Privacy Impact Assessment Update
for the

Automated Targeting System –

TSA/CBP Common Operating Picture Phase II

DHS/CBP/PIA-006(d)

September 16, 2014

Contact Point
David Dodson

Director, Passenger Targeting
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
(202) 344-1150

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Automated Targeting System (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 Privacy Impact Assessment (PIA) update to describe Phase II for the Common Operating Picture (COP) program, which enhances information sharing about watchlisted travelers and their traveling companions between DHS components. CBP and the Transportation Security Administration (TSA) are adding new information to the COP to further promote information sharing between CBP and TSA during Phase II. CBP will publish additional updates to this PIA prior to deployment of any subsequent phases to the COP program.

Overview

The Department of Homeland Security (DHS)/CBP operates ATS to facilitate legitimate trade and travel while managing the shared threat to the homeland posed by certain people or cargo entering or exiting the United States. ATS supports CBP in identifying individuals and cargo that may require additional scrutiny across various transportation networks using the following functionalities:[1]

- Comparison: ATS compares information about travelers and cargo arriving in, transiting through, or exiting the country, against law enforcement and intelligence databases. For example, ATS compares information about individuals (identified as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) against the Terrorist Screening Database (TSDB)[2] as well as data concerning outstanding wants and warrants.
- Rules: ATS compares existing information about individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, trend analysis 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 about a person or entity.

[1] For a complete overview of ATS, its modules, and the associated privacy risks, *see* DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

[2] ATS ingests the TSDB via the DHS Watchlisting Service (WLS). Please see DHS/ALL/PIA-027 Watchlist Service and subsequent updates for a full description of the WLS, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_wls_update027(b).pdf.

Information received from TSA as part of the COP program is stored in ATS-Passenger (ATS-P).

Common Operating Picture Program Phase I

DHS continuously strives to improve traveler vetting and information sharing among DHS components, such as TSA and CBP, that have overlapping vetting authorities and operations, including TSA and CBP. Both components review information about airline passengers to determine whether the passengers may access U.S. transportation networks or require additional scrutiny when traveling to, from, within, or over the United States. Both TSA and CBP also review information about airline passengers traveling on U.S. aircraft operators that are required to have a "full [security] program" under the Transportation Aircraft Operator Security Rule[3] ("covered U.S. aircraft operators").

To determine which passengers may warrant additional scrutiny, TSA and CBP identify passengers who appear on the Center for Disease Control and Prevention (CDC) Do Not Board List (DNBL), or the No Fly and Selectee subsets of the Terrorist Screening Center (TSC) TSDB (hereinafter referred to as "watchlisted passengers"). Phase I of the COP program focused on the reconciliation of vetting discrepancies among TSA and CBP-identified watchlisted passengers and their traveling companions. TSA provided CBP with information about persons identified as watchlisted passengers through its normal vetting procedures through TSA-WebEOC,[4] TSA's operations center incident management system during the first phase of the COP. CBP stored the information in ATS-P and displayed the TSA-identified watchlisted passengers alongside CBP-identified watchlisted passengers on a read-only common dashboard display at CBP's National Targeting Center (NTC) and TSA's operations center. This display enabled CBP and TSA to quickly identify and resolve discrepancies in vetting.

Phase I of the COP program successfully resolved vetting inconsistencies of watchlisted passengers. However, TSA and CBP determined that an accurate and complete picture of all potential threats (including but not limited to the watchlisted passengers) in the air domain remains incomplete. Due to the success of resolving vetting inconsistencies in Phase I, TSA and CBP will expand the amount of passenger information shared via the COP dashboard to enhance the overall picture of the air domain security. With Phase II, the COP will continue to show TSA and CBP-identified passengers that appear on the initial watchlists, as well as "Inhibited Travelers":

---

[3] 49 C.F.R. § 1544.101 (2014), a*vailable at,* http://www.gpo.gov/fdsys/pkg/CFR-2010-title49-vol9/pdf/CFR-2010-title49-vol9-sec1544-101.pdf.

[4] 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.

- passengers who are confirmed or possible matches to the watchlists on international flights of covered U.S. aircraft operators;
- passengers on domestic flights who are confirmed matches to the DNBL and TSDB watchlists;
- passengers who possess certain derogatory holdings that warrant enhanced scrutiny; and
- travelers with a high probability of being denied boarding by an aircraft operator on a carrier bound for or departing the United States. These travelers and their traveling companions are collectively referred to as "Inhibited Passengers."

