ATS SORN and PIA and to assess its compliance with the 2011 Agreement.

IV. FINDINGS and RECOMMENDATIONS

In conducting this review, the Privacy Office has used the internationally recognized Fair Information Practice Principles (FIPPs) as the analytical framework for measuring the Department's compliance with the 2012 ATS SORN and PIA and the 2011 Agreement. The discussion that follows sets forth the Privacy Office's findings as they relate to each of the FIPPs. Each section of the discussion includes a cross-reference to the sections of the ATS PIA and SORN and the 2011 Agreement that set out the applicable requirements. All of these documents are included as appendices to this Report.

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, has taken numerous steps to raise awareness among the traveling public and the affected air carriers regarding the 2011 Agreement.

CBP updated the ATS PIA and ATS SORN in 2012 and posted them on the DHS website. These documents address the Department's collection, use, dissemination, and maintenance of 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.

Additional documents pertaining to the U.S. – EU PNR Agreements can be found under the Reports[19] section of the Privacy Office website. These include the 2011 Agreement; *DHS Procedures for Access, Correction or Rectification, and Redress for Passenger Name Records*; earlier PNR Agreements and related documents, and previous reports by the Privacy Office and the European Commission. CBP's Privacy Policy and Frequently Asked Questions (FAQ) reflecting previous U.S. – EU PNR Agreements have been posted on its website since 2010. Updated PNR FAQs and Privacy Policy to reflect the 2011 Agreement can be found at http://www.cbp.gov/xp/cgov/travel/clearing/pnr/.

---

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

[19] http://www.dhs.gov/privacy-foia-reports#5

Since the 2011 Agreement entered into force, CBP has also promoted awareness by reaching out, via email and telephone, to all air carriers that are required by Article 15 of the Agreement to change from PNR "pull" to PNR "push." CBP also hosted a conference call with the trade group Airlines for America, to discuss the 2011 Agreement and its impact on carriers. During this outreach, CBP explained significant changes from the previous Agreements, offered technical guidance to move to "push," and encouraged carriers to provide information to their passengers regarding the Department's collection and use of PNR. This guidance highlighted four primary provisions that directly impact air carriers covered by the Agreement:

- the time intervals for PNR transfer;
- the requirement to move to PNR "push;"
- the need to provide passengers with information on DHS's collection, processing, and use of PNR; and
- information on 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 DHS does not have the authority to require air carriers to transmit PNR to DHS via the "push" method, 32 of 47 impacted carriers (68%) currently do so. This reflects an increase of 20 carriers since the Privacy Office's 2010 Report.

Findings: DHS continues to promote a culture of transparency and awareness regarding its collection and use of PNR. CBP has updated its public notices to meet the notice requirements of the ATS SORN and PIA and the transparency provisions of the 2011 Agreement, and will be fully compliant when the updated documents are posted publicly. The Privacy Office expects the documents to be posted promptly.

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.[20]

Using the criteria in Article 4 of the 2011 Agreement, the Privacy Office analyzed the reasons that individuals are identified for further scrutiny based in part on their PNR. Between July 1, 2012 and April 30, 2013, 0.002 percent of individuals traveling to the U.S. were identified by ATS for additional attention based primarily on analysis of their PNR. These individuals were identified during an investigation related to terrorism or other serious crime as defined in Article

[20] 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d

4 of the 2011 Agreement. CBP documented that during the same time period sharing of PNR was for purposes related to terrorism or law enforcement investigations, including investigations of serious crimes, which are transnational in nature.

The Privacy Office also reviewed the purposes for which DHS personnel who have access to ATS-P used PNR and found these to be consistent with the ATS SORN and PIA and the 2011 Agreement. For example, ICE HSI uses PNR to investigate terrorism related cases and serious transnational crime, primarily pursuant to the Immigration and Naturalization Act. [21]

To ensure that the Department does not use PNR to discriminate against individuals, the Privacy Office (together with representatives of the Office for Civil Rights and Civil Liberties, the Office of the General Counsel, and relevant program staff) conducts quarterly reviews to oversee implementation of ATS and to assess whether privacy and civil liberties protections are adequate and consistently implemented. All travel targeting scenarios, analysis, and rules are reviewed to ensure that they are appropriately 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 Privacy Office interviewed NTC staff and saw live demonstrations of how CBP has programmed ATS-P to use flight numbers and airport codes to identify flights with a U.S. nexus. The system filters out PNR for travelers whose journey 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. If a designated system user seeks to implement an override to access PNR without a clear U.S. nexus, a warning box appears informing him 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. The following day, an email notice is sent to a group of managers 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.

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, 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 was not reflected in the flight itinerary). If a manager is not able to independently verify from a review of available CBP data sets that a U.S. nexus override is justified, he or she contacts the officer who implemented the override for further clarification. If the manager is not satisfied with the officer's rationale for the override, the manager has the authority to revoke the officer's access to ATS-P, if appropriate. Between July 1, 2012 and May 15, 2013, CBP officers implemented 192 overrides, including three cases in which managers were not able to readily determine the justification for the override. In each of these cases, managers sought clarification from the officers and found, after careful review of the officer's explanation, that each override was justified and each officer involved received a reminder of the policy on PNR access and usage.

[21] 8 U.S.C. Chapter 12

Findings: Based on the foregoing, the 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: CBP provided the Privacy Office statistics on its use of PNR leading to 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. The CBP Directive requires that no decisions concerning travelers are to be 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 or be allowed or denied admission into the United States.

CBP conducts comprehensive verification of user accounts within ATS-P. Each user's level of access is validated twice a year by supervisory and management review. This process includes seeking supervisors' verification that users have continued need for access. The Privacy Office reviewed biannual reports of CBP's ATS-P User Access Verification audits from July 2010 to September 2012, demonstrating that CBP has modified user access to ATS-P, adjusted user roles, and even withdrawn user access completely, as appropriate, depending on the results of field and headquarters review. During interviews at the NTC, CBP's Office of Information Technology and Office of Intelligence and Investigative Liaison demonstrated that the audits not only improved operational efficiency, but improved compliance with use limitations pursuant to the ATS PIA and SORN and the 2011 Agreement by limiting user access.

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 Privacy Office that any use of repersonalized 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.

<u>Sharing PNR within DHS:</u> Pursuant to legal authorities[22] and consistent with the DHS Policy for Internal Information Exchange and Sharing, CBP grants PNR access to DHS personnel who, in

[22] 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

the course of performing their official duties, require such access for the authorized purposes enumerated in the ATS SORN and the 2011 Agreement. This access is granted while securing PNR and ATS-P, safeguarding the privacy of persons to whom the records pertain, and ensuring compliance with all applicable laws, regulations, DHS policies, and international agreements and arrangements. CBP receives written confirmation from the DHS component that a DHS employee requires access to PNR to perform his or her official duties.

The Privacy Office reviewed PNR sharing and use within DHS and confirmed it is on a need-to-know basis and for purposes specified in Article 4 of the 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. This sharing only takes place 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. This 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. 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 a sample of PNR disclosure forms documenting that CBP receives the requisite confirmations.

The Privacy Office reviewed a random sample of 13 disclosures of PNR that CBP provided to other U.S. government agencies between July 1, 2012, and March 31, 2013. In addition to disclosures for terrorism related cases or active investigations of transnational crimes, CBP shared seven PNR with the Center for Disease Control (CDC) to coordinate appropriate responses to health concerns associated with international air transportation. The 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 takes place 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 by non-U.S. authorities for PNR, determines whether the intended use is consistent with the purposes identified in the ATS SORN, and also 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 data must enter into an express understanding with DHS 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. The Privacy Office, together with CBP, reviews each international access arrangement to ensure that the terms are observed and that continued sharing of PNR with a non-U.S. user is appropriate.

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).

Between July 1, 2012, and March 31, 2013, CBP shared PNR on a case-by-case basis with non-U.S. government entities twice. In both instances the recipients were provided with written directions on additional restrictions connected with the recipient's use of PNR and any further sharing of the data. In one case, CBP shared EU PNR with the relevant EU Member State. In the second case, CBP shared PNR with a non-EU international partner, and the PNR involved was not EU PNR. The Privacy Office reviewed these cases and found that in both instances the PNR was shared for an authorized purpose and pursuant to an agreement or arrangement that included specific language governing the use and protection of the PNR shared. Pursuant to an existing arrangement, CBP has also shared EU PNR with one international partner. As it pertains to PNR, this information sharing arrangement has been in place since 2006 and was updated in 2009 and is designed to ensure that only PNR records with a nexus to terrorism or serious transnational crime are transmitted. As a result of the Privacy Office review, DHS continues to assess whether the current transmission process is functioning optimally. For this specific international arrangement, DHS found that notification to Member States was not provided. Other DHS components authorized to use PNR have not disclosed PNR information to a third country.

Findings: The Privacy Office found that CBP's use and sharing of PNR, both domestically and internationally, is generally compliant with the ATS SORN, ATS PIA, and 2011 Agreement. CBP is assessing whether the current transmission process for a certain international information sharing arrangement is functioning optimally. The Privacy Office has determined that the types of records being shared and the purposes for which they are being shared is compliant with the ATS SORN, ATS PIA, and 2011 Agreement, but that the notification process to EU Member States has not occurred in connection with this one arrangement with our international partner.

Recommendation: CBP should review the process for sharing and the scope of PNR shared with one of its international partners to ensure it is set up optimally. Pursuant to existing requirements, CBP should provide the DHS Office of International Affairs (OIA) with notification about disclosures and, in turn, OIA should notify EU Member States, as appropriate, in a timely manner and develop a consistent approach moving forward for notifications. CBP, together with the CBP Privacy Officer and DHS Chief Privacy Officer, should continue to review existing and future information sharing arrangements with non-DHS entities to ensure that PII is 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 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. As demonstrated to the Privacy Office, certain codes and terms that may appear in a PNR have been identified as "sensitive" and are masked by ATS-P to prevent routine viewing. In exceptional cases, for example, when the life of an individual could be imperiled or seriously impaired, access to sensitive data may be granted but 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.

Based on analysis of these daily email notifications and a review of randomly selected PNR, the Privacy Office determined that no PNR data outside of the 19 PNR types listed in the Annex to the 2011 Agreement was received. Within the 19 PNR data elements, the Privacy Office observed that sensitive terms were appropriately masked.

As of March 31, 2013, there have been three instances of CBP access to masked sensitive data, all for the sole purpose of testing the email notification functionality. The Privacy Office reviewed samples of raw PNR from seven randomly-selected dates to verify that ATS automatically filters out sensitive PNR codes and terms. Each PNR showed blocked data fields where a sensitive term that may have been included in an air carrier's records was hidden from DHS view.

Authorized ATS users have access to PNR in an active database for up to five years. PNR in the active database 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. CBP is developing a process to move PNR after five years to the dormant database, which will be operational by July 1, 2017, as the 2011 Agreement requires.

To confirm PNR has been depersonalized following its six-month retention as required by Article 8 of the 2011 Agreement, the Privacy Office reviewed depersonalized records and the process to "repersonalize" those records based on an approved purpose. ATS-P is programmed to automatically depersonalize PNR six months from its last receipt. Records older than six months reviewed by the Privacy Office 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 Privacy Office reviewed records in the active database stored between July 1 and September 1, 2012, and confirmed that they are being depersonalized.

If an authorized user believes there is a need for 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 repersonalize that PNR. If permission to repersonalize the PNR is granted, the user has access to the repersonalized data for no more than 24 hours per authorization. As of May 1, 2013, 29 PNR had been repersonalized.

PNR 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 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.

Findings: The Privacy Office finds that DHS and CBP's data minimization and retention processes are compliant with the ATS SORN, ATS PIA, and the 2011 Agreement.

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: As discussed elsewhere in this report, DHS 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. In seeking accurate data, CBP obtains PNR directly from travel reservation systems of commercial carriers. DHS recognizes that information provided from commercial sources does not guarantee data accuracy, however. If CBP becomes aware of inaccuracies of PNR due to correction, rectification, or redress procedures available to travelers, ATS updates this information immediately.

To promote data integrity in PNR, DHS provides individuals with the means to seek correction or rectification of their PNR. DHS has not yet received a request to correct or rectify a traveler's PNR. As discussed below under Individual Participation, the Department promotes several options for filing such requests.

CBP continues to operate using the 72-hour interval for providing PNR to DHS stipulated in the 2007 Agreement, and has not begun to require air carriers to "push" PNR to DHS 96 hours prior to a flight's departure. As noted above, currently 32 of 47 air carriers affected by the 2011 Agreement (68%) "push" PNR to DHS and CBP uses the "pull" method for 15 carriers. Carriers pushing PNR to DHS are complying with the technical requirements to do so. CBP is currently notifying "push" carriers of the time change to 96 hours and is working to implement this change.

On a case-by-case basis, DHS has required air carriers to provide PNR between or after regular transfers due to operational needs or due to technical issues, such as when a carrier fails to push the data to CBP due to a carrier outage. In the case of a technical issue, CBP pulls the

information it is legally authorized to collect. In 2012, the number of PNR retrievals prior to, between, or after regularly scheduled transmissions amounted to 0.3 percent of total PNR received. In addition, on one occasion, CBP requested one retransmission of data not provided timely by an EU-based service provider.

Findings: The Privacy Office finds that DHS efforts to ensure data integrity and accuracy generally comply with the ATS SORN, ATS PIA, and the 2011 Agreement. CBP is working toward full implementation of the 96-hour interval for receipt of PNR from affected airlines and, as noted earlier in this report, continues to encourage affected airlines to "push" PNR to DHS.

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 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.[23]

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 Customer Service Center or DHS TRIP. Between July 1, 2012, and March 31, 2013, the CBP Customer Service Center did not receive requests related specifically to PNR information. In the event of such a request, the Center would direct the requestor to submit a FOIA or Privacy Act request.

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

- FOIA 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,[24] individuals who are not U.S. citizens or lawful permanent residents may request amendment of their records, including PNR, by filing a Privacy Act

[23] This information is available at http://www.cbp.gov/xp/cgov/travel/customerservice/, https://foia.cbp.gov/palMain.aspx, and http://www.dhs.gov/dhs-trip respectively.
[24] 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

Amendment Request through the CBP FOIA Headquarters Office. Individuals may contact CBP FOIA Headquarters either online[25] or by mail.[26] An individual may file a concern, complaint, or request for correction with regard to accessing his or her PNR by contacting the Assistant Commissioner, CBP Office of Field Operations.[27]

- DHS TRIP provides a means for all individuals, regardless of citizenship, to apply for redress—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 July 1, 2012, and March 31, 2013, CBP received a total of 21,606 FOIA requests. 16,875 of these requests were for "traveler" data, including 27 specific requests for PNR. PNR-specific FOIA requests were processed on average within 38 days – a significant improvement since the 2008 Privacy Report, when some requests for PNR took more than one year to process. The average response time for PNR-specific requests was comparable to the average response time for all CBP FOIA requests.

In response to the Privacy Office's 2008 and 2010 Privacy Report recommendations, CBP developed *Processing Instructions for PNR*, a comprehensive review of FOIA procedures that includes instructions on conducting searches in ATS in response to FOIA requests for PNR. The Privacy Office reviewed these standard operating procedures, together with responses to all PNR FOIA requests from July 1, 2012, to March 31, 2013, and found that none were EU-related[28] and that all responses were provided to first party requestors (this includes the individual, his or her documented representative, or his or her legal guardian). The Privacy Office found one instance in which third-party PII was released to a requestor. As a result, a new supervisory review process has been implemented to double check all responses prior to release. The PNR FOIA responses were comprehensive and consistent in terms of the information provided. The Privacy Office found that there were no instances of refusal or restriction of access to PNR in response to any FOIA requests. DHS has not received any requests from individuals to correct or rectify (including the possibility of erasure or blocking) their PNR data.

