



**Privacy Impact Assessment Update
for the**

**Automated Targeting System –
TSA/CBP Common Operating Picture
Program**

DHS/CBP/PIA-006(c)

January 31, 2014

Contact Point

Kevin Leung

Office of Field Operations

U.S. Customs and Border Protection

(202) 325-4211

Reviewing Official

Karen Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. U.S. Customs and Border Protection (CBP) is publishing this update to the Privacy Impact Assessment (PIA) for the Automated Targeting System (ATS), which was last updated June 1, 2012.¹ This update will evaluate the privacy impacts of the Common Operating Picture (COP) program, which permits TSA and CBP to share certain information about watchlisted travelers and their traveling companions, as a new part of ATS.

Overview

In order to facilitate legitimate trade and travel while managing the shared threat to the homeland posed by people or cargo entering or exiting the United States, DHS CBP operates the Automated Targeting System (ATS). ATS provides the following basic functionalities to support CBP in identifying individuals and cargo for additional review across the different means or modes of travel to, through, and from the United States:

- **Comparison:** ATS compares information about 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 about 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.
- **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 these functionalities, ATS uses data from many different source systems. ATS is divided into five modules: 1) Automated Targeting System-AntiTerrorism (ATS-AT); 2) Automated Targeting System-Inbound (ATS-N); 3) Automated Targeting System-

¹ For detailed information about the ATS program, please see DHS/CBP/PIA-006(b) – Automated Targeting System (ATS), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.



Land (ATS-L); 4) Automated Targeting System-Passenger (ATS-P); and 5) ATS-Targeting Framework (ATS-TF), which provides a view of risks across the four previous areas. Each of these modules supports the CBP officer in determining whether or not a particular individual or cargo requires additional scrutiny or presents a higher risk. The final module looks across the different areas to find common concerns and risks.

Common Operating Picture Program

DHS seeks to improve its mission of vetting of travelers, pursuant to the authorities described below, through the leveraging of common procedures, technology, and information sharing among DHS agencies that conduct vetting operations. Two such components are the Transportation Security Administration (TSA) and CBP, which review information about international airline passengers to determine whether the passengers may access U.S. transportation networks and airspace. TSA and CBP make this determination, in part, by identifying passengers who appear on the Center for Disease Control and Prevention (CDC) Do Not Board List (DNBL), the No Fly and Selectee subsets of the Terrorist Screening Center (TSC) Terrorist Screening Database (TSDB), or who are these travelers' traveling companions (collectively "Inhibited Passengers"). To improve information sharing of Inhibited Passenger travel, CBP and TSA are creating a Common Operating Picture (COP), a single unclassified location where all Inhibited Passenger travel discovered by TSA and CBP will be displayed to both components. The COP program serves three purposes:

- 1) To ensure consistent vetting of watchlisted individuals across components;
- 2) To refine each component's ability to positively identify individuals who are prohibited from flying to, from, through, or over the United States, or involving international travel, individuals who may require additional scrutiny prior to traveling, and to make a determination that an individual is not a match to the CDC DNBL or the No Fly or Selectee subsets of the TSDB; and
- 3) To allow TSA and CBP to coordinate responses.

To achieve these purposes, TSA will share information regarding persons it identifies as Inhibited Passengers through its normal vetting procedures with CBP through TSA-WebEOC, TSA's operations center incident management system.² CBP will store the information in ATS-P and display the TSA-identified Inhibited Passengers alongside CBP-identified Inhibited Passengers on a read-only common dashboard display at CBP's National Targeting Center and

² TSA uses WebEOC to process and disseminate information related to transportation security incidents or individuals who violate, or are suspected of violating transportation security laws, regulations, policies or procedures. For more detailed information on the WebEOC system, please see DHS/TSA/PIA-029 - Operations Center Incident Management System PIA, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_ocims_update.pdf.



TSA's operations center. This display will enable CBP and TSA to quickly identify and resolve discrepancies in vetting.

Reason for the PIA Update

DHS/CBP is updating the existing PIA (DHS/CBP/PIA- 006(b)), published on June 1, 2012, to provide notice to the public of the new COP program.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

TSA collects and maintains the information it is providing to CBP as part of its transportation security mission. TSA was created by the Aviation and Transportation Security Act (Pub.L. 107-71, 115 Stat. 597). TSA is responsible for security in all modes of transportation (49 U.S.C. § 114(d)). TSA is authorized to receive, assess, and distribute intelligence information related to transportation security as well as assess threats, and develop policies, strategies, and plans for dealing with threats to transportation security (49 U.S.C. § 114(f)). Other authorities include the Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135), as amended; the Aviation and Transportation Security Act (Pub. L. 107-71, 115 Stat. 597) (49 U.S.C. § 114(m)); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173, 116 Stat. 543). Information developed and provided by TSA from WebEOC is covered under DHS/TSA-019 Secure Flight Records System of Records Notice (SORN), last published on September 10, 2013 (78 FR 55270).