CBP and TSA created the COP to promote information sharing between the two components and to provide a single unclassified location in which all identified Inhibited Passenger travel is displayed to both components. The expansion of the COP in Phase II mitigates this security gap (the risk of an incomplete or inaccurate picture of all potential threats in the air domain) and aligns with the aviation security and counterterrorism missions of both components supporting the COP program's original intent.

Accordingly, the COP program's expanded purposes include:

1. To ensure consistent vetting of and refine each component's ability to positively identify individuals matched to the CDC DNBL or the No Fly and Selectee subsets of the TSDB who fly to, from, through, or over the United States or on international flights that are operated by covered U.S. aircraft operators;
2. To increase the operational awareness of both components concerning travelers who may require additional scrutiny prior to traveling or pose a risk to aircraft safety or to national security; and
3. To allow TSA and CBP to coordinate responses.

Reason for the PIA Update

This PIA was last updated on January 31, 2014. DHS/CBP is further updating the PIA to notify the public that the COP program is transitioning from Phase I to Phase II. This change describes the additional data elements shared with the COP that provides both components with increased operational awareness of identified Inhibited Passenger travel.

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

The legal authorities to operate the COP have not changed with the implementation of Phase II.

TSA collects and maintains the information it is providing to CBP as part of its transportation security mission. CBP has a mission-need to receive certain domestic traveler information to obtain a more comprehensive awareness and understanding of those travel patterns which, in turn, strengthen CBP's inbound and outbound activities in support of its border security mission as set forth in Title IV of the Homeland Security Act of 2002 and related authorities.

In Phase II, TSA shares information of identified possible and confirmed matches of international travelers and confirmed matches of domestic travelers to the DNBL and TSDB watchlists through TSA-WebEOC pursuant to the Aviation and Transportation Security Act.[5] Information developed and provided by TSA from WebEOC is covered under DHS/TSA-019 Secure Flight Records System of Records Notice (SORN).[6] Confirmed matches to the DNBL and TSDB watchlists for domestic flights are displayed in the dashboard (which can be viewed by TSA and CBP). TSA may disclose this information to CBP to advance CBP's mission-related responsibilities under subsection (b)(1) of the Privacy Act. The DHS/CBP-006 ATS SORN covers all information received from TSA. Moreover, all information provided by CBP to the COP is covered by the DHS/CBP-006 ATS SORN.[7]

The authority to collect Electronic System for Travel Authorization (ESTA)[8] application information and make eligibility determinations is authorized under Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007.[9] The authority to collect information on visa revocations and lost and stolen passports is granted under the Enhanced Border Security and Visa Reform Act of 2002.[10]

Characterization of the Information

In Phase II of the COP, the TSA WebEOC system pushes the following data elements to ATS-P regarding all travelers who are confirmed or possible matches for certain international flights, and confirmed matches for domestic flights to the DNBL and TSDB watchlists:

---

[5] Pub. L. 107-71 (115 Stat. 597, 2001, codified at 49 U.S.C. § 114(f); 49 U.S.C. § 44903; 49 U.S.C. 44909).
[6] DHS/TSA-019 Secure Flight Records SORN, 78 FR 55270 (September 10, 2013), *available at* http://www.dhs.gov/system-records-notices-sorns.
[7] DHS/CBP-006 Automated Targeting System SORN, 77 FR 30297 (May 22, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.
[8] For additional information about the ESTA process, please *see* DHS/CBP/PIA-007 Electronic System for Travel Authorization, and subsequent updates, *available at* http://www.dhs.gov/publication/dhscbppia-007c-electronic-system-travel-authorization.
[9] Pub. L. 110-53, codified at 8 U.S.C. § 1187(a)(11), (h)(3).
[10] Pub. L. 107-173, 116 Stat. 543.

- Biographic information (first name, last name, date of birth);
- Itinerary;
- Match type;
- Comments/remarks;
- TSC-ID; and
- Status (awaiting check-in, denied boarding, etc.)

Similarly, CBP populates the COP common dashboard, viewable by CBP and TSA, with the following data elements already retained in ATS-P including:

- Travelers whose visa has been denied or revoked;
- Travelers who match a lookout for a lost or stolen passport;
- Travelers whose ESTA application has been denied; and
- TSA and CBP -generated rule hit data.