The Privacy Office reviewed statistics related to DHS TRIP inquiries from July 1, 2012 – March 31, 2013, and found that of the over 13,000 inquiries, only two were specifically related to PNR and neither involved inquires from individuals from the EU. The Privacy Office also reviewed DHS TRIP redress applications from individuals who either live in an EU Member State or have a passport from an EU Member State and who raised a potential privacy issue. None of these

---

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.

[25] https://foia.cbp.gov/palMain.aspx

[26] CBP FOIA Headquarters Office, U.S. Customs and Border Protection, FOIA Division, 90 K Street NE, 9th Floor, Washington, DC 20002, Fax Number: (202) 325-0230.

[27] U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Washington, DC 20229.

[28] CBP deems a FOIA request to be "EU related" if the requester claims citizenship, a mailing address, or place of birth in the EU.

individuals alleged that their PNR data was misused. The average processing time for DHS TRIP requests of EU origin was comparable to the average processing time for all DHS TRIP requests.

Findings: The Privacy Office finds that DHS has effectively implemented recommendations from the 2008 and 2010 Privacy Office Reports to improve the efficiency and effectiveness of its responses to requests for PNR under FOIA. We commend the CBP FOIA Office for developing standard operating procedures for processing these FOIA requests, for updating *DHS Procedures for Access, Correction or Rectification, and Redress for PNR*, and for significantly improving the processing time for these FOIA requests. The Privacy Office finds that DHS mechanisms for obtaining appropriate access, correction, and redress comply with the ATS SORN, the ATS PIA, and the 2011 Agreement.

7. SECURITY

Requirements

2012 ATS SORN: Section on Safeguards; Section on Routine Use A and B, 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 and may not be disclosed outside DHS without the express permission of CBP.

As discussed in further detail below, layers of oversight ensure compliance with data security requirements. To guard against the risk of unauthorized access or use of PNR, CBP's Office of Internal Affairs audits the use of ATS and the CBP Office of Intelligence and Investigation Liaison (OIIL) verifies that users with PNR access are authorized to retain that access. To guard against unintended or inappropriate disclosure of PNR data, OIIL 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.

OIIL, in coordination with CBP's Office of Field Operations (OFO) and Office of Information and Technology (OIT), is responsible for maintaining updated technical/security procedures by which PNR is accessed by DHS and Non-DHS Users. CBP completed a security plan for ATS and in 2011 received its certification and accreditation (C&A) under the Federal Information

Security Management Act (FISMA) and Authority to Operate ATS for three years. 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 July 1, 2012 and March 31, 2013, the Privacy Office received no reports of the loss or compromise of EU PNR.

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

8. ACCOUNTABILITY/AUDITING

Requirements

2012 ATS SORN: Section on Use and Control

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, including the authority to investigate and review all programs, such as ATS, and policies for their privacy impact. The 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 Reports. CBP has implemented recommendations from previous 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 Directive is the core framework for establishing user accountability for protecting PNR data, and 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. As recently updated, the CBP Directive ensures that access to, and use and disclosures of, PNR comply with the ATS PIA, ATS SORN, and the 2011 Agreement.

<u>User Awareness:</u> CBP first issued its Directive in 2010 and distributed it to all PNR users together with a management memorandum and additional field guidance. An updated Directive reflecting the 2011 Agreement is currently 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. The updated Directive has been distributed throughout CBP and to other DHS PNR users with updated field guidance.

Auditing Functions: CBP maintains a record of all sharing of PNR within DHS. When a user logs into ATS, notice is provided on the appropriate use of PNR and policies regarding further dissemination of the information outside of the ATS 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, a notice to the recipient is automatically generated by ATS stating the permissible uses of PNR and the parameters for further disclosure of the information. As discussed above, the Privacy Office reviewed 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 of this information must meet the purposes defined in Article 4 of the Agreement, and that the information cannot be released to any third party without CBP's express written consent.

CBP employs 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. In addition to these activities, CBP's Office of Internal Affairs audits the use of ATS-P to guard against unauthorized use, and the CBP Privacy Office maintains a record of access determinations for oversight purposes. The CBP Directive defines 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. In order to obtain access to PNR through ATS-P, CBP employees are required to meet all privacy and security training requirements necessary to obtain access to TECS.[29] To retain access to TECS (and, thus, ATS), all system users are required to complete annual training in privacy awareness and must pass an examination. If an individual does not successfully complete the training, he or she loses access to all computer systems, including ATS.

[29] 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.

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. To reinforce the requirements of the 2011 Agreement and CBP policy with respect to PNR, the updated CBP Directive, together with additional guidance, was distributed to all CBP personnel in the field and to other DHS PNR users. 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 above, CBP's FOIA Office created new *Processing Instructions for PNR* to provide staff a comprehensive review of FOIA procedures that includes instructions on conducting searches in ATS in response to FOIA requests for PNR.

Findings: The Privacy Office finds that DHS has taken steps to ensure accountability for complying with the ATS SORN, ATS PIA, and 2011 Agreement, provides appropriate training for authorized users of PNR, and has implemented an effective process for auditing access to, and use and disclosure of, PNR.

Recommendation: To enhance accountability and ensure efficient oversight, CBP should consider consolidating the results of its various audits into one report for review by the CBP Privacy Office.

V. Conclusion

Based on the above comprehensive review, the Privacy Office finds that with one minor exception DHS and CBP are in compliance with the ATS PIA, the ATS SORN, and the 2011 Agreement.

APPENDIX 1: 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 three primary sections: Active Portion, which contains the name(s) of the passenger(s); the itinerary; Supplemental Information (such as baggage, frequent flier information, special requests, or other information related to the reservation); and Historical Portion, which contains changes made to the active component. When CBP receives PNR from an air carrier it may have all this information or, more likely, it will have some portions of this information. CBP takes the PNR in unformatted form and parses it so that no matter which air carrier system is involved, the PNR is displayed in a common format for CBP Officers who are reviewing it to identify high-risk passengers.

CBP uses PNR related to flights between the U.S. and EU, as in other regions of the world, to facilitate legitimate travel into and out of the United States and to 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[30] 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,[31] 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.

[30] 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.).

[31] 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 after the end of travel specified in the itinerary of the PNR, the PNR data will be moved to a dormant, non-operational status, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.

Step 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 2: 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 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 Acting Chief Privacy Officer, Jonathan R. Cantor. The Chief Privacy Officer serves under the authority of the Secretary and Section 222 of the Homeland Security Act of 2002, as amended.[32] 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.[33]

The Privacy Office has programmatic responsibilities for the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act, and the numerous laws, Executive Orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personally identifiable and Departmental information.

The Privacy Office has oversight of privacy policy matters and information disclosure policy. It is also statutorily required to evaluate all new technologies used by the Department for their impact on personal privacy. The Privacy Office is required to report to Congress on these matters, as well as on complaints about possible privacy violations. Further, the Privacy Office is responsible for privacy-related education and training initiatives for DHS's more than 240,000 employees.

The DHS Privacy Office established its new Privacy Oversight Team in February 2012, as an outgrowth of the Office's 2012–2015 Strategic Plan. The Privacy Oversight Team includes several pre-existing Office functions that logically follow from the Office's core responsibility to ensure that Department programs and systems comply with DHS privacy policy: compliance reviews, privacy investigations, privacy incident response, and privacy complaint handling and redress. Bringing together these complementary functions has strengthened the Office's oversight role throughout DHS.

The 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

[32] 6 U.S.C. § 142, as amended by the Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53).
[33] *Id*.

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 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 and training of new personnel. Externally, the 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.

2. DHS Office of Policy Responsibilities

The Office of Policy contributed a senior member to the U.S. negotiating team for the 2011 Agreement. In fulfilling this responsibility, the Office of Policy identified and ensured consistency between DHS's operational, policy, and legal requirements, including those associated with information sharing, data management, and privacy.

C. DHS Office of International Affairs

1. DHS International Affairs Mission

The Office of International Affairs 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 International Affairs Responsibilities

The Office of International Affairs contributed a member 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 Privacy Office, and the Office of the General Counsel.

D. U.S. Customs and Border Protection

1. CBP Mission

CBP, headed by the Deputy Commissioner of CBP performing the duties of the Commissioner of CBP, Thomas S. Winkowski, 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 3: 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

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

THE UNITED STATES OF AMERICA,

hereinafter referred to also as "the United States", and

THE EUROPEAN UNION,

hereinafter referred to also as "the EU",

together hereinafter referred to as "the Parties",

DESIRING to prevent and combat terrorism and serious transnational crime effectively as a means of protecting their respective democratic societies and common values;

SEEKING to enhance and encourage cooperation between the Parties in the spirit of transatlantic partnership;

RECOGNIZING the right and responsibility of states to ensure the security of their citizens and protect their borders and mindful of the responsibility of all nations to protect the life and safety of the public including those using international transportation systems;

CONVINCED that information sharing is an essential component in the fight against terrorism and serious transnational crime and that in this context, the processing and use of Passenger Name Records (PNR) is a necessary tool that gives information that cannot be obtained by other means;

DETERMINED to prevent and combat terrorist offenses and transnational crime, while respecting fundamental rights and freedoms and recognizing the importance of privacy and the protection of personal data and information;

HAVING REGARD for international instruments, U.S. statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to make PNR available to the Department of Homeland Security (DHS) to the extent they are collected and contained in the air carrier's automated reservation/departure control systems, and comparable requirements that are or may be implemented in the EU;

NOTING that DHS processes and uses PNR for the purpose of preventing, detecting, investigating and prosecuting terrorist offenses and transnational crime in compliance with safeguards on privacy and the protection of personal data and information, as set out in this Agreement;

STRESSING the importance of sharing PNR and relevant and appropriate analytical information obtained from PNR by the United States with competent police and judicial authorities of Member States of the European Union, hereinafter "EU Member States", and Europol or Eurojust as a means to foster international police and judicial cooperation;

ACKNOWLEDGING both Parties' longstanding traditions of respect for individual privacy, as reflected in their laws and founding documents;

MINDFUL of the EU's commitments pursuant to Article 6 of the Treaty on European Union on respect for fundamental rights, the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union, the principles of proportionality and necessity concerning the right to private and family life, the respect for privacy, and the protection of personal data under Article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional Protocol 181, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union;

MINDFUL that DHS currently employs robust processes to protect personal privacy and ensure data integrity, including physical security, access controls, data separation and encryption, audit capabilities and effective accountability measures;

RECOGNIZING the importance of ensuring data quality, accuracy, integrity, and security, and instituting appropriate accountability to ensure these principles are observed;

NOTING in particular the principle of transparency and the various means by which the United States ensures that passengers whose PNR is collected by DHS are made aware of the need for and use of their PNR;

FURTHER RECOGNIZING that the collection and analysis of PNR is necessary for DHS to carry out its border security mission, while ensuring that collection and use of PNR remains relevant and necessary for the purposes for which it is collected;

RECOGNIZING that, in consideration of this Agreement and its implementation, DHS shall be deemed to ensure an adequate level of data protection for the processing and use of PNR transferred to DHS;

MINDFUL that the United States and the European Union are committed to ensuring a high level of protection of personal information while fighting crime and terrorism, and are determined to reach, without delay, an agreement to protect personal information exchanged in the context of fighting crime and terrorism in a comprehensive manner that will advance our mutual goals;

ACKNOWLEDGING the successful Joint Reviews in 2005 and 2010 of the 2004 and 2007 Agreements between the Parties on the transfer of PNR;

NOTING the interest of the Parties, as well as EU Member States, in exchanging information regarding the method of transmission of PNR as well as the onward transfer of PNR as set forth in the relevant articles of this Agreement, and further noting the EU's interest in having this addressed in the context of the consultation and review mechanism set forth in this Agreement;

AFFIRMING that this Agreement does not constitute a precedent for any future arrangements between the Parties, or between either of the Parties and any other party, regarding the processing, use, or transfer of PNR or any other form of data, or regarding data protection;

RECOGNIZING the related principles of proportionality as well as relevance and necessity that guide this Agreement and its implementation by the European Union and the United States; and

HAVING REGARD to the possibility of the Parties to further discuss the transfer of PNR data in the maritime mode;

HEREBY AGREE:

CHAPTER I

GENERAL PROVISIONS

ARTICLE 1

Purpose

1. The purpose of this Agreement is to ensure security and to protect the life and safety of the public.

2. For this purpose, this Agreement sets forth the responsibilities of the Parties with respect to the conditions under which PNR may be transferred, processed and used, and protected.

ARTICLE 2

Scope

1. PNR, as set forth in the Guidelines of the International Civil Aviation Organization, shall mean the record created by air carriers or their authorized agents for each journey booked by or on behalf of any passenger and contained in carriers' reservation systems, departure control systems, or equivalent systems providing similar functionality (collectively referred to in this Agreement as "reservation systems"). Specifically, as used in this Agreement, PNR consists of the data types set forth in the Annex to this Agreement ("Annex").

2. This Agreement shall apply to carriers operating passenger flights between the European Union and the United States.

3. This Agreement shall also apply to carriers incorporated or storing data in the European Union and operating passenger flights to or from the United States.

ARTICLE 3

Provision of PNR

The Parties agree that carriers shall provide PNR contained in their reservation systems to DHS as required by and in accordance with DHS standards and consistent with this Agreement. Should PNR transferred by carriers include data beyond those listed in the Annex, DHS shall delete such data upon receipt.

ARTICLE 4

Use of PNR

1. The United States collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting:

(a) Terrorist offenses and related crimes, including

(i) Conduct that –

1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

2. appears to be intended to –

   a. intimidate or coerce a civilian population;

   b. influence the policy of a government by intimidation or coercion; or

   c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

(ii) Activities constituting an offense within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

(iii) Providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

(iv) Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

(v) Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

(vi) Organizing or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

(vii) Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

(viii) Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

(b) Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.

A crime is considered as transnational in nature in particular if:

(i) It is committed in more than one country;

(ii) It is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

(iii) It is committed in one country but involves an organized criminal group that engages in criminal activities in more than one country;

(iv) It is committed in one country but has substantial effects in another country; or

(v) It is committed in one country and the offender is in or intends to travel to another country.

2. PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.

3. PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

4. Paragraphs 1, 2, and 3 shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR.

CHAPTER II

SAFEGUARDS APPLICABLE TO THE USE OF PNR

ARTICLE 5

Data Security

1. DHS shall ensure that appropriate technical measures and organizational arrangements are implemented to protect personal data and personal information contained in PNR against accidental, unlawful or unauthorized destruction, loss, disclosure, alteration, access, processing or use.

2. DHS shall make appropriate use of technology to ensure data protection, security, confidentiality and integrity. In particular, DHS shall ensure that:

(a) encryption, authorization and documentation procedures recognized by competent authorities are applied. In particular, access to PNR shall be secured and limited to specifically authorized officials;

(b) PNR shall be held in a secure physical environment and protected with physical intrusion controls; and

(c) a mechanism exists to ensure that PNR queries are conducted consistent with Article 4.