TSA and CBP share this information pursuant to HSPD-6, Directive on Integration and Use of Screening Information to Protect Against Terrorism (September 16, 2003); HSPD-11, Comprehensive Terrorist-Related Screening Procedures (August 27, 2004); Executive Order 13388 (October 25, 2005); and interagency MOUs relating to this information.

Once the information is received from TSA, it and information developed and provided by CBP are covered by the ATS SORN, last published on May 22, 2012 (77 Fed. Reg. 30297). 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; EBSVRA (Pub. L. 107-173); the Trade Act of 2002 (Pub.L. 107-210); IRTPA (Pub.L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub.L. 109-347).

Characterization of the Information

TSA will push certain WebEOC information to ATS, which will be displayed on the common dashboard developed in ATS-P. The common dashboard will display read-only



information relating to confirmed matches to the CDC's DNBL, the No Fly and Selectee subsets of the TSDB, and information relating to the traveling companions of these confirmed matches. CBP will only receive information on individuals on flights to, from, through, or over the United States, or involving international travel.

The following data elements will be pushed from the TSA-WebEOC system to ATS-P:

- biographic information (first name, last name, date of birth);
- itinerary;
- match type;
- comment/remarks;
- TSC-ID; and
- status (e.g., awaiting check in, denied boarding).

TSA will share the biographic, itinerary, and status information already collected from passengers and air carriers. The TSA-generated match type (indicating which watchlist the individual matches, CDC DNBL, Selectee, or No Fly), comment/remarks describing the basis for the match and any persons associated with the match, and TSC-ID information are new data elements being ingested by CBP, though CBP independently generates similar information as it processes international air travelers.

Uses of the Information

The COP information will only be available to authorized ATS users with roles permitting them to access this watchlist information and similarly authorized TSA users at TSA's operations center. CBP and TSA will use the COP for the following purposes:

- 1) To ensure consistent vetting of watchlisted individuals across components;
- 2) To refine each component's ability to positively identify or exclude individuals who are prohibited from flying to, from, through, or over the United States, and individuals who may require additional scrutiny prior to traveling; and
- 3) To allow TSA and CBP to coordinate responses.

Through the COP, TSA will provide CBP the list of Inhibited Passengers - positive matches to the watchlists and those associated with the match. CBP will perform the comparison, rule, and federated query functions listed above to identify pertinent CBP-held information on the Inhibited Passengers. CBP will then compare TSA's list of Inhibited Passengers with its own list of Inhibited Passengers to check for consistency and identify enhancements to the component's respective systems and procedures.

For example CBP will be able to identify situations when TSA identifies a TSDB No Fly individual and, the TSC confirms a positive match, but the individual fails to appear on CBP's



list of matches to the TSDB No Fly subset. This may be due to differences in the algorithms run by each system or due to differing matching procedures. CBP may then adjust its algorithms or provide additional officer training, as needed, to ensure that all watchlisted individuals are properly identified in the future. Similarly, if TSA misidentifies an individual as belonging on the CDC DNBL, but CBP has resolved the individual's identity as a misidentification, the COP will alert both components to the discrepancy. Alerting TSA to the misidentification will lead to TSA de-identifying the individual and saving the individual from unnecessary scrutiny.

Notice

No additional notice is being provided through this program aside from this PIA as CBP and TSA are not collecting any additional information from the public. Rather, CBP and TSA are making better use of the information already collected from air carriers in conformance with their existing authorities and missions.

Data Retention by the project

ATS retains ingested information pursuant to the source system's retention schedule or 15 years, whichever is less.³ While the TSA retention for confirmed matches to a watchlist is 99 years, CBP will only retain this information for 15 years. Records created about persons associated with the match that are determined not to be a threat will be destroyed within seven days after completion of the last leg of the individual's directional travel itinerary, in conformance with the Secure Flight SORN.⁴ This retention permits CBP and TSA to accurately and consistently identify watchlisted travelers while minimizing the information they retain about legitimate travelers.

Information Sharing

TSA and CBP information will be made available to both components through the COP common operating dashboard. However, only authorized personnel at the CBP and TSA operations centers will be able to view this information for the purposes stated above.

Redress

The redress procedures for CBP and TSA will not change through this program. Through the COP, CBP and TSA will be better able to resolve misidentified individuals and prevent them from requiring any redress. Further, the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals seeking redress for

³ See DHS/CBP-006 - Automated Targeting System May 22, 2012 (77 FR 30302).

⁴ See DHS/TSA-019 Secure Flight Records System of Records, September 10, 2013 (78 FR 55273).



difficulties they experienced during their travel screening and inspection at transportation hubs—like airports and train stations—or crossing U.S. borders, including:

- watch list issues
- problems at ports of entry
- situations in which travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening or inspection at our nation's transportation hubs

For more information, please visit the DHS TRIP website: <http://www.dhs.gov/dhs-trip>.

Auditing and Accountability

All persons with access to this information are existing ATS-P users. There are no changes to the auditing and accountability procedures of ATS.

Responsible Official

Laurence Castelli
Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Karen Neuman
Chief Privacy Officer
Department of Homeland Security