In Phase II of the COP program, TSA continues to push the WebEOC information to ATS, which is displayed on the common dashboard developed in ATS-P. In Phase I, TSA shared the biographic, itinerary, and status information already collected from passengers, their traveling companions, and air carriers. In Phase I, CBP only received information on individuals who were confirmed matches to the watchlists on flights involving a nexus to certain international travel. In Phase II, CBP receives information from TSA about DNBL and TSDB possible and confirmed matches for individuals on international flights of covered U.S. aircraft operators. TSA also sends CBP the confirmed matches on domestic flights operating within the United States, consistent with CBP's mission.

Phase II of the COP also introduces additional datasets pushed by CBP to the COP dashboard. CBP now displays visa denials and revocations, lost or stolen passport information, and ESTA denial data on the COP dashboard, viewable by TSA. These expanded datasets give TSA advanced awareness about travelers who will likely be denied boarding. Thus, TSA reduces time spent vetting travelers that are unlikely to travel by providing this information to TSA through the COP.

Confirmed Matches of Domestic and Confirmed and Possible Matches on International Passenger Data

The COP offered limited utility for users in Phase I because only individuals on certain international flights were displayed on the COP dashboard. COP users could not perform an accurate, real-time assessment of all identified threats to aviation, U.S. interests, or national security without confirmed DNBL and TSDB matches of passengers on domestic flights and

possible and confirmed matches of travelers on international flights that are operated by covered U.S. aircraft operators. Phase II introduces confirmed watchlist matches of individuals traveling within domestic airspace and possible and confirmed matches of travelers on international flights that are operated by covered U.S. aircraft operators in order to maximize the effectiveness of the COP as a visualization tool. Adding these matches to the COP provides operational awareness across the entire air spectrum further improving cross-component passenger vetting capabilities.

Data Displayed Through ATS-P

Currently, ATS-P is used to vet non-immigrant and immigrant visa applications for the Department of State (State). State sends online visa application data to ATS-P for pre-adjudication investigative vetting. ATS-P vets the visa application and provides a response to State's Consular Consolidated Database (CCD)[11] indicating whether or not derogatory information was identified by DHS about the individual. With the implementation of Phase II of the COP program, all confirmed visa denial and revocation records will be displayed on the COP dashboard from ATS-P.

ATS-P also vets ESTA applicants.[12] Individuals submit their biographical information and answer eligibility questions when completing an ESTA application. After vetting the information against selected security and law enforcement databases for terrorists or threats to aviation and border security, CBP makes a determination about the applicant's eligibility to travel to the U.S. ATS-P retains a copy of ESTA application data to identify potential high-risk ESTA applicants. An individual's ESTA application is denied if the vetting process identifies derogatory data that prohibits the issuance of a travel authorization. The denied ESTA record is then displayed on the COP dashboard.

ATS-P receives lost and stolen passport lookout information from State and Interpol via TECS.[13] The record will be displayed on the COP dashboard if any inbound or outbound international traveler with a passport matches against a lost or stolen passport lookout.

Prior to the development of the COP, CBP shared information about travelers with a high likelihood of being denied boarding[14] with TSA through an automated process in ATS that

---

[11] For more information on State Department's Consular Consolidated Database (CCD) please see the CCD PIA, *available at*, http://foia.state.gov/_docs/PIA/ConsularConsolidatedDatabase_CCD.pdf, and the following associated SORNs: Overseas Citizens Services Records (STATE-05); Passport Records (STATE-26); and Visa Records (STATE-39), *available at*, http://foia.state.gov/Learn/SORN.aspx#1.

[12] For additional information about the ESTA process, please *see* DHS/CBP/PIA-007 Electronic System for Travel Authorization, and subsequent updates, *available at* http://www.dhs.gov/publication/dhscbppia-007c-electronic-system-travel-authorization.

[13] DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf; and DHS/CBP-011 U.S. Customs and Border Protection TECS SORN, 73 FR 77778 (December 19, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

[14] Travelers have a high likelihood of being denied boarding by an aircraft operator on an aircraft destined for the

generated an email to TSA. By including this information in the COP, both TSA and CBP are now able to visualize the information and TSA receives advance notice of passengers likely to be denied boarding by an aircraft operator on an aircraft. As a result, TSA minimizes the time for vetting passengers who are unlikely to travel and can instead allocate resources on larger unknown traveling populations.