3. In the event of a privacy incident (including unauthorized access or disclosure), DHS shall take reasonable measures to notify affected individuals as appropriate, to mitigate the risk of harm of unauthorized disclosures of personal data and information, and to institute remedial measures as may be technically practicable.

4. Within the scope of this Agreement, DHS shall inform without undue delay the relevant European authorities about cases of significant privacy incidents involving PNR of EU citizens or residents resulting from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any unlawful forms of processing or use.

5. The United States confirms that effective administrative, civil, and criminal enforcement measures are available under U.S. law for privacy incidents. DHS may take disciplinary action against persons responsible for any such privacy incident, as appropriate, to include denial of system access, formal reprimands, suspension, demotion, or removal from duty.

6. All access to PNR, as well as its processing and use, shall be logged or documented by DHS. Logs or documentation shall be used only for oversight, auditing, and system maintenance purposes or as otherwise required by law.

ARTICLE 6

Sensitive Data

1. To the extent that PNR of a passenger as collected includes sensitive data (i.e., personal data and information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning the health or sex life of the individual), DHS shall employ automated systems to filter and mask out sensitive data from PNR. In addition, DHS shall not further process or use such data, except in accordance with paragraphs 3 and 4.

2. DHS shall provide to the European Commission within 90 days of the entry into force of this Agreement a list of codes and terms identifying sensitive data that shall be filtered out.

3. Access to, as well as processing and use of, sensitive data shall be permitted in exceptional circumstances where the life of an individual could be imperiled or seriously impaired. Such data may be exclusively accessed using restrictive processes on a case-by-case basis with the approval of a DHS senior manager.

4. Sensitive data shall be permanently deleted not later than 30 days from the last receipt of PNR containing such data by DHS. However, sensitive data may be retained for the time specified in U.S. law for the purpose of a specific investigation, prosecution or enforcement action.

ARTICLE 7

Automated Individual Decisions

The United States shall not make decisions that produce significant adverse actions affecting the legal interests of individuals based solely on automated processing and use of PNR.

ARTICLE 8

Retention of Data

1. DHS retains PNR in an active database for up to five years. After the initial six months of this period, PNR shall be depersonalized and masked in accordance with paragraph 2 of this Article. Access to this active database shall, unless otherwise permitted by this Agreement, be restricted to a limited number of specifically authorized officials.

2. To achieve depersonalization, personally identifiable information contained in the following PNR data types shall be masked out:

(a) name(s);

(b) other names on PNR;

(c) all available contact information (including originator information);

(d) General Remarks, including other supplementary information (OSI), special service information (SSI), and special service request (SSR); and

(e) any collected Advance Passenger Information System (APIS) information.

3. After this active period, PNR shall be transferred to a dormant database for a period of up to ten years. This dormant database shall be subject to additional controls, including a more restricted number of authorized personnel, as well as a higher level of supervisory approval required before access. In this dormant database, PNR shall not be repersonalized except in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk. As regards the purposes as set out in Article 4(1)(b), PNR in this dormant database may only be repersonalized for a period of up to five years.

4. Following the dormant period, data retained must be rendered fully anonymized by deleting all data types which could serve to identify the passenger to whom PNR relate without the possibility of repersonalization.

5. Data that are related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived. This paragraph is without prejudice to data retention requirements for individual investigation or prosecution files.

6. The Parties agree that, within the framework of the evaluation as provided for in Article 23(1), the necessity of a 10-year dormant period of retention will be considered.

ARTICLE 9

Non-discrimination

The United States shall ensure that the safeguards applicable to processing and use of PNR under this Agreement apply to all passengers on an equal basis without unlawful discrimination.

ARTICLE 10

Transparency

1. DHS shall provide information to the traveling public regarding its use and processing of PNR through:

(a) publications in the Federal Register;

(b) publications on its website;

(c) notices that may be incorporated by the carriers into contracts of carriage;

(d) statutorily required reporting to Congress; and

(e) other appropriate measures as may be developed.

2. DHS shall publish and provide to the EU for possible publication its procedures and modalities regarding access, correction or rectification, and redress procedures.

3. The Parties shall work with the aviation industry to encourage greater visibility to passengers at the time of booking on the purpose of the collection, processing and use of PNR by DHS, and on how to request access, correction and redress.

ARTICLE 11

Access for Individuals

1. In accordance with the provisions of the Freedom of Information Act, any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS. DHS shall timely provide such PNR subject to the provisions of paragraphs 2 and 3 of this Article.

2. Disclosure of information contained in PNR may be subject to reasonable legal limitations, applicable under U.S. law, including any such limitations as may be necessary to safeguard privacy-protected, national security, and law enforcement sensitive information.

3. Any refusal or restriction of access shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis on which information was withheld and shall inform the individual of the options available under U.S. law for seeking redress.

4. DHS shall not disclose PNR to the public, except to the individual whose PNR has been processed and used or his or her representative, or as required by U.S. law.

ARTICLE 12

Correction or Rectification for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence may seek the correction or rectification, including the possibility of erasure or blocking, of his or her PNR by DHS pursuant to the processes described in this Agreement.

2. DHS shall inform, without undue delay, the requesting individual in writing of its decision whether to correct or rectify the PNR at issue.

3. Any refusal or restriction of correction or rectification shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis of such refusal or restriction and shall inform the individual of the options available under U.S. law for seeking redress.

ARTICLE 13

Redress for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with U.S. law.

2. Any individual is entitled to seek to administratively challenge DHS decisions related to the use and processing of PNR.

3. Under the provisions of the Administrative Procedure Act and other applicable law, any individual is entitled to petition for judicial review in U.S. federal court of any final agency action by DHS. Further, any individual is entitled to petition for judicial review in accordance with applicable law and relevant provisions of:

(a) the Freedom of Information Act;

(b) the Computer Fraud and Abuse Act;

(c) the Electronic Communications Privacy Act; and

(d) other applicable provisions of U.S. law.

4. In particular, DHS provides all individuals an administrative means (currently the DHS Traveler Redress Inquiry Program (DHS TRIP)) to resolve travel-related inquiries including those related to the use of PNR. DHS TRIP provides a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, any such aggrieved individual is entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns.

ARTICLE 14

Oversight

1. Compliance with the privacy safeguards in this Agreement shall be subject to independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer, who:

(a) have a proven record of autonomy;

(b) exercise effective powers of oversight, investigation, intervention, and review; and

(c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate.

They shall, in particular, ensure that complaints relating to non-compliance with this Agreement are received, investigated, responded to, and appropriately redressed. These complaints may be brought by any individual, regardless of nationality, country of origin, or place of residence.

2. In addition, application of this Agreement by the United States shall be subject to independent review and oversight by one or more of the following entities:

(a) the DHS Office of Inspector General;

(b) the Government Accountability Office as established by Congress; and

(c) the U.S. Congress.

Such oversight may be manifested in the findings and recommendations of public reports, public hearings, and analyses.

CHAPTER III

MODALITIES OF TRANSFERS

ARTICLE 15

Method of PNR Transmission

1. For the purposes of this Agreement, carriers shall be required to transfer PNR to DHS using the "push" method, in furtherance of the need for accuracy, timeliness and completeness of PNR.

2. Carriers shall be required to transfer PNR to DHS by secure electronic means in compliance with the technical requirements of DHS.

3. Carriers shall be required to transfer PNR to DHS in accordance with paragraphs 1 and 2, initially at 96 hours before the scheduled flight departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS.

4. In any case, the Parties agree that all carriers shall be required to acquire the technical ability to use the "push" method not later than 24 months following entry into force of this Agreement.

5. DHS may, where necessary, on a case-by-case basis, require a carrier to provide PNR between or after the regular transfers described in paragraph 3. Wherever carriers are unable, for technical reasons, to respond timely to requests under this Article in accordance with DHS standards, or, in exceptional circumstances in order to respond to a specific, urgent, and serious threat, DHS may require carriers to otherwise provide access.

ARTICLE 16

Domestic Sharing

1. DHS may share PNR only pursuant to a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

(b) Only with domestic government authorities when acting in furtherance of the uses outlined in Article 4;

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement; and

(d) PNR shall be shared only in support of those cases under examination or investigation and pursuant to written understandings and U.S. law on the exchange of information between domestic government authorities.

2. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraph 1 of this Article shall be respected.

ARTICLE 17

Onward Transfer

1. The United States may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with those terms.

2. Apart from emergency circumstances, any such transfer of data shall occur pursuant to express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS as set out in this Agreement.

3. PNR shall be shared only in support of those cases under examination or investigation.

4. Where DHS is aware that PNR of a citizen or a resident of an EU Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity.

5. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1 to 4 shall be respected.

ARTICLE 18

Police, Law Enforcement and Judicial Cooperation

1. Consistent with existing law enforcement or other information-sharing agreements or arrangements between the United States and any EU Member State or Europol and Eurojust, DHS shall provide to competent police, other specialized law enforcement or judicial authorities of the EU Member States and Europol and Eurojust within the remit of their respective mandates, as soon as practicable, relevant, and appropriate, analytical information obtained from PNR in those cases under examination or investigation to prevent, detect, investigate, or prosecute within the European Union terrorist offenses and related crimes or transnational crime as described in Article 4(1)(b).

2. A police or judicial authority of an EU Member State, or Europol or Eurojust, may request, within its mandate, access to PNR or relevant analytical information obtained from PNR that are necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union terrorist offenses and related crimes or transnational crime as described in Article 4(1)(b). DHS shall, subject to the agreements and arrangements noted in paragraph 1 of this Article, provide such information.

3. Pursuant to paragraphs 1 and 2 of this Article, DHS shall share PNR only following a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

(b) Only when acting in furtherance of the uses outlined in Article 4; and

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement.

4. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1-3 of this Article shall be respected.

CHAPTER IV

IMPLEMENTING AND FINAL PROVISIONS

ARTICLE 19

Adequacy

In consideration of this Agreement and its implementation, DHS shall be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing and use. In this respect, carriers which have provided PNR to DHS in compliance with this Agreement shall be deemed to have complied with applicable legal requirements in the EU related to the transfer of such data from the EU to the United States.

ARTICLE 20

Reciprocity

1. The Parties shall actively promote the cooperation of carriers within their respective jurisdictions with any PNR system operating or as may be adopted in the other's jurisdiction, consistent with this Agreement.

2. Given that the establishment of an EU PNR system could have a material effect on the Parties' obligations under this Agreement, if and when an EU PNR system is adopted, the Parties shall consult to determine whether this Agreement would need to be adjusted accordingly to ensure full reciprocity. Such consultations shall in particular examine whether any future EU PNR system would apply less stringent data protection standards than those provided for in this Agreement, and whether, therefore, this Agreement should be amended.

ARTICLE 21

Implementation and Non-Derogation

1. This Agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public. Each Party shall ensure that the provisions of this Agreement are properly implemented.

2. Nothing in this Agreement shall derogate from existing obligations of the United States and EU Member States, including under the Agreement on Mutual Legal Assistance between the European Union and the United States of 25 June 2003 and the related bilateral mutual legal assistance instruments between the United States and EU Member States.

ARTICLE 22

Notification of Changes in Domestic Law

The Parties shall advise each other regarding the enactment of any legislation that materially affects the implementation of this Agreement.

ARTICLE 23

Review and Evaluation

1. The Parties shall jointly review the implementation of this Agreement one year after its entry into force and regularly thereafter as jointly agreed. Further, the Parties shall jointly evaluate this Agreement four years after its entry into force.

2. The Parties shall jointly determine in advance the modalities and terms of the joint review and shall communicate to each other the composition of their respective teams. For the purpose of the joint review, the European Union shall be represented by the European Commission, and the United States shall be represented by DHS. The teams may include appropriate experts on data protection and law enforcement. Subject to applicable laws, participants in the joint review shall be required to have appropriate security clearances and to respect the confidentiality of the discussions. For the purpose of the joint review, DHS shall ensure appropriate access to relevant documentation, systems, and personnel.

3. Following the joint review, the European Commission shall present a report to the European Parliament and the Council of the European Union. The United States shall be given an opportunity to provide written comments which shall be attached to the report.

ARTICLE 24

Resolution of Disputes and Suspension of Agreement

1. Any dispute arising from the implementation of this Agreement, and any matters related thereto, shall give rise to consultations between the Parties, with a view to reaching a mutually agreeable resolution, including providing an opportunity for either Party to cure within a reasonable time.

2. In the event that consultations do not result in a resolution of the dispute, either Party may suspend the application of this Agreement by written notification through diplomatic channels, with any such suspension to take effect 90 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

3. Notwithstanding any suspension of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its suspension shall continue to be processed and used in accordance with the safeguards of this Agreement.

ARTICLE 25

Termination

1. Either Party may terminate this Agreement at any time by written notification through diplomatic channels.

2. Termination shall take effect 120 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

3. Prior to any termination of this Agreement, the Parties shall consult each other in a manner which allows sufficient time for reaching a mutually agreeable resolution.

4. Notwithstanding any termination of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its termination shall continue to be processed and used in accordance with the safeguards of this Agreement.

ARTICLE 26

Duration

1. Subject to Article 25, this Agreement shall remain in force for a period of seven years from the date of its entry into force.

2. Upon the expiry of the period set forth in paragraph 1 of this Article, as well as any subsequent period of renewal under this paragraph, the Agreement shall be renewed for a subsequent period of seven years unless one of the Parties notifies the other in writing through diplomatic channels, at least twelve months in advance, of its intention not to renew the Agreement.

3. Notwithstanding the expiration of this Agreement, all PNR obtained by DHS under the terms of this Agreement shall continue to be processed and used in accordance with the safeguards of this Agreement. Similarly, all PNR obtained by DHS under the terms of the 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), signed at Brussels and Washington July 23 and 26, 2007, shall continue to be processed and used in accordance with the safeguards of that Agreement.

ARTICLE 27

Final provisions

1. This Agreement shall enter into force on the first day of the month after the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for this purpose.

2. This Agreement, as of the date of its entry into force, shall supersede the July 23 and 26, 2007 Agreement.

3. This Agreement will only apply to the territory of Denmark, the United Kingdom or Ireland, if the European Commission notifies the United States in writing that Denmark, the United Kingdom or Ireland has chosen to be bound by this Agreement.

4. If the European Commission notifies the United States before the entry into force of this Agreement that it will apply to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of the relevant State on the same day as for the other EU Member States bound by this Agreement.

5. If the European Commission notifies the United States after entry into force of this Agreement that it applies to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of the relevant State on the first day following receipt of the notification by the United States.

Done at…this…day of…2011, in two originals in the English language.

Pursuant to EU law, this Agreement shall also be drawn up by the EU in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages.

ANNEX

PNR Data Types

1. PNR record locator code

2. Date of reservation/issue of ticket

3. Date(s) of intended travel

4. Name(s)

5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.)

6. Other names on PNR, including number of travelers on PNR

7. All available contact information (including originator information)

8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)

9. Travel itinerary for specific PNR

10. Travel agency/travel agent

11. Code share information

12. Split/divided information

13. Travel status of passenger (including confirmations and check-in status)

14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote

15. All baggage information

16. Seat information, including seat number

17. General remarks including OSI, SSI and SSR information

18. Any collected APIS information

19. All historical changes to the PNR listed under points 1 to 18

APPENDIX 4: 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

[Federal Register Volume 77, Number 99 (Tuesday, May 22, 2012)]
[Notices]
[Pages 30297-30304]
From the Federal Register Online via the Government Printing Office [www.gpo.gov]
[FR Doc No: 2012-12396]
==========
DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0019]

Privacy Act of 1974; U.S. Customs and Border Protection, DHS/CBP-006--Automated Targeting System, System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and expand an existing Department of Homeland Security system of records notice titled, U.S. Customs and Border Protection, DHS/CBP-006--Automated Targeting System (ATS) 72 FR 43650, August 6, 2007. The Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) have designed ATS to efficiently perform risk assessments on information pertaining to international travelers and import and export shipments attempting to enter or leave the United States. ATS uses a rule-managed technology that facilitates the targeting of high-risk travelers and cargo.