TSA and CBP-Generated Rule Hit Data

The purpose of TSA's Secure Flight program is to screen individuals before they access airport sterile areas or board aircraft. This screening has generally been designed to identify and prevent known or suspected terrorists or other individuals from gaining access to airports and airplanes where they may jeopardize the lives of passengers and others. Generally, the Secure Flight program will compare passenger and non-traveler information to the No Fly and Selectee List components of the TSDB, which are currently used for the pre-flight passenger watch list matching conducted by aircraft operators. However, as recommended in the final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), TSA may use the "larger set of watch lists maintained by the Federal government." Therefore, pursuant to 49 U.S.C. § 114(f), which requires TSA to assess threats to transportation when warranted by security considerations, TSA may use the full TSDB or other government databases, such as intelligence or law enforcement databases. For example, TSA may obtain intelligence that flights flying a particular route may be subject to an increased security risk. Under this circumstance, TSA may decide to compare passenger information on some or all of the flights flying that route against the full TSDB or other government databases.

Based on the watchlist matching results produced by Secure Flight (using either the No Fly and Selectee List or the full TSDB or other government databases when warranted by security considerations), TSA will instruct an aircraft operator to process the individual in the normal manner, to identify the individual for enhanced screening at a security checkpoint, or to deny the individual transport or authorization to enter the airport sterile area.

TSA also provides risk-based, intelligence-driven, scenario rules to CBP for use in ATS-P to identify international travelers requiring enhanced screening. TSA receives a continuously updated watchlist of these individuals from CBP for use in the Secure Flight program.[15]

United States if their visa applications are denied or revoked, if their ESTA applications are denied, or if their passport number matches a lookout for a lost or stolen passport.

[15] Certain intelligence-driven scenario rules may result in some travelers receiving enhanced screening for subsequent domestic and international flights for a period of time. *See* the previously published Secure Flight PIAs for a complete understanding of TSA's Secure Flight program: DHS/TSA/PIA-018(f) Secure Flight Program Update PIA, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-secure-flight-update-09042013.pdf; DHS/TSA-019 Secure Flight Records SORN, 78 FR 55270 (September 10, 2013), *available at* https://www.federalregister.gov/articles/2013/09/10/2013-21980/privacy-act-of-1974-department-of-homeland-security-transportation-security.

CBP compares existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny in ATS. The patterns are based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence corroborating those trends. For example, ATS can compare information on travelers against a set of scenario-based targeting rules that indicate a particular travel pattern is used by drug smugglers. CBP can then send the person who meets such criteria to secondary inspection for additional examination. Previously published ATS SORN and PIAs provide more information about the ATS rules.

TSA and CBP-generated rule hits on international travelers are displayed on the COP dashboard with the implementation of Phase II of the COP program. Populating the COP dashboard with TSA and CBP rule hits allows both components to have immediate operational awareness of potential Inhibited Passenger travel or those who may require additional scrutiny, and aligns with the COP program's original purpose of improving information sharing by displaying all Inhibited Passenger travel and others of potential concern to both components in a single location.

Uses of the Information

Phase II continues the ability of TSA and CBP to use the records displayed on the COP common dashboard for operational purposes related to cross-component information sharing of identified threats and accurate air domain security threat assessments. The additional datasets introduced in Phase II are only accessed by authorized ATS users with roles permitting them to access this information and by authorized TSA users at TSA's operations center. CBP and TSA continue to use the COP for the following purposes:

1. To ensure consistent vetting of and refine each component's ability to positively identify individuals matched to the CDC DNBL or the No Fly and Selectee subsets of the TSDB who fly to, from, through, or over the United States, or on international flights that are operated by covered U.S. aircraft operators;
2. To increase the operational awareness of both components concerning travelers who may require addition scrutiny prior to traveling or pose a risk to aircraft safety, U.S. interests, or to national security; and
3. To allow TSA and CBP to coordinate responses.

TSA provides CBP with the data elements listed above regarding travelers who are confirmed watchlist matches on domestic flights and confirmed and possible matches on international flights, and their travel companions in Phase II of the COP. CBP performs comparison, rule, and federated query functions and identifies pertinent CBP-held information on these travelers. CBP compares TSA's list of confirmed watchlisted passengers with its own list of confirmed watchlisted passengers for consistency and identifies enhancements to the

component's respective systems and procedures. CBP determines situations in which inconsistencies exist between positive matches to the watchlists of the respective components by displaying confirmed matches to the watchlists of domestic travelers. These inconsistences may be due to differences in algorithms run by the different systems or to differing matching procedures. CBP or TSA adjusts its algorithms or provides additional training to ensure that all confirmed watchlisted travelers are properly identified in the future if vetting inconsistencies are identified.

The COP dashboard alerts both components of any vetting discrepancies and allows both components to determine that a traveler was misidentified, thus facilitating his or her travel. In addition, possible matches are displayed for travelers on international flights operated by covered U.S. aircraft operators. CBP leverages its holdings to try to further determine whether the possible match is or is not a positive match to a watchlist in coordination with the appropriate third agencies. This helps prevent DHS from inconveniencing travelers who are determined to not be a match.

CBP also performs comparison, rule, and federated query functions in ATS-P to provide data about travelers whose visas are revoked, match a lookout for a lost or stolen passport, have been denied an ESTA, or are positive hits of TSA or CBP-generated rules processed in ATS-P. Once these travelers are identified in ATS-P their information is displayed on the COP to provide both components with enhanced operational awareness of potential threats to aviation, U.S. interests, and national security.

Notice

No additional notice is being provided aside from this PIA update to reflect Phase II of the COP because no new information is collected from the public. However, CBP and TSA improve the use of the information already collected in conformance with their existing authorities and missions in Phase II of COP implementation.

Data Retention by the Project

CBP has concluded that the previously established retention periods for data residing in the COP should be revised.[16] CBP previously determined that confirmed matches to a watchlist would be retained for 15 years to mirror the retention schedule for ATS. Records created about persons associated with the match but determined not to be a threat would be destroyed within seven days after the completion of the last leg of the individual's directional travel itinerary, in conformance with the Secure Flight SORN.[17]

[16] DHS/CBP/PIA-006(c) Automated Targeting System PIA Update - TSA/CBP Common Operating Picture Program, *available at*, http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-atsupdate-01312014.pdf.
[17] "Records relating to an individual determined by the automated matching process to be neither a match nor or potential match to a watchlist will be destroyed within seven days after completion of the last leg of the individual's directional travel itinerary. Records relating to an individual determined by the automated matching process to be a

Retaining confirmed watchlist data for either domestic or international travelers is unwarranted because this information is also retained in the TSDB. As a result, an individual's records are displayed on the COP dashboard for two hours after the completion of his or her travel itinerary and purged completely within 72 hours.

Records created about an individual associated with a confirmed or possible match to a watchlist that require additional analysis in the ATS case management module ATS-Targeting Framework (TF) will be retained for 15 and seven years respectively in ATS if the individual is ultimately determined not to be a threat. However, COP 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. In addition, CBP may include information in TECS on individuals who may need additional scrutiny and will abide by the TECS retention schedule.

The justification for the revised retention period for COP records is based on both CBP and TSA's business needs to ensure accurate and consistent identification of Inhibited Passenger travel while minimizing the information retained about legitimate travelers. This revision 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. For example, potential terrorists may make multiple visits to the United States before 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 to assist 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 effectively identify suspect travel patterns and irregularities.

Information Sharing

There has been no change to information sharing in Phase II of the COP program. TSA and CBP information is available to both components through the COP dashboard. However, only authorized personnel at the CBP and TSA operations centers are able to view this information for the purposes stated above.

Redress

---

potential watch list match will be retained for seven years after the completion of the individual's directional travel itinerary. Records relating to an individual determined to be a confirmed watchlist match will be retained for 99 years after the date of match confirmation. Lists of individuals stored in Secure Flight, such as individuals identified as Known Travelers and individuals who have been disqualified from eligibility to receive expedited screening as a result of their involvement in certain security incidents, will be deleted or destroyed when superseded by an updated list." *See* DHS/TSA-019 Secure Flight Records SORN, 78 FR 55270 (September 10, 2013), *available at* https://www.federalregister.gov/articles/2013/09/10/2013-21980/privacy-act-of-1974-department-of-homeland-security-transportation-security.

The redress procedures for CBP and TSA have not changed with the implementation of Phase II of the COP program. CBP and TSA are better able to resolve misidentified individuals and prevent them from requiring any redress through the COP. Further, the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals seeking redress for difficulties they experienced during their travel screening and inspection at transportation hubs—like airports and train stations—or crossing U.S. borders. For more information, please visit the DHS TRIP website: http://www.dhs.gov/dhs-trip.

Auditing and Accountability

The auditing and accountability procedures have not changed in Phase II of the COP program and continue to be the same procedures employed by ATS. All individuals with access to the information described in this PIA are existing ATS-P users with a demonstrated need to know the information displayed on the COP.

Responsible Official

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

Approval Signature

Original signed and on file at the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security