DHS/CBP is publishing this System of Records Notice (SORN) to update ATS and to update and expand the categories of individuals, categories of records, routine uses, access provisions, and sources of data stored in ATS. Elsewhere in the Federal Register, the Department of Homeland Security is concurrently issuing a Notice of Proposed Rulemaking exempting this system of records from certain provisions of the Privacy Act. This updated and expanded system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before June 21, 2012. This system will be effective June 21, 2012.

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0019 by one of the following methods:

Federal e-Rulemaking Portal: http://www.regulations.gov.
Follow the instructions for submitting comments.

Fax: 703-483-2999.

Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-325-0280), CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street NW., Washington, DC 20229. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and expand an existing Department of Homeland Security SORN titled, U.S. Customs and Border Protection, DHS/CBP-006--Automated Targeting System (ATS) 72 FR 43650, August 6, 2007.

This SORN is being updated and expanded to inform the public about changes to the Automated Targeting System (ATS) categories of individuals, categories of records, routine uses, access provisions, and sources of data. DHS/CBP is updating and expanding the categories of individuals, categories of records, and sources of records stored in ATS because it has certain data that it must ingest for performance purposes. The Privacy Impact Assessment (PIA), which DHS will publish on its Web site (http://www.dhs.gov/privacy) concurrently with the publication of this SORN in the Federal Register, provides a full discussion of the functional capabilities of ATS and its modules. DHS and CBP have previously exempted portions of ATS from the notification, access, amendment, and public accounting provisions of the Privacy Act because it is a law enforcement system. DHS and CBP, however, will consider each request for access to records maintained in ATS to determine whether or not information may be released. DHS and CBP further note that despite the exemption taken on this system of records they are providing access and amendment to passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d, Importer Security Filing (10+2 documentation) information, and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act.

ATS provides the following basic functionalities to support CBP in identifying individuals and cargo that need additional review across the different means or modes of travel to and from the United States:

Comparison: ATS compares information on travelers and cargo coming into and going out of the country against law enforcement and intelligence databases to identify individuals and cargo requiring additional scrutiny. For example, ATS compares information on individuals (identified

as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) trying to enter the country or trying to enter merchandise into the country against the Terrorist Screening Database (TSDB), which ATS ingests from the DHS Watchlist Service (WLS), and outstanding wants and warrants.

Rules: ATS compares existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence corroborating those trends. For example, ATS might compare information on cargo entering the country against a set of scenario-based targeting rules that indicate a particular type of fish rarely is imported from a given country.

Federated Query: ATS allows users to search data across many different databases and correlate it across the various systems to provide a person centric view of all data responsive to a query about the person's identity from the selected databases.

In order to do the above, ATS pulls data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system. Below is a summary:

Official Record: ATS maintains the official record for Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d; for Importer Security Filing (10+2 documentation) information, which provides advanced information about cargo and related persons and entities for risk assessment and targeting purposes; for results of Cargo Enforcement Exams; for the combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; for law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source and/or classified information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department.

Ingestion of Data: ATS maintains copies of key elements of certain CBP databases in order to minimize the processing time for searches on the operational systems and to act as a backup for certain operational systems, including, but not limited to: Automated Commercial Environment (ACE), Automated Commercial System (ACS), Automated Export System (AES), Advance Passenger Information System (APIS), Border Crossing Information (BCI), Consular Electronic Application Center (CEAC), Enforcement Integrated Database (EID)[which includes the Enforcement Case Tracking System (ENFORCE)], Electronic System for Travel Authorization (ESTA), Global Enrollment System (GES), Non-Immigrant Information System (NIIS), historical National Security Entry-Exit Registration System (NSEERS), Seized Asset and Case Tracking System (SEACATS), U.S. Immigration and Customs Enforcement (ICE) Student Exchange and Visitor Information System (SEVIS), Social Security Administration (SSA) Death Master File, TECS, Terrorist Screening Database (TSDB) through the DHS Watchlist Service (WLS), and WebIDENT. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in this SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

Pointer System: ATS accesses and uses additional databases without ingesting the data, including, but not limited to: CBP Border Patrol Enforcement Tracking System (BPETS), Department of State Consular Consolidated Database (CCD), commercial data aggregators,

CBP's Enterprise Geospatial Information Services (eGIS), DHS/USVISIT IDENT, National Law Enforcement Telecommunications System (Nlets), DOJ's National Crime Information Center (NCIC), the results of queries in the FBI's Interstate Identification Index (III), and the National Insurance Crime Bureau's (NICB's) private database of stolen vehicles. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in this SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

DHS/CBP has reorganized the ATS routine uses to provide greater uniformity across DHS systems. Consistent with DHS's information sharing mission, information stored in ATS may be shared with other DHS components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies. This sharing will only take place 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 this SORN.

DHS has exempted the system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974 because of the law enforcement nature of ATS. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d, Importer Security Filing (10+2 documentation) information, and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler may obtain access to his or her PNR and request amendment as appropriate, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, projects developed by CBP that may include public source and/or classified information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information, will not be accessible to the individual.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a “system of records.” A “system of records” is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy (Privacy Policy Guidance Memorandum 2007-1, most recently updated January 7, 2009), DHS extends administrative Privacy Act protections to all persons, regardless of citizenship, where a system of records maintains information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent,

to notify individuals regarding the uses to which their records are put, and to assist individuals with more easily finding such files within the agency. Below is the description of the U.S. Customs and Border Protection DHS/CBP-006 Automated Targeting System system of records.

In accordance with 5 U.S.C.552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records DHS/CBP-006.

System name:

U.S. Customs and Border Protection Automated Targeting System.

Security classification:

Unclassified, sensitive, classified.

System location:

Records are maintained at the CBP Headquarters in Washington, DC, and can be accessed from field offices and from locations abroad where ATS users are stationed.

Categories of individuals covered by the system:

ATS handles information relating to the following individuals:

A. Persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence by land, air, or sea.

B. Crew members traveling on commercial aircraft that fly over the United States.

C. Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise, including those required to submit an Importer Security Filing.

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

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

F. Owners of vehicles that cross the border.

G. Persons whose data was received by the Department as the result of memoranda of understanding or other information sharing agreement or arrangement because the information is relevant to the border security mission of the Department.

H. Persons who were identified in a narrative report, prepared by an officer or agent, as being related to or associated with other persons who are alleged to be involved in, who are suspected of, or who have been arrested for violations of the laws enforced or administered by DHS.

I. Persons who may pose a threat to the United States.

Categories of records in the system:

ATS contains various types of data to support its targeting missions, incorporating information germane to the identification of individuals, including, but not limited to:

Name

Addresses (home, work, and/or destination, as appropriate)

Telephone and fax numbers
Tax ID number (e.g., Employer Identification Number (EIN) or
Social Security Number (SSN), where available)
Date and place of birth
Gender
Nationality
Country of Residence
Citizenship
Alias
Physical characteristics, including biometrics where available (e.g., height, weight, race, eye and hair color, scars, tattoos, marks, fingerprints)
Familial relationships and other contact information
Property information
Occupation and employment information
Biographical and biometric information from or associated with online immigrant and non-immigrant visa applications, including (as available):
[cir] U.S. sponsor's name, address, and phone number
[cir] U.S. contact name, address, and phone number
[cir] Employer name, address, and phone number
[cir] Email address, IP Address, applicant ID
[cir] Marital Status
[cir] Alien number
[cir] Social Security Number
[cir] Tax Identification Number
[cir] Organization Name
[cir] U.S. Status
[cir] Income information for Joint Sponsors
[cir] Education, military experience, relationship information
[cir] Responses to vetting questions pertaining to admissibility or eligibility
Information from documents used to verify the identity of individuals (e.g., driver's license, passport, visa, alien registration, citizenship card, border crossing card, birth certificate, certificate of naturalization, re-entry permit, military card) including the:
type
number
date of issuance
place of issuance

The system contains travel information pertaining to individuals, including:

The combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing
Information derived from an ESTA application including responses to vetting questions pertaining to admissibility (where applicable)
Travel itinerary
Date of arrival or departure, and means of conveyance with associated identification (e.g., Vehicle Identification Number, year, make, model, registration)

Passenger Name Record (PNR):

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

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

The system contains information collected for the importation or exportation of cargo and/or property, including:

Bill of lading
Commodity type
License number and license country for Office of Defense Trade Controls registrants
Inspection and examination results

The system contains Importer Security Filing (ISF) information, which must contain the following items, in addition to the Vessel Stow Plan (VSP) and the Container Status Message (CSM):

Manufacturer (or supplier)
Seller (i.e., full name and address or widely accepted business number such as a Data Universal Numbering System (DUNS) number)

Buyer (i.e., full name and address)
Ship to party (full name and/or business name and address)
Container stuffing location
Consolidator (stuffer)
Importer of record number/Foreign Trade Zone applicant identification number
Consignee number(s)
Country of origin
Commodity: Harmonized Tariff Schedule of the United States (HTSUS) number

Alternatively, for shipments consisting entirely of Freight Remaining on Board (FROB) or shipments consisting of goods intended to move through the United States, ISF Importers, or their agents, must submit the following five elements, unless an element is specifically exempted:

Booking party (i.e., name and address)
Foreign port of unlading
Place of delivery
Ship to party
Commodity HTSUS number

The system contains assessments and other information obtained in accordance with the terms of memoranda of understanding or other arrangement because the information is relevant to the border security mission of the Department.

The system also contains information created by CBP, including:
Admissibility determinations
Results of Cargo Enforcement Exams
Law enforcement or intelligence information regarding an individual
Risk-based rules developed by analysts to assess and identify high-risk cargo, conveyances, or travelers that should be subject to further scrutiny or examination
Assessments resulting from the rules, with a record of which rules were used to develop the assessment
Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.

Authority for maintenance of the system:

ATS derives its authority 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).

Purpose(s):

PURPOSES FOR PNR IN ATS: PNR may be used,

(1). To prevent, detect, investigate, and prosecute:

a. Terrorist offenses and related crimes, including

i. Conduct that--

1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

2. appears to be intended to--

a. intimidate or coerce a civilian population;

b. influence the policy of a government by intimidation or coercion; or

c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

ii. Activities constituting an offense within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

iii. Providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

iv. Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

v. Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

vi. Organizing or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

vii. Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

viii. Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

b. Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature;

A crime is considered as transnational in nature in particular if:

i. It is committed in more than one country;

ii. It is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

iii. It is committed in one country but involves an organized criminal group that engages in criminal activities in more than one country;

iv. It is committed in one country but has substantial effects in another country; or

v. It is committed in one country and the offender is in or intends to travel to another country;

(2) on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court;

(3) to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

(4) for domestic law enforcement, judicial powers, or proceedings, where violations of law or indications thereof are detected in the course of the use and processing of PNR.

PURPOSES OF ATS (EXCEPT for PNR):

ATS uses all other data for purposes listed above as well as below:

(a) To perform targeting of individuals who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law;

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

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

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Information ingested into this system from another source system is to be handled consistent with the published system of records notice for the source system and will continue to be governed by the routine uses for that source system. The routine uses below apply only to records that are maintained as official records in ATS (i.e., records which are maintained in ATS that are not covered by other originating systems of record, including: PNR; Importer Security Filings; Cargo Enforcement Exams; the combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department). With respect to PNR, DHS only discloses information to those authorities who intend to use the information consistent with the purposes identified above, and have sufficient capability to protect and safeguard the information. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary or relevant to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. any employee of DHS in his/her official capacity;

3. any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. the United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made pursuant to a written Privacy Act waiver at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

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

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, of identity theft or fraud, or of harm to the security or integrity of this system or of harm to other systems or programs (whether maintained

by DHS or another agency or entity) or harm to the individuals that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

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

H. To federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or to assist in anti-terrorism efforts;

I. To an organization or person in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a person;

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

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

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

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

N. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:
None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:
Storage:
Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.
Retrievability:
Records may be retrieved by any of the data elements described in "Categories of Records," including by name or personal identifier from an electronic database.

Safeguards:
Records in this system 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. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:
Official Records in this system (Passenger Name Records (PNR); Importer Security Filings (10+2 documentation); results of Cargo Enforcement Exams; the combination of license plate, Department of Motor Vehicle registration data, and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008. ATS collects information directly, ingests information from various systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data is retained in ATS in accordance with the record retention requirements of those systems, or the retention period for ATS, whichever is shortest. The retention period for the official records maintained in ATS will not exceed fifteen years, after which time the records will be deleted, except as noted below. The retention period for PNR will be subject to the following further access restrictions: ATS users with PNR access will have access to PNR in an active database for up to five years, during which time the PNR will be depersonalized following the first six months retention. After this initial five-year retention, the PNR data will be transferred to a dormant database for a period of up to ten years. PNR data in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be repersonalized in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this

information and allowing CBP to continue to identify potential high-risk travelers. Notwithstanding the foregoing, information maintained only in ATS that is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

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

System Manager and address:

Executive Director, Automation and Targeting Division, Office of Intelligence and Investigative Liaison, U.S. Customs and Border Protection, and Director, Targeting and Analysis, Systems Program Office, Office of Information and Technology, U.S. Customs and Border Protection, both of whom are located at 1300 Pennsylvania Avenue NW., Washington, DC 20229.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, amendment, and certain accounting procedures of the Privacy Act because it is a law enforcement system. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place. To the extent that a record is exempted in a source system, the exemption will continue to apply. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. Individuals seeking notification of and access to records contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or CBP FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under ``contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP-0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must

either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

An explanation of why you believe the Department would have information on you,

Identify which component(s) of the Department you believe may have the information about you,

Specify when you believe the records would have been created,

Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records, and

If your request is seeking records pertaining to another living individual, you must include a statement from that individual
certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See ``Notification procedure" above.

Contesting record procedures:

See ``Notification procedure" above.

Record source categories:

Records are ingested from other DHS and federal systems, and from foreign governments (in accordance with the terms of international agreements and arrangements), including but not limited to ACE, ACS, AES, APIS, BCI, CEAC (including Forms DS-160 and DS-260), ENFORCE, ESTA, GES, NIIS, NSEERS, SEACATS, SEVIS, TECS, TSDB-WLS, Social Security Administration's Death Master File, and WebIDENT,
Additionally, PNR is obtained from travel reservation systems of commercial carriers. Information from Importer Security Filings is received from importers and ocean carriers. Records are accessed from BPETS, CCD, eGIS, NCIC, and Nlets. Also, the results of queries in the FBI's Interstate Identification Index (III), the National Insurance Crime Bureau's (NICB's) private database of stolen vehicles, and commercial data aggregators are stored in ATS. Lastly, records are also developed from analysis created by users as a result of their use of the system.

Exemptions claimed for the system:

Pursuant to 6 CFR Part 5, Appendix C, certain records and information in this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. 552a (k)(1) and (k)(2): 5 U.S.C. 552a(c)(3); (d)(1), (d)(2), (d)(3), and (d)(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger

name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler may obtain access to his or her PNR, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information will not be accessible to the individual.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2012-12396 Filed 5-21-12; 8:45 am]
BILLING CODE 9110-06-P

[FR Doc. 2012-12396 Filed 5-21-12; 8:45 am]
BILLING CODE 9110-06-P [FR Doc. 2012-12396 Filed 5-21-12; 8:45 am]

APPENDIX 5: Privacy Impact Assessment for the Automated Targeting System DHS/CBP/PIA-006(b) June 1, 2012

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf

Privacy Impact Assessment
for the
Automated Targeting System

DHS/CBP/PIA-006(b)

June 1, 2012

Contact Point
Thomas Bush
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
(202) 344-1150

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS). As a decision support tool, ATS compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. This PIA is being conducted to notify the public about the changes in modules and expansion of access to datasets used by and stored in ATS.

This PIA is being published in conjunction with an updated System of Records Notice (SORN) that has been published in the *Federal Register*.

Overview

In order to facilitate legitimate trade and travel while managing the risk of people or cargo entering or exiting the United States who may pose a threat, DHS CBP has designed and continues to operate the Automated Targeting System (ATS).

ATS provides the following basic functionalities to support CBP in identifying individuals and cargo that need additional review across the different means or modes of travel to, through, and from the United States:

- *Comparison:* ATS compares information on travelers and cargo arriving in, transiting through, and exiting the country against law enforcement and intelligence databases to identify individuals and cargo requiring additional scrutiny. For example, ATS compares information on individuals (identified as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) trying to enter the country or trying to enter merchandise into the country against the Terrorist Screening Database (TSDB), which ATS ingests from the DHS Watchlist Service (WLS), as well as data concerning outstanding wants and warrants.
- *Rules:* ATS compares existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, analysis of trends of suspicious activity, law enforcement cases and raw intelligence. For example, ATS might compare information on cargo entering the country against a set of scenario-based targeting rules that indicate a particular type of commodity rarely is imported from a given country.
- *Federated Query:* ATS allows users to search data across many different databases and systems to provide a consolidated view of data responsive to a query about a person or entity.

In order to execute the above three functionalities, ATS utilizes data from many different source systems. In some instances ATS is the official record for the information, while in other

instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system. Below is a summary:

- *Official Record:* ATS maintains the official record for Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d; for Importer Security Filing (10+2 documentation) and express consignment manifest information, which provides advanced information about cargo and related persons and entities for risk assessment and targeting purposes; for results of Cargo Enforcement Exams; for the combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information; and certain information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department.

- *Ingestion of Data:* ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems, including, but not limited to: Automated Commercial Environment (ACE), Automated Commercial System (ACS), Arrival and Departure Information System (ADIS), Automated Export System (AES), Advance Passenger Information System (APIS), Border Crossing Information (BCI), Consular Electronic Application Center (CEAC), Enforcement Integrated Database (EID) (which includes the Enforcement Case Tracking System (ENFORCE)), Electronic System for Travel Authorization (ESTA), Global Enrollment System (GES), Non-Immigrant Information System (NIIS), historical National Security Entry-Exit Registration System (NSEERS), Seized Asset and Case Tracking System (SEACATS), U.S. Immigration and Customs Enforcement (ICE) Student Exchange and Visitor Information System (SEVIS), Social Security Administration (SSA) Death Master File, TECS, Terrorist Screening Database (TSDB) which ATS ingests from the DHS Watchlist Service (WLS), and Refused VISA data from CCD . See Appendix D for referenced SORN citations.

- *Pointer System:* ATS accesses and uses additional databases without ingesting the data, including, but not limited to: CBP Border Patrol Enforcement Tracking System (BPETS), Department of State Consular Consolidated Database (CCD), commercial data aggregators, CBP's Enterprise Geospatial Information Services (eGIS), DHS Automated Biometric Identification System (IDENT), WebIDENT, Nlets (not an acronym), DOJ's National Crime Information Center (NCIC), the results of queries in the FBI's Interstate Identification Index (III), and the National Insurance Crime Bureau's (NICB's) private database of stolen vehicles. See Appendix D for referenced SORN citations.

- *Data Manually Processed:* ATS is used to manually process certain datasets to identify national security and public safety concerns and correlate records. Currently, DHS conducts this process for those records in Arrival and Departure Information that have been identified as individuals who may have overstayed their permitted time in the United States.[1] Appendix D will be updated as necessary.

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).

ATS support for CBP's mission is directed into five general areas: 1) export of cargo; 2) import of cargo; 3) land borders; 4) air/sea borders; and 5) cross cutting view of risks across the four previous areas. Each of these sub-systems or modules supports the CBP officer in determining whether or not a particular individual or cargo is higher risk than other individuals or cargo. The final module looks across the different areas to find common concerns and risks. Each sub-system uses slightly different data to conduct its risk assessment, but the basic purposes as described above remain the same. Below is a summary of the sub-systems and data used for the specific purposes.

1) Automated Targeting System-AntiTerrorism (ATS-AT)

ATS-AT evaluates export information, which includes information filed electronically with AES and AESDirect. The export data is sorted, compared to rules, and scored so that CBP officers can identify exports with transportation safety and security risks, such as the Office of Foreign Assets Control (OFAC) violations, smuggled currency, illegal narcotics, and other contraband. ATS-AT not only screens commodity information on export documents, but also screens individuals identified on those documents. ATS-AT provides a consolidated user interface to view the export information. Officers can input findings from outbound exams of exports and generate multiple reports. Further, ATS-AT allows officers to internally track shipments through custom rule criteria, review marking, and watched entity lists. Through the ATS-AT web interface CBP personnel can create *ad hoc* queries on exports.

2) Automated Targeting System-N (ATS-N)

ATS-N evaluates all cargo to identify high risk inbound cargo for examinations. ATS-N uses numerous rule and weight sets to analyze information from manifest, importer security filing, and entry data, to prioritize shipments for review, and to generate recommended targets by scoring each shipment. In some cases, ATS-N automatically places shipments on hold when they score above a specified risk threshold. ATS-N not only screens commodity information on manifest, importer security filing, and entry data, but also screens individuals, against lookouts and prior violations, who are identified on those data sources. Additionally, ATS has been updated so that if a broker or importer files a simplified entry through the Automated Broker

[1] DHS/All/PIA-041 One DHS Overstay Vetting Pilot published December 29, 2011.

Interface (ABI), ATS will screen that information and then transmit the simplified entry information to ACS and/or ACE. Through the ATS-N web interface CBP personnel can create *ad hoc* queries on cargo data. Previously, the ATS PIA identified ATS-International (ATS-I) and ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP) as modules distinct from ATS-N. In reviewing these modules and their uses, DHS/CBP determined that while these parts of ATS have a different look and feel, they provide the user with the same types of information and are used to accomplish the same purposes. As such, DHS/CBP has determined that segregation of these two separate aspects of ATS-N is no longer required.

As indicated above, the ATS-N module also includes these sub-modules:

- **ATS-I** provides designated foreign customs authorities with controlled access to automated cargo targeting capabilities. If cargo information from foreign authorities is run through the ATS-I module, it may also, consistent with applicable cooperative arrangements with that foreign authority, be retained in ATS-I and used by CBP to enhance CBP's cargo targeting capabilities. ATS-I uses the same log-in screen as ATS-N, but cargo information is screened based on a set of targeting rules defined by the participating authority without access to underlying CBP systems. Foreign customs authorities are only able to access their own data and cannot access any other data in ATS unless covered by an approved MOU.
- **Cargo Enforcement Reporting and Tracking System (CERTS)** provides CBP officers with a user-friendly, single point of entry for exam findings data. It also allows the CBP officer to query and build custom reports. CERTS establishes a historical database linking targeting reasons, risks, issues, actions, decisions, events, and past and present findings with commodities, shipping parties, and manifest information. CERTS allows trend analysis on the targeting rules based on historical enforcement information.
- **Trend Analysis and Analytical Selectivity Program (TAP) 2000** provides a user-friendly interface to quickly collect and download entry summary information to study importers and importing trends. It enables users to analyze profiles and trends, identify anomalies (unusual pricing, shifts in activity, etc.), and easily retrieve the entry summaries related to the anomalies to facilitate the detection of trade enforcement issues. The application also allows users to analyze workloads and produce resource allocation models.

As CBP continues to modernize cargo targeting, the User-Defined Rules (UDR) component allows the CBP officer to develop rules by using predefined concepts or through the matching of existing data elements in the manifest or entry.

3) Automated Targeting System-Land (ATS-L)

ATS-L evaluates previous crossing records as well as internal and external data sources for targeting at the land border. These internal and external data sources are SEVIS, CBP TECS, FBI TSDB, DOJ NCIC, Department of State's CCD, and Nlets. ATS-L stores vehicle

registration (year, make, model, and Vehicle Identification Number (VIN)) as well as registered owner information (first name, last name, date of birth, if available, and address) for U.S.-plated vehicles and biographical information on the occupants of the vehicle collected through vehicle primary processing at land border ports of entry.

4) Automated Targeting System-Passenger (ATS-P)

ATS-P is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals and, in some cases, other persons who pose a higher risk of violating U.S. law. ATS-P capabilities are used at ports of entry to augment the CBP officer's decision-making about whether a passenger or crew member should receive additional screening.

ATS-P is also used within CBP by Passenger Analytical Units (PAUs) at Ports of Entry, the National Targeting Center (NTC), Border Patrol agents, CBP headquarters intelligence analysts, and within DHS by DHS agents, analysts, and officers in the Office of Intelligence and Analysis (I&A), ICE, U.S. Coast Guard, and the Transportation Security Administration (TSA). ATS-P provides an hierarchical system that allows DHS personnel to focus efforts on potentially high-risk passengers by eliminating labor-intensive manual reviews of traveler information or interviews with every traveler. The assessment process is based on a set of uniform and user-defined rules based on specific operational, tactical, intelligence, or local enforcement efforts.

Additionally, ATS-P is used to vet non-immigrant and immigrant visa applications for the Department of State (DoS). DoS sends online visa application data to ATS-P for pre-adjudication investigative screening. ATS-P screens the visa application and provides a response to the DoS's CCD indicating whether or not derogatory information was identified by DHS about the individual. Applications of individuals for whom derogatory information is identified are referred for manual review to the appropriate agency conducting the screening. If, following manual review, an applicant is determined to be eligible for a visa, an updated response is sent to CCD. If the manual review does not result in any change to the individual's eligibility, an additional processing occurs in the ICE Visa Security Program Tracking System (VSPTS-Net) case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD.

ATS-P is used to vet arrival and departure information received from ADIS to identify potential visa overstay candidates based on supporting data available in ATS, i.e., border crossing information, I-94, and SEVIS. In addition to identifying the list of potential overstay candidates, ATS also develops priorities based on associated risk patterns. This prioritized list of overstay candidates is then passed on to LeadTRAC, case management system for ICE to generate case leads.

By logging into ATS-P, authorized CBP and DHS personnel can access information from the various source systems on passengers who have arrived in and/or departed from the U.S. ATS-P allows users to query other available federal government systems as well as publicly available information on the Internet through the user interface. In addition, ATS-P maintains a

copy of information from the following systems: APIS, I-94, NIIS, ESTA, BCI, TECS secondary processing, seizure and enforcement data as well as Suspect and Violator Indices (SAVI), TSDB via the Watchlist Service, and DoS's CCD to identify individuals requiring additional screening prior to entering or exiting the country.

In addition to the above, ATS-P permits specifically authorized DHS users to access PNR obtained from airlines or their travel reservation systems through the Airline Reservation Monitoring System (ResMon). ResMon interfaces with the airline reservation systems, allowing the airline reservation system to push PNR to CBP or, for certain carriers, allowing CBP to pull PNR based on a set schedule. ResMon also allows authorized CBP personnel to pull data in certain circumstances on an *ad hoc* basis, with supervisory approval, to ensure CBP has received the latest available information on specific high-risk travelers or flights.

Through the ATS-P web interface, authorized CBP personnel can create *ad hoc* queries on selected enforcement data, arrival and departure information, travel reservation information, visa and ESTA applications and secondary referrals. Additionally, the ATS-P web interface may be displayed on approved mobile devices to support officer activities in the context of the Immigration Advisory Program (IAP) and at the ports of entry.

5) ATS-Targeting Framework (ATS-TF)

A limited number of ATS users use the Targeting Framework (TF) to track information of targeting interest regarding passengers and cargo. The TF permits a user to search across the data sources available in the other modules of ATS based on role-based access for research and analysis purposes. If the user does not have access to the data, the search will not return any data. Information from these queries can be shared with other ATS-TF users. For example, a user at the NTC could quickly search relevant data maintained in ATS for information regarding a person of interest detained at a port of entry, and then provide the research to the port of entry. The ATS-TF provides the user with the ability to initiate research activities, fosters collaboration among analysts, and allows all users to use past activity logs as additional intelligence sources by tracking past research activity with respect to persons and entities of interest. The ATS-TF includes workflow functionality, which allows authorized users to assign activities to other users, operating units, or ports of entry for additional processing. The ATS-TF allows the creation of projects, which track information intended for use over long periods of time, or operational and analytical reports that may include public source information obtained by users for reference or incorporation into the report or project. Through the ATS-TF web interface, authorized CBP personnel can create *ad hoc* queries that allow users to find information related to a specific activity or entity contained within each activity. The ATS-TF allows users to integrate data from multiple sources and show possible relationships between entities and data elements.

Users in ATS-TF may, subject to their access permissions, query the other four modules of ATS (ATS-AT, ATS-N, ATS-L, and ATS-P) and other systems, including but not limited to those noted below, and save the results:

- Border Patrol Enforcement Tracking System - Significant Incident Report (BPETS-SIR) Module - managed by CBP
- CCD - managed by Department of State
- Commercial data aggregators
- EID - managed by ICE
- eGIS - managed by CBP
- ICE PDF Forms Generator - managed by ICE
- Social Security Administration Death Master File - managed by SSA. A copy of this file is kept in ATS-TF.
- DHS IDENT and FBI IAFIS provided through Web-IDENT - managed by ICE or E3 Biometrics - managed by CBP
- Watchlist Service - managed by DHS
- TECS - managed by CBP

The ATS-TF allows authorized users to attach public source information, such as responsive Internet links and related documents, to an assigned report and/or project and search for any text contained within the system via full text search functionality. The ATS-TF also includes sophisticated *ad hoc* reporting features for both system data and workflow metrics as well as initial reporting features through data warehouse capabilities.

The ATS-TF is made up of multiple sub-systems with distinct user interfaces specific to each user community. Each sub-system has access to all or a subset of the external data sources listed above.

- NTC interface for NTC-P, NTC-C, Port of Entry Targeting Units, and U.S. Consulates and Embassies
- Border Patrol and Intelligence Reporting System (IRS) interface for Office of Border Patrol (OBP) and Office of Air and Marine (OAM)
- Intel interface for Office of Intelligence and Investigative Liaison (OIIL)
- SIGMA interface for Office of Field Operations (OFO) users at Ports of Entry Secondary Operations
- Enforcement Link Mobile Operations – Passenger and Cargo interfaces for OFO users at Immigration Advisory Program (IAP) locations and Inbound/Outbound operations at Ports of Entry, as well as OBP users at Border Patrol Sectors
- Fraudulent Document Analysis Unit (FDAU) interface for OFO users
- Admissibility Review Office (ARO) interface for OFO users

Accessing ATS

All ATS databases and web resources are located in the National Data Center (NDC) and/or the DHS Data Centers. ATS is accessed through a web-based user interface, which enables authorized users to generate queries against ATS data on the appropriate database servers. End users communicate with web servers over the DHS infrastructure or remotely through secure encrypted devices with one-factor authentication. ATS-P is also accessible through secure-encrypted mobile devices for certain CBP officers in foreign locations and at Ports of Entry. Access to ATS is limited to those individuals with a need to know in order to carry out their official duties. Furthermore, access to specific data sets within ATS is further controlled by providing each user only those accesses required to perform his or her job. Each user's access to ATS is reviewed twice a year by the supervisor who authorized the role. Within ATS, audit trails of what information has been accessed by whom are maintained and used to support internal audits to ensure compliance with the stated purposes of the system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

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).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CBP is publishing a newly updated SORN in the Federal Register to reflect the revision and expansion of ATS and to cover the official records maintained by ATS. The information contained in the source systems performing the original collection that ATS ingests from or provides a pointer to is covered by the individual SORNs of those systems as listed in Appendix D.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A system security plan for ATS was completed and an Authority to Operate (ATO) was granted to ATS for three years, on January 21, 2011. ATS has a FIPS 199 categorization of Confidentiality "MEDIUM," Integrity "MEDIUM" and Availability "MEDIUM." ATS processes, transmits and stores PII data.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. Official Records (Passenger Name Records (PNR) collected under 49 U.S.C § 44909; Importer Security Filings (10+2 documentation); results of Cargo Enforcement Exams; the combination of license plate, Department of Motor vehicle registration data, and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department) in this system will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008 and for certain PNR, the 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, signed in December 2011. ATS collects information directly, ingests information from various systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data are retained in ATS in accordance with the record retention requirements of those systems, or the retention period for ATS, whichever is shortest.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information contained in ATS is not covered by the Paperwork Reduction Act because ATS does not collect any information directly from the public through any paper forms. ATS does collect information from other systems, however, which in turn collect information from the public using various customs, immigration, agricultural, and admissibility forms.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

ATS collects, uses, disseminates, or maintains the following information in the following modules:

ATS-AT sub-system evaluates export information, including information which is filed electronically with AES. The export data are sorted, compared to rules, and scored so that CBP officers can identify exports with aviation safety and security risks, such as FAA violations. ATS-AT also identifies the risk of exports for such violations as smuggled currency, illegal narcotics,

dual use technology, export licencing, and other contraband. ATS-AT not only screens commodity information on export documents, but also screens individuals identified on those documents.

ATS-AT may collect and store PII and data, including but not limited to the following:

- Exporter:
  - Tax ID (EIN or SSN)
  - First Name
  - Last Name
  - Address
  - City
  - State
  - Zip Code
  - Phone Number
- Office of Defense Trade Controls Registrant:
  - First Name
  - Last Name
  - Address
  - City
  - State
  - Zip Code
  - Phone Number
  - License Country
  - License Number
- Commodity:
  - VIN
  - Title State
  - Title ID
  - Bills of lading
  - Cargo manifest information (including quantity and description)

ATS-N may collect and store PII and data about incoming cargo, including but not limited to:

- Bills of lading
- Entries and importer security filings (See Appendix B for a complete listing of the ISF data elements), which identify parties in transaction by name
- Simplified entry information, including:
  - Importer of record number
  - Buyer name and address
  - Buyer Employer Identification Number
  - Seller name and address
  - Manufacturer/supplier name and address
  - Harmonized Tariff Schedule 10 digit number
  - Country of origin
  - Bill of lading/house air waybill number
  - Bill of lading issuer code
  - Entry number
  - Entry type
  - Estimated shipment value
- Tax ID (Employer Identification Number (EIN) or Social Security Number (SSN)), address and contact information including telephone and fax numbers.
- Conveyance crew information, including:
  - Name
  - Date of Birth
  - Address
  - SSN
  - Drivers License
  - Passport Numbers
- User information, including CBP internal contact information and SSN, which is masked.
- Inspection and exam results, including a narrative that can include information about the parties involved.
- Targeting information and rules that include law enforcement data about parties including name, tax ID (EIN or SSN), and address.

ATS-L accesses several external data sources for targeting at the land border. These external data sources include Nlets, NCIC, CCD, and SEVIS. The ATS-L system stores vehicle registration and biographical information collected through vehicle primary inspection. ATS-L collects and stores PII about the registered owner of the vehicle and the occupants, including but not limited to:

- Name (first and last)
- Date of birth (if available)
- Vehicle identification number (VIN) along with year, make, and model information and other vehicle registration data
- Registered owner's address
- Travel Document type and number, issue date, city, state, country

ATS-P may collect and store PII, including but not limited to the following:

- Name
- Alias
- Address
- Phone number
- Email
- License Registration
- Date of Birth
- Country of citizenship
- Country of birth
- Payment/Billing information (e.g., Credit Card or Debit Card Numbers as available)
- Gender
- Travel Document type and number, issue date, city, state, country
- Visa type and number, issue date and location
- Employment occupation code
- Fingerprint Number (FIN), where available
- Person's Physical Characteristics (height, weight, eye color, hair color, etc.)
- PNR (See appendix A for a complete PNR listing)
- SSN when provided by source system

- PII associated with targeting results or data obtained in accordance with the terms of a memorandum of understanding or other arrangement
- Ethnicity and/or Race (TECS), based on CBP officer reporting in the secondary TECS record and only if available
- Biographical and biometric information from or associated with online immigrant and non-immigrant VISA and ESTA applications, including (as available):
  - U.S. sponsor's name, address, and phone number
  - U.S. contact name, address, and phone number
  - Employer name, address, and phone number
  - E-mail address, IP address, applicant ID
  - Marital status
  - Alien number
  - SSN
  - Travel Document type and number, issue date, city, state, country
  - Tax Identification Number
  - Organization Name
  - U.S. status
  - Income information for joint sponsors
  - Education, military experience, relationship information
  - Responses to vetting questions pertaining to admissibility or eligibility

Targeting Framework may collect and store PII, including but not limited to the following:

- Name
- Address
- Alias
- Business
- Cargo information (export cargo, import cargo, express consignment with associated trade entity information)
- Country of Citizenship
- Country of Residence
- Date of Birth

- Disposition (assigned by CBP officer or agent)
- Employment Information
- PII derived from an ESTA or VISA application
- IP address
- Travel Itinerary
- Personal Identifier (marks, scars, tattoos, etc.)
- Person Type (assigned by CBP Officer or Agent)
- Place of Birth
- Property Information
- Record ID (assigned by FBI, DHS, CBP, or other agency)
- Relatives
- Remarks (entered by CBP officer or agent)
- SSN when provided by source system
- Seizure Entity
- Conveyance
- TECS lookout information
- Travel Document type and number, issue date, city, state, country
- Visa type and number, issue date and location
- Public source (e.g., Internet) information obtained by users/analysts for reference or incorporation into operational and analytical reports and/or projects

Data Manually Processed: ATS is used to manually process certain datasets to identify national security and public safety concerns and correlate records. Currently, DHS conducts this process for those records in Arrival and Departure Information that have been identified as individuals who may have overstayed their permitted time in the United States.[2] Appendix D will be updated as necessary.

[2] DHS/All/PIA-041 One DHS Overstay Vetting Pilot published December 29, 2011.

2.2 What are the sources of the information and how is the information collected for the project?

ATS does not collect information directly from individuals, but rather ingests or accesses and uses information collected, generated, and stored by and in other systems. As described in section 1.2 above, ATS ingests information from the systems of records identified in section 1.2, provides a pointer to data in other systems, queries databases, and may receive data in accordance with certain cooperative arrangements with foreign governments. Additionally, some of the information maintained in ATS is created by ATS users.

The data ATS ingests comes from systems, including the following: ACE, ACS, ADIS, AES, APIS, BCI, CCD, CEAC (including Forms DS-160 and DS-260), ENFORCE, ESTA, GES, NIIS, NSEERS, SEACATS, SEVIS, TECS, TSDB-WLS, and Social Security Administration's Death Master File. Additionally, PNR collected under 49 U.S.C. § 44909 is obtained from travel reservation systems of commercial carriers. Information from Importer Security Filings is received from importers and ocean carriers. Simplified entry information is obtained from importers or brokers through ABI.

Records are accessed from BPETS, CCD, eGIS, NCIC, WebIDENT, and Nlets. Also, the results of queries in the FBI's Interstate Identification Index (III), the National Insurance Crime Bureau's private database of stolen vehicles, and commercial data aggregators are stored in ATS. ATS receives commercial data about persons and businesses as part of the analysis process for researching individuals and cargo requiring additional screening from commercial data aggregators. ATS also collects air waybill data from certain express consignment services in conjunction with specific cooperative programs.

Reports and/or projects developed in ATS-TF are created by authorized users and may include public source and/or law enforcement sensitive information uploaded by the user. Additionally, ATS records results of Cargo Enforcement Exams input by the CBP officer.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ATS collects PNR data directly from commercial carriers pursuant to CBP's statutory authority, 49 U.S.C. § 44909, as implemented by 19 C.F.R. 122.49d. PNR is used in conjunction with other data noted above to identify individuals requiring additional screening prior to entering the country.

ATS also collects air waybill data from certain express consignment services and other air cargo transportation providers in conjunction with specific cooperative programs.

ATS-TF uses commercial data aggregators, which provide commercial data about persons and businesses, as part of the analysis process for researching individuals and cargo requiring additional screening. ATS-TF and ATS-P users may also upload public source

information such as Internet links and documents in ATS-TF. This data are used to cross-check, confirm, and broaden the scope of information available to the user.

2.4 Discuss how accuracy of the data is ensured.

ATS relies upon the source systems listed in 2.2 to ensure that data used by ATS is accurate and complete. Discrepancies may be identified in the context of a CBP officer's review of the data, and CBP officers are required by policy to take action to correct the data if they become aware of inaccurate data, when appropriate. For PNR, CBP officers may become aware of inaccuracies due to correction, rectification or redress procedures available to travelers, including non-U.S. persons. Although ATS is not the system of record for most of the source data, ATS receives updates with any changes to the source system databases. Continuous source system updates occur in real-time or near real-time. When corrections are made to data in source systems, ATS updates this information immediately and only the latest data are used. In this way, ATS integrates all updated data (including accuracy updates) in as close to real-time as possible.

To the extent information that is obtained from another government source (for example, vehicle registration data that is obtained through Nlets) is determined to be inaccurate, this problem would be communicated to the appropriate government source by the CBP officer for remedial action.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk:

ATS aggregates data from many systems, which may exceed the minimal amount necessary to achieve its missions.

Mitigation:

The nature of CBP's mission to provide effective risk management at the border requires ATS to collect any relevant information. To mitigate the risks posed in the collection of large amounts of data, CBP has imposed strict controls to maximize the security of the information that is being stored. Officers rely on data to make accurate determinations and are trained to identify inaccurate information. Data are kept in secure areas protected by armed guards. Access to ATS records is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Privacy Risk:

Information about two different individuals with similar names and dates of birth could be mischaracterized as the same individual, thus attributing the wrong information to the wrong individual.

Mitigation:

DHS personnel are required to review and cross reference the records in ATS to improve the level of confidence and reliability in derogatory information before any action is taken against an individual.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

ATS-AT collects and stores the information described in 2.1, such as, exporter's name, SSN, address, and phone number to evaluate export data, including Electronic Export Information (EEI) (previously known as the Shippers Export Declaration (SED)), which is filed electronically with AES. The export data are sorted, compared to rules, and scored so that CBP officers can identify exports with transportation safety and security risks, such as FAA violations, as well as exports which may pose a risk for violation of U.S. law.

ATS-N collects and stores information described in 2.1, such as, bills of lading, entries, simplified entries, and importer security filings, which identify parties by name, tax ID (EIN or SSN), address, and contact information including telephone and fax numbers. ATS-N also leverages conveyance crew information, including name, date of birth, address, SSN (if provided), driver's license, and passport number to assist in the risk assessment of import cargo shipments aboard the conveyance. ATS-N helps to identify and select import cargo shipments that appear to have a higher likelihood of being associated with terrorism or possibly containing implements of terrorism, narcotics or other contraband in the sea, air (including mail and express mail), rail and truck modes of transportation.

ATS-L collects and stores information described in 2.1, such as, vehicle registration numbers and contact information, name, address, and travel document information for land border controls. ATS-L then parses the vehicle registration information and stores it into the ATS-L database for historical purposes and sends back the parsed results to the land border primary officers. The information sent includes vehicle registration (year, make, model, and VIN) as well as registered owner information (first name, last name, date of birth, if available, and address) for U.S.-plated vehicles.

ATS-P collects and stores information described in 2.1, such as name, address, date of birth, payment/billing information (such as credit card or debit card numbers), and passport number from the PNR, for risk assessment purposes. ATS-P augments the CBP officer's decision-making process about whether a traveler or crew member should receive additional screening. ATS-P provides an automated solution that allows CBP personnel to focus efforts on potentially high-risk travelers by eliminating labor-intensive manual comparison of traveler information or interviews with every traveler. Additionally, ATS-P receives online visa application data to provide pre-adjudication investigative screening to DoS for non-immigrant

and immigrant visa appications. ATS-P receives ESTA application data to identify potential high risk ESTA applicants. ATS-P receives ADIS data to identify potential overstay candidate leads.

ATS-TF collects and stores information described in 2.1, such as, name, SSN, address, date of birth, business, country of citizenship, country of residence, employment information, unique physical attributes (marks, scars, tattoos, etc.), and travel itinerary to authenticate travelers and cargo. CBP records in ATS-TF information on individuals and cargo that are of targeting interest.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. ATS builds a risk-based assessment for cargo and conveyances based on criteria and rules developed by CBP. ATS maintains the assessment results from rules together with a record of which rules were used to develop the assessment results. With regard to travelers, ATS identifies persons whose information matches criteria comprising a targeting rule. This initial match and any subsequent matches are reviewed by CBP officers to confirm continued official interest in the identified person. It is worth clarifying, however, that only the ATS components pertaining to cargo or conveyances rely on rules-based targeting to build a score for the cargo or conveyance to subsequently identify cargo and/or conveyances of interest. Persons associated with cargo shipments are screened against TECS lookouts and prior law enforcement actions to permit any identified violations to be considered as part of the overall score. Travelers identified by risk-based targeting scenarios are not assigned scores.

ATS rules and assessment results from rules are designed to signal to CBP officers that further inspection of a person, shipment, or conveyance may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise be noted as a person of concern to law enforcement. ATS-TF is a workflow and reporting function that separately allows users to track assessment results from rules and create various reports permitting a more comprehensive analysis of CBP's enforcement efforts.

ATS risk assessments are always based on predicated and contextual information. As noted above, unlike in the cargo and conveyance environments, ATS traveler risk assessments do not use a score to determine an individual's risk level; instead, it compares PII described above against lookouts and patterns of suspicious activity identified through past investigations and intelligence. This analysis is done in advance of a traveler's arrival in or departure from the United States and becomes one tool available to DHS officers in identifying illegal activity.

3.3 Are there other components with assigned roles and responsibilities within the system?

The principal users of ATS data are within DHS and CBP, including:

- CBP Office of Field Operations (OFO)
- CBP Office of Border Patrol (OBP)
- CBP Office of Air and Marine (OAM)
- CBP Office of Intelligence and Investigative Liaison (OIIL)
- CBP National Targeting Center (NTC)
- CBP Office of International Trade (OT)
- CBP Office of Internal Affairs (IA)
- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Citizenship and Immigration Services (CIS)
- DHS Office of Inspector General (OIG)
- DHS Office of Intelligence & Analysis (I&A)
- United States Coast Guard (USCG)
- Transportation Security Administration (TSA)

The information collected through ATS may be shared with components within DHS on a need to know basis consistent with the component's mission pursuant to section 552a(b)(1) of the Privacy Act. Access to ATS is role-based and assigned according to the mission of the component and the user's need to know. Furthermore, access to specific data sets within ATS is further controlled by providing each user only those accesses required to perform his or her job.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk:

Authorized users of ATS could utilize their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation:

All ATS users must undergo privacy training and obtain approval from their supervisor and the ATS system owner before gaining access to ATS. ATS performs extensive auditing that records the search activities of all users. These audit logs are reviewed upon request and any inappropriate use will be referred to the appropriate internal investigations (such as Internal Affairs, the Joint Intake Center, or others as required) for handling. The detection of inappropriate

use will also result in the suspension of the user's access to ATS until the use can be investigated. ATS auditing capabilities are discussed in greater depth later in this document.

Audit trails are created throughout the process and are reviewed if a problem or concern arises regarding the use or misuse of the information. During the log-in process, the account owner must acknowledge his/her consent to monitoring for inappropriate use or he/she cannot access the system.

Additionally, ATS has role-based access which is restricted based on a demonstrated need to know. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. CBP officers with access to ATS are required to complete annual security and data privacy training and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

Privacy Risk:

One potential risk to individuals from the use of ATS is that a traveler, conveyance, or cargo in which an individual has an interest may be referred to secondary inspection even though that traveler, conveyance, or cargo does not present any risk of harm to the United States and has not committed or been associated with any violation of U.S. law.

Mitigation:

Referral to secondary inspection, as necessary, permits an officer to intercede and resolve mis-identifications, and to clarify information associated with an individual's travel document records. Determinations in secondary regarding admissibility are made by a CBP officer or supervisor. Secondary processing is a necessary component of CBP's admissibility determination for each person arriving in the United States when admissibility cannot be determined at primary inspection. Generally, other than random referrals employed periodically as an internal control to ensure consistent procedures, decisions to refer travelers to secondary inspection are made by a CBP Officer. As a decision support system, ATS operates according to the rules within the system that were created in parallel with the policies and procedures governing the CBP inspection process. The review, analysis, and training of the officer making a decision regarding admissibility at secondary inspection provides the greatest mitigation to the risk that information in ATS may be improperly obtained or inappropriately accessed or used.

Likewise, all cargo shipments arriving in or exported from the United States are subject to further review or physical inspection to determine that the shipment poses no threat and that the shipment is in compliance with all applicable U.S. laws and regulations. This data review or physical inspection of the cargo shipment serves a similar function in allowing CBP or other applicable regulatory agency to determine that no violation has occurred.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

ATS does not collect any information directly from individuals. ATS does collect and maintain PNR data derived from commercial carrier reservation/departure control systems, as indicated in the SORN for ATS published at the same time as this PIA in the Federal Register and discussed above at paragraph 1.1. DHS provides extensive notice about its use of PNR on both the CBP and DHS Privacy Office websites. In addition, airlines provide general notification about their obligation to report PNR in the contract of carriage.

In cases where an individual has a concern during an interaction with a CBP officer, the CBP officer may provide the individual with a copy of the fact sheet, "If You Experience Problems With Your Arrival in the U.S." (See Appendix C), which provides general information concerning CBP's border enforcement mission and responsibilities and specific information concerning where to direct inquiries about CBP's actions or the information collected. In addition, travelers may also contact DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

Most of the information that ATS uses is collected from government data sources. Notice was provided through the applicable source SORNs and PIAs (where applicable), as well as through the publication of the laws and regulations authorizing the collection of such information. This information is collected and stored in the source systems of record, is collected for compatible purposes, and would be collected with or without ATS. See Appendix D for listing of the relevant SORNs.

This information is collected by CBP primarily for law enforcement purposes related to the entry and exit from the United States of people, cargo, and conveyances; use of this data also facilitates legitimate trade and travel.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Generally, the decision whether to travel to or from, or to import and/or export goods/merchandise into or out of the United States is within the discretion of the individual. United States law requires individuals seeking to enter the country to identify themselves and

demonstrate admissibility to the United States; likewise, persons seeking to import or export goods and merchandise into or out of the United States are required to provide certain information to allow CBP to determine whether the goods/merchandise may enter the United States, and are in compliance with relevant export requirements, as applicable.

ATS does not require individuals to provide information beyond that authorized by law. This information is captured by the source systems (e.g., AES, ACS and/or ACE, and TECS) and used by ATS to efficiently and expeditiously identify persons, conveyances, and cargo that may pose a concern to law enforcement, resulting in further review by appropriate government officers.

While ATS does not collect information directly from individuals, it employs information obtained from persons by these source systems. The only way an individual can decline to provide information is to refrain from traveling to, from, through, or over the United States or by not bringing in, shipping, or mailing any goods/merchandise to, through, or from the United States.

Any consent individuals may grant is controlled by the source systems described in earlier sections. Because the submission of information is required in order to travel to, from, through, or over the United States or to bring in, ship, or mail any goods/merchandise to, through, or from the United States, restrictions on CBP use and sharing of accessed information are limited by legal requirements set forth in the Privacy Act, the Trade Secrets Act, the uses published in SORNs and, for certain PNR, the U.S.-EU Passenger Name Record Agreement. Consent to store or use this information must be done in accordance with the above legal requirements.

Opportunities for individuals to consent to particular uses of information are addressed using the processes defined by the source systems. As most information collected by these systems is mandated by law, there is effectively no consent mechanism other than the choice whether to travel or ship items.

Many commercial carriers have provided their own notice to customers concerning the requirement to provide PNR.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk:

There is a risk that the individual may not know that the information is being used by ATS in the ways described.

Mitigation:

CBP has published the SORN for ATS and this PIA (as well as previous versions) to increase transparency of its operations. Regarding PNR, CBP and DHS have provided information via the DHS Privacy and CBP websites and other mechanisms to effectively notify the traveling public. Additionally, CBP and DHS have drafted language regarding PNR for commercial carriers to include in their privacy statements so as to provide further transparency.

Many air carriers have provided their own notice to customers concerning the uses and transmission of PNR.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

Official Records (including PNR collected under 49 U.S.C. § 44909; Importer Security Filings (10+2 documentation); results of Cargo Enforcement Exams; the combination of license plate, Department of Motor vehicle registration data, and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department) in this system will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008. ATS collects information directly, ingests information from various other systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data are retained in ATS in accordance with the record retention requirements of those systems, or the retention period for ATS, whichever is shortest.

The retention period for the official records maintained in ATS will not exceed 15 years, after which time the records will be deleted, except as noted below. The retention period for PNR will be subject to the following further access restrictions and masking requirements: ATS users with PNR access will have access to PNR in an active database for up to five years, with the PNR depersonalized and masked after the first six months of this period. 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. Within the dormant database, PNR will be accessible for criminal matters for up to five years but will remain available for counter-terrorism purposes for the full duration of its 15-year retention. PNR in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be repersonalized in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers. Notwithstanding the foregoing, information maintained only in ATS that is linked to a specific case or investigation will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

The justification for a 15-year retention period for the official records is based on CBP's law enforcement and security functions at the border. This retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that

potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Travel records, including historical records, are essential in assisting CBP Officers with their risk-based assessments of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing these records for these purposes allows CBP to continue to effectively identify suspect travel patterns and irregularities.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk:

Data may be retained too long.

Mitigation:

ATS retains data according to the SORN requirements of the system from which the data was obtained. PNR is retained for five years in an active state and ten years in a dormant state. However, users will only be able to view the PII in PNR for six months. After six months PII will be masked and require each user to obtain supervisory approval before unmasking the PII. All of these accesses are logged and reviewed to ensure compliance. These retention periods permit CBP to perform the necessary assessment results from rules, because much of the targeting environment relies upon historical data. Acknowledging the changing nature of the targeting environment and the sensitivity of the data, CBP archives data after the prescribed period to further protect data that may not be immediately required, but may become relevant within the retention period.

ATS maintains the assessment results from rules together with a record of which rules were used to develop the risk assessment. This assessment and related rules history associated with developing assessment results from rules are maintained for up to fifteen years to support ongoing targeting requirements. Notwithstanding this limitation, information maintained in ATS that is linked to an active law enforcement matter will be retained for the duration of that law enforcement matter.

Nonetheless, the touchstone for data retention is the data's relevance and utility. Accordingly, CBP will regularly review the retention period for ATS to ensure its continued relevance and usefulness. If these reviews demonstrate that certain data is no longer relevant and useful, CBP will revise the retention period and delete the information.

All assessment results from rules need to be maintained because assessment results from rules for individuals who are deemed low risk will be relevant if their risk attributes change in the future, for example, if new terrorist associations are identified. Additionally, certain data maintained by ATS may be subject to shorter retention limitations pursuant to separate arrangements. The adoption of shorter retention periods may not be publicly disclosed if DHS concludes that disclosure would affect operational security.

Privacy Risk:

ATS may retain data longer than the source system.

Mitigation:

In general, ATS has implemented controls that delete data in ATS if such data are deleted in the source system. For data that has been identified by a CBP Officer in ATS as having law enforcement relevance, the record may be maintained longer than allowed for in the source system. In the relevant retention schedules of the source systems, DHS has allowed for the retention of records of law enforcement relevance.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to DHS. External sharing encompasses sharing with other federal, state, and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Non-DHS requesters may only access information in the various modules of ATS if there is a specific information sharing arrangement in place between DHS and the outside entity. Each arrangement defines the nature of the outside access to or sharing of ATS information, including the scope of the ATS information being access or shared and the legal basis upon which they receive it. Depending on the information sharing arrangement, the non-DHS requesters may be provided direct access to ATS and in other instances the non-DHS requester may be provided access through a CBP/DHS user of ATS, as described below.

CBP provides varied levels of access to ATS-N for imported commodities to the following:

- Air cargo transportation providers including express consignment carriers receive access to receipt acknowledgments from CBP regarding document review and official government cargo hold messages from users of ATS.
- Consumer Product Safety Commission and other members of the CBP hosted Commercial Targeting and Analysis Center (CTAC) receive direct system access to cargo and commodity targeting information pertaining to import safety to fulfill the targeting mandate of the Consumer Product Safety Improvement Act of 2008, and other import safety statutes.

CBP may provide the results of passenger screenings to the following:

- Various law enforcement task forces outside of DHS that require queries to be run against ATS data (for example, the FBI-led Joint Terrorism Task Force) in response to a specific threat or to analyze specific travel routes of concern.
- Law enforcement and counterterrorism agencies, in response to direct requests and authorized releases.

- National Counterterrorism Center (NCTC) in the event that the National Targeting Center-Passenger (NTC-P) nominates an individual for inclusion within the TSDB.
- Terrorist Screening Center (TSC) – Interface (DHS data transfer) for Outbound departures where there is a potential match to the TSDB.
- Other domestic and foreign agencies consistent with the published Routine Uses in the SORN.

CBP provides online visa application pre-adjudication investigative screening results to DoS, including justification for the determination.

ATS allows all users, including non-DHS users, to access source system data consistent with their user roles. In some instances users have less access through ATS than their direct access to the source system. Agencies with this type of access include:

- Department of Justice (Federal Bureau of Investigation, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms, and Explosives)
- Department of State (Diplomatic Security and Consular Affairs)
- U.S. Department of Commerce (Bureau of Industry and Security)
- U.S. Department of Agriculture (this access includes viewing of specific USDA rule sets and assessment results from rules)
- Department of Health and Human Services (U.S. Food and Drug Administration FDA) (limited to FDA personnel working at NTC in support of FDA Prior Notice requirements)
- United States Postal Service

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As stated in section 1.2 of this document, the Privacy Act SORN that applies to ATS was revised and expanded in conjunction with this PIA. In updating the ATS SORN, DHS reviewed it to ensure that the sharing described above is compatible with the purpose of the system.

6.3 Does the project place limitations on re-dissemination?

External users of ATS must meet the terms and conditions of the arrangements permitting their access to ATS in order to obtain and maintain access. Generally, CBP requires that the external users employ the same or similar security and safeguarding precautions as employed by CBP and only use the data for legitimate purposes. For CBP, ATS has role-based security. Users from other government organizations must use the ATS interface to access the system where access is limited via a user profile/role. ATS user roles are highly restricted and audited. Application access is restricted in the form of role based access, which is based on a demonstrated need to know. Users may not re-disseminate information without prior express written consent by CBP.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Information shared outside of the Department is tracked through the use of the DHS-191, Accounting of Disclosure Form, or a Memorandum of Understanding (MOU). CBP and DHS users of ATS prepare a DHS-191 form each time they share PII from ATS outside of DHS. The ATS-P module automatically generates an electronic copy of the DHS-191 in each instance of sharing when PNR data are shared from ATS. CBP and DHS share information from ATS pursuant to the terms of an arrangement for access to one or more of the modules of ATS, or in accordance with the language of a letter of authorization, which facilitates the sharing of a limited number of records from ATS in response to a request for assistance from another law enforcement agency.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk:

Information may be shared under inappropriate circumstances.

Mitigation:

Risks related to sharing of information outside DHS, including any potential risk of further dissemination of information by the external agency to a third agency, are mitigated through arrangements governing access to ATS by external parties and sharing of ATS information with external parties. Each arrangement defines the nature of the outside access to or sharing of ATS information, including the scope of the ATS information being accessed or shared and the legal basis upon which they receive it. The arrangements generally require the external party accessing or receiving information to employ measures relating to security, privacy, and safeguarding of information that are equivalent or comparable to measures employed by DHS. As a general matter, the arrangements also stipulate that any further dissemination of ATS information by the receiving party to a third party is subject to prior authorization by CBP. Lastly, CBP emphasizes that, within each arrangement, each external user is provided with training designed to ensure that data accessed through ATS is safeguarded and secured in an appropriate manner and that dissemination restrictions are observed, consistent with applicable laws and policies.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress, which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place. To the extent that a record is exempted in a source system, the exemption will continue to apply. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: PNR collected pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler, regardless of his or her citizenship or residence, may obtain access to his or her PNR, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information will not be accessible to the individual.

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP in accordance with procedures and points of contact published in the applicable SORN.

Procedures for individuals to gain access to data maintained in source systems that provide data ingested into ATS would be covered by the respective SORNs for the source systems. Individuals may follow the procedures outlined in the PIAs and SORNs of the source systems to gain access to their information stored in those systems.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

U.S. Customs and Border Protection
FOIA Division
799 9th Street NW, Mint Annex
Washington, DC 20229-1177

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under *contacts*.

While DHS has exempted ATS from the access and amendment provisions of the Privacy Act, individuals may make a request to view their records. When seeking records about oneself from ATS or any other CBP system of records, the request must conform to the Privacy Act regulations set forth in 6 CFR part 5. An individual must first verify their identity, meaning that they must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov/foia or 1–866–431–0486. In addition, the following should be provided:

- An explanation of why the individual believes DHS would have information on them,
- Details outlining when they believe the records would have been created, and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

Without this bulleted information, CBP may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
OPA—Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Avenue
Washington, DC 20229

Travelers may also contact DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

As many of the records used by ATS come from TECS, CBP has instituted an Officer-initiated function in TECS to address certain issues pertaining to some records that may contain conflicting information. This function is referred to as the Primary Lookout Override (PLOR) function. The PLOR function was developed to assist travelers who are erroneously designated for secondary inspections because they possess a characteristic similar to a person of interest. PLOR allows CBP Officers to override certain TECS Records where a similar biographical trait exists between the traveler and another person who is the subject of a TECS Record, provided that the non-subject traveler is able to provide a unique characteristic that differentiates him or her from the person of interest. The PLOR procedures require supervisory approval before a PLOR record may become active. All such amended transactions are logged by TECS and attributed to the authorized user performing the correction. This includes any required supervisory approval.

7.3 How does the project notify individuals about the procedures for correcting their information?

Upon request, CBP officers will provide the fact sheet, "If You Experience Problems With Your Arrival in the U.S.," that provides information on appropriate redress (See Appendix C). The redress procedure provides the ability to correct data in the source systems, including ATS. Additional information is available on DHS's website. The source system SORNs also provide information on accessing and amending information collected through those systems as discussed in 7.1 and 7.2, above.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals may not get the level of redress they desire.

Mitigation: Redress procedures allow for correction of individual-provided data.

As set forth in the SORN published in conjunction with this PIA, DHS has exempted portions of ATS from the access, amendment, and certain accounting provisions of the Privacy Act (specifically 5 U.S.C. §§ 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I); (e)(5), and (8); (f) and (g)) pursuant to 5 U.S.C. §§ 552a (j)(2). Additionally, DHS has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. §§ 552a(k)(1) and (k)(2): 5 U.S.C. §§ 552a(c)(3); (d)(1), (2), (3), and (4); (e)(1), (e)(4)(G) through (I); and (f). DHS and CBP, however, will consider each request for access to records maintained in ATS to determine whether or not information may be released. Also, as noted above in paragraph 7.1, individuals may, pursuant to the FOIA, seek access to information for which ATS is the source system or which originates from another government source system and as a matter of CBP policy, redress may also be requested in the manner described above in paragraph 7.2.

However, individuals, regardless of nationality, country of origin or place of residence who believe their PNR has been used in an inappropriate manner may seek redress, including but not limited to, through the DHS Traveler Redress Inquiry Program.

Additionally, DHS Privacy Office published guidance on February 11, 2011 specifically on identifying, processing, tracking, and reporting on requests for amendment to records submitted to DHS under the Privacy Act.[3]

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The controls in place to ensure that information is handled in accordance with the above described uses include:

Misuse or Breach of ATS: ATS has role-based access. All user groups will have access to the system defined by the specific user's profile and limited through reference to the determined rights and responsibilities of each user. Access by users, managers, system administrators, developers, and others to the ATS data is defined in the same manner and employs profiles to tailor access to mission or operational functions. ATS user roles are highly restricted and audited. Access is restricted in the form of role based access, which is based on a demonstrated need to know. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. All ATS users with access to ATS are required to complete security and data privacy training on an annual basis and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

ATS is hosted at the NDC and/or the DHS Data Centers. Both are secure, access-controlled facilities with physical security and protective services 24 hours a day, 7 days a week. The computer room is further restricted to a controlled list of authorized individuals. The building floors are occupied by CBP personnel who are required to pass a security background investigation. No non-government system hosting is involved.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All ATS users are required to take annual security training such as the "CBP Sensitive Security Information," "CBP IT Security Incident Response Training," "CBP Safeguarding Classified National Security Information," and "CBP IT Security Awareness and Rules of Behavior Training" through the online DHS - Virtual Learning Center (VLC). Each of the VLC security trainings covers what constitutes PII and how to handle PII.

---

[3] *Privacy Policy Guidance Memorandum 2011-01*

The Targeting and Analysis Systems Program Office (TASPO) maintains a master list of all ATS users to ensure an accurate record.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

ATS user access is restricted in the form of role-based access assigned based on the user's role. Users cannot assign their roles to any other user, nor can they elevate their own rights within the system. User access is enforced by the user's role-based access, and roles are assigned only after supervisor request, process owner approval, and appropriate security checks have been confirmed.

Initial requests for access to the system are routed from the user through the supervisor to the System Administrator for processing. Need to know determinations are made at both the supervisor and Process Owner level. If validated, the request is passed on to the System Administrator. System Security Personnel are tasked to determine the user Background Investigation (BI) status. Once the BI is validated, the user's new profile changes are implemented. The user, supervisor, and Process Owner are notified via email that the request has been processed along with instructions for the initial login. These records are maintained by CBP. Profile modification requests follow the same process as for an initial request. If an individual has not used the system for more than 90 days, that individual's access will be denied and the same procedures as noted above must be completed to renew access. In addition, access is periodically reviewed by the Process Owner to ensure that only appropriate individuals have access to the system.

ATS user access is highly restricted and audited based on a demonstrated need to know. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Data are retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access the ATS web-based interface.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, and new access to the system by organizations within DHS and outside?

There are arrangements in place to govern access to or sharing of information from ATS. These agreements or arrangements are drafted by the business owners with input from the program managers. Arrangements that involve PII are sent to the CBP Privacy Officer for review and to DHS for final approval in accordance with procedures developed by the DHS Information Sharing Governance Board.

Responsible Officials

Laurence Castelli
CBP Privacy Officer
Office of International Trade
U.S. Customs and Border Protection
Department of Homeland Security

Thomas Bush
Executive Director
Targeting Division
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A: PNR Data Types

PNR may include the following types of information when available:*

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

*Not all carriers collect PNR and of those that do collect this data, not all collect the same sets of PNR data. Not all carriers maintain the same sets of information for PNR and an individual PNR is not likely to include information for all possible categories.

Appendix B: Importer Security Filing Data Elements

The Importer Security Filing (ISF) must contain the following items, in addition to the Vessel Stow Plan (VSP) and the Container Status Message (CSM):

1) Manufacturer (or supplier);

2) Seller (*i.e.*, full name and address or widely accepted business number such as a Data Universal Numbering System (DUNS) number);

3) Buyer (*i.e.*, full name and address);

4) Ship to party (full name and/or business name and address);

5) Container stuffing location;

6) Consolidator (stuffer);

7) Importer of record number/Foreign Trade Zone applicant identification number;

8) Consignee number(s);

9) Country of origin; and

10) Commodity Harmonized Tariff Schedule of the United States (HTSUS) number.

Alternatively, for shipments consisting entirely of Freight Remaining on Board (FROB) or shipments consisting of goods intended to move through the United States, ISF Importers, or their agents, must submit the following five elements, unless an element is specifically exempted:

1) Booking party (*i.e.*, name and address);

2) Foreign port of unlading;

3) Place of delivery;

4) Ship to party; and

5) Commodity HTSUS number.

Appendix C: Fact Sheet—"If You Experience Problems With Your Arrival in the U.S."

U.S. Customs and Border Protection

If You Experience Problems With Your Arrival in the U.S.

FACT SHEET

United States Customs and Border Protection (CBP) is an agency within the Department of Homeland Security. Our job is to keep America's borders safe and secure while encouraging legitimate travel and trade. We must keep terrorists and their weapons out of the country while enforcing hundreds of laws designed to protect our citizens, border, and commerce. To accomplish this, CBP officers must screen all arriving people, goods and vehicles to make sure they meet all requirements for entry into the United States.

Authority to search

The Congress of the United States has authorized CBP to enforce all homeland security-related laws and laws of other federal agencies at the border and to conduct searches and examinations necessary to assure compliance with those laws. CBP's broad authority therefore allows us to conduct searches of people and their baggage, cargo, and means of transportation entering the United States.

The laws and regulations we enforce include (but are not limited to):

- Admissibility of aliens
- Importation of agriculture, plant, and animal products
- Importation of goods, animals and produce
- Transportation and reporting of currency and other monetary instruments
- Exportation of weapons and items subject to defense trade controls

What to expect during a CBP examination

The CBP officer may request specific, detailed information about your travel, may inspect your baggage, or may conduct a personal search.

If you are subject to inspection, you should be treated in a courteous, dignified, and professional manner. However, please keep in mind that this is a law enforcement environment, and travelers who are intent on breaking the law will attempt to find out what the officer is doing in order to avoid detection. For this reason, our CBP officers may not answer specific questions about an examination that is underway. You may always ask to speak with a CBP supervisor.

Why you may be chosen for an inspection

You may be subjected to an inspection for a variety of reasons including but not limited to:

- Your travel documents are incomplete, or you do not have the proper documents or visa;
- You have previously violated one of the laws CBP enforces;
- You have a name that matches a person of interest in one of the government's enforcement databases; or
- You have been selected for a random search.

A search may not be made on any discriminatory basis (e.g., solely based on race, gender, religion, ethnic background).

Collection of personal information

CBP collects information about people traveling into and out of the United States. This includes basic biographic data, travel documents and their unique identifiers, where the traveler is staying in the U.S., and the planned purpose for the traveler's visit. This information may be collected from a traveler at a port of entry, or, in the case of international air and sea travel, it may be collected before a traveler's arrival in or departure from the U.S. This information is used to determine

For more information, visit the CBP.gov website or contact the Office of Public Affairs at 202–344–1770.

10/07

the admissibility of aliens and to effectively and efficiently enforce U.S. laws at the border. CBP also collects pertinent data about businesses, vehicles, aircraft, and vessels related to the laws we enforce.

CBP receives and shares this type of information as appropriate with other federal, state, and local agencies. CBP may query its record systems to ensure compliance with U.S. customs, immigration, agriculture, and other federal laws. For example, our border enforcement systems provide officers with access to information on outstanding watches and warrants; stolen vehicles, vessels or firearms; license information; criminal histories; and previous federal inspections.

Privacy protection

CBP stores all data we collect in secure computer systems on a secure network. CBP is committed to protecting travelers' personal data consistent with U.S. laws. We have privacy protections in place to properly safeguard this data. We also have policies in place to prevent misuse and those policies are regularly evaluated and updated to ensure continued security and protection.

Customer service contacts

1. Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP)

DHS TRIP provides a single point of contact for individuals who experience repeated referrals for security screenings or who believe that they have been denied boarding or entry into the United States because of inaccurate or incorrect information about them in law enforcement records, or because they have been confused with someone who is a concern to U.S. authorities. For more information on TRIP or to submit an inquiry, please see the DHS TRIP website at: http://www.dhs.gov/trip.

If you are uncertain as to the source of the information or the agency responsible for maintaining the information causing your travel concern, then you should begin your inquiry with DHS TRIP.

2. Customer Service Center

If you know you were stopped or delayed because of a previous incident involving CBP or one of its legacy components (Immigration and Naturalization Service, U.S. Border Patrol, or U.S. Customs Service) but believe that this matter should no longer be a factor in your clearing customs and immigration, you may ask CBP to review and possibly amend your records. If you want to ask why you were stopped, then you may ask CBP through its Customer Service Center.

CBP's Customer Service Center responds to travelers' general or specific questions or concerns about a CBP examination. You can contact us in one or three ways:

- **Telephone:** at or (877) 227-5511 for U.S. callers during the hours of 8:30 a.m. to 5:00 p.m. Eastern Time;
- **Online:** through the "Questions" tab at http://www.cbp.gov.xp.cgov/travel/customerservice; or
- **Mail:** by sending a letter to CBP Customer Service Center (Rosslyn VA), 1300 Pennsylvania Avenue NW, Washington, DC 20229.

When you contact the Customer Service Center for a written response, you should provide in writing: your full name, address, date of birth, and a copy of the photo page of your passport (or other photo identification if you do not have a passport). In addition, you should provide as detailed an explanation of the problem and why you think it should no longer be a concern and your records should be amended.

3. Freedom of Information Act (FOIA) and Privacy Act (PA) Requests

If you have concerns about being stopped or delayed and would like CBP to provide you with a copy of the records in its possession that pertain to you, then you may submit a request to CBP at the following address:

U.S. Customs and Border Protection
1300 Pennsylvania Avenue, NW,
Attn: Mint Annex Building, FOIA Division
Washington, DC 20229

You should provide your full name, address, date of birth, and any other personal identifying information you believe might be helpful in locating records related to your inquiry or resolving your concern. After receiving your request, we will research the matter, and respond with copies of those records, which may be disclosed. Please note that neither the FOIA nor the PA is intended to provide a mechanism for asking questions of CBP. FOIA and PA requests are intended to provide access to certain records under the control of the agency from which you request them. If you have questions concerning, for example, the reason why an action was taken, then you should contact DHS TRIP or CBP's Customer Service Center.

Appendix D: List of Relevant Systems and SORNs, where applicable, for data available through ATS

ATS maintains copies of key elements of certain databases, including but not limited to:

- DHS/CBP-001 Automated Commercial Environment (ACE) (published January 19, 2006, 71 FR 3109)
- DHS/CBP-015 Automated Commercial System (ACS) (published December 19, 2008, 73 FR 77759)
- Commerce/Census-012 Foreign Trade Statistics (published June 23, 2009, 74 Fed. Reg. 29676) - which covers the Automated Export System (AES)
- DHS/CBP-005 Advanced Passenger Information System (APIS) (published November 18, 2008, 73 FR 68435)
- DHS/CBP-007 Border Crossing Information (BCI) (published July 25, 2008, 73 FR 43457)
- Department of State's Consular Electronic Application Center (CEAC) (published August 2, 1995, 60 FR 39469)
- DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) (published May 3, 2010, 75 FR 23274) - which covers EID
- DHS/CBP-009 Electronic System for Travel Authorization (ESTA) (published November 2, 2011, 76 FR 67751)
- DHS/CBP-002 Global Enrollment System (GES) (published April 21, 2006, 71 FR 20708)
- DHS/CBP-016 Non Immigrant Information System (NIIS) (published December 19, 2008, 73 FR 77739)
- DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS) (published December 19, 2008, 73 FR 77764)
- DHS/ICE-001 Student Exchange and Visitor Information System (SEVIS) (published January 5, 2010, 75 FR 412)
- Social Security Administration (SSA) Death Master File
- DHS/CBP-010 TECS (published December 19, 2008, 73 FR 77778)
- DHS/USVISIT-001 Arrival and Departure Information System (ADIS) August 22, 2007 (72 FR 47057)
- DHS/ALL-030 Use of the Terrorist Screening Database System of Records (published July 6, 2011, 76 FR 39408)

Pointer System: ATS accesses and uses the following additional databases:

- CBP Border Patrol Enforcement Tracking System (BPETS)
- Department of State Consular Consolidated Database (CCD) (PIA available at http://www.state.gov/documents/organization/93772.pdf)
- Commercial data aggregators
- CBP's Enterprise Geospatial Information Services (eGIS)
- DHS/US-VISIT-0012 DHS Automated Biometric Identification System (IDENT) (June 5, 2007, 72 FR 31080)
- Nlets (formerly National Law Enforcement Telecommunications System)
- DOJ/FBI-001 National Crime Information Center (NCIC) (published September 28, 1999, 64 FR 52343, January 31, 2001, 66 FR 8425, and January 25, 2007, 72 FR 3410)

Manually Processed Data: ATS processes certain data in ATS and provides results back to owner of the data:

- ATS receives possible overstays from USVISIT and processes them to identify additional information on whether the individual has left the country as well as whether the individual is a possible national security or public safety risk. [4]

[4] DHS/All/PIA-041 One DHS Overstay Vetting Pilot published December 29, 2011.