

U.S. Department of Homeland Security
Washington, DC 20229



U.S. Customs and
Border Protection

Commissioner

FEB 21 2007

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter of January 17, 2007 concerning U.S. Customs and Border Protection's (CBP) Automated Targeting System – Passenger (ATS-P). We are also aware of the comments you submitted to the Department of Homeland Security (DHS) regarding the System of Records Notice (SORN) for ATS.

This letter will address the questions and concerns you raised in your letter of January 17, 2007. Please be aware that the ATS SORN (which includes ATS-P) and any comments related thereto are currently under review. Consequently, the following statements reflect the current state of ATS-P. They do not include any considerations or changes that may be addressed or implemented in response to comments received from you and others regarding the SORN.

1. The Risk Assessment Portion of the Process

Question:

1(a) Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

Response

Contrary to what has been reported recently in the media, ATS-P does not use an actual score to determine an individual's risk. Nor does CBP assign a score to an individual to assess a level of risk. Instead, using a risk-based methodology, ATS-P helps CBP target and identify travelers who may require further scrutiny or examination when they present themselves for admission to the United States. More specifically, ATS-P is a decision support tool that allows CBP Officers to determine whether a sufficient combination of potential risk indicators exist for travelers and/or their flight transactions to warrant additional scrutiny. The targeting regime in the ATS *cargo* modules, by contrast, does employ a scoring system to identify cargo shipments of interest.

To clarify what you believe to be "contradictory information," we would offer several points. ATS-P was a specific passenger application of a broader ATS effort. ATS-P grew out of and was based on the development and success of ATS as applied to cargo. As the SORN generally addressed ATS in all its forms, there may be some confusion regarding the nature of the assessments employed in the cargo versus the passenger environments. The use of ATS to assess risk on cargo movement into the United States does both generate and utilize a score. As one of the most publicly known applications of ATS, it has sometimes been generally noted that ATS creates a score to assess risk. However, that is only true for CBP's assessment of cargo containers and vehicles at the land border. While CBP, then legacy U.S. Customs, recognized and understood early on that the same risk factors that applied to cargo certainly did not apply to passengers, it determined that the capabilities of the ATS could be leveraged and redesigned to specifically address risk indicators that are present in the passenger environment.

Thus, ATS-P was first operationalized in 2000, building off the success of the broader Automated Targeting System. In August 2004, CBP developed the Threshold Targeting module within ATS-P. This module uses current classified intelligence available to the U.S. Government to identify, through risk-based targeting rules, if a passenger has a combination of potentially high-risk indicators associated with his/her travel. These rules are scenario-based and do not incorporate or use a score. If a passenger matches a scenario-based rule, then the passenger would receive further examination by a CBP Officer. If the passenger does not match the scenario-based rule, then the passenger will not be referred for this reason. CBP continuously reviews current intelligence and changes the rules in accordance with changes in intelligence. Furthermore, changes in intelligence may require a deactivation or modification of the current rules or possibly the creation of a new rule.

When ATS-P was first rolled-out in 2000, the system had the ability to generate numbers, corresponding to the number of risk indicators associated with a specific transaction. These numbers were never seen by CBP Officers in primary inspection, however, nor did CBP Officers use them to assign an individual a particular score or "risk level." Instead, the system provided a notification to the officers that indicated further scrutiny might be necessary. CBP subsequently determined that these scoring algorithms were inefficient and unnecessary, and therefore decided not to use scores in the review of travelers arriving into the United States. Instead, in line with recommendations of the 9/11 Commission, CBP improved the system's performance and enhanced its targeting approaches with more sophisticated algorithms based on real-time intelligence, refined rules-based scenarios obtained by direct interviews with passengers, and improvements in the integration of information from other relevant Federal agencies. These improvements enabled CBP to end the use of scores in the ATS-P platform for purposes of its targeting efforts for passengers and move to a "threshold" system based on rules matched.

Currently, no CBP Officer at primary or otherwise has access to any scores, and scores are not used in determining a person's potential "risk level."

The historical ATS-P numerical data, often referred to as scores, has been archived so that it is not available for access. We also maintain copies of this archived data on our disaster recovery and other back-up tapes, as we are required to maintain an accurate "picture" of our data at any point in time. Should we be required to use these back-up tapes to restore ATS-P, the historical data will remain in archive status and not be available for use. The ATS-P graphical user interface has been modified to further ensure that any archived numerical data is not available for access. The historical data would only be made available in response to mandatory access requests, such as Internal Affairs or Inspector General investigations.

Question:

1(b) Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

Response:

Passenger Name Record (PNR) data (access to which is obtained by CBP through the air carrier reservation systems in accordance with 49 U.S.C. 44909 and 19 CFR 122.49d) is indeed collected in and used by ATS-P. In addition, ATS-P relies on data supplied from other government databases, including Advance Passenger Information System (APIS) data, to process and evaluate travelers for potential risk indicators. Additionally, as stated above, current intelligence is used to help define appropriate risk indicators and thresholds within the context of the ATS-P targeting module. For further information, please refer to our response to the next question.

Question:

1(c) Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

Response:

No. ATS-P does not check commercial databases in the risk assessment process. Furthermore, commercial databases that CBP may purchase for other applications are not incorporated or accessed in any automated assessment performed by ATS-P. As noted in the preceding response, ATS-P relies on data supplied from other government databases and uses current intelligence to define appropriate risk indicators and thresholds within the context of the ATS-P targeting module.

Individual CBP officers or analysts at the National Targeting Center (NTC) may access and conduct further research in publicly available commercial databases to verify, refute, or supplement data obtained from government databases, including data highlighted by ATS-P, or from interviews with travelers of interest. For example, a CBP officer may access Dunn and Bradstreet records to confirm the legitimacy of addresses or business names. This sort of additional research is not unique or novel. CBP officers and legacy precursor Customs and U.S. Immigration and Naturalization (INS) inspectors have long had the ability and tools to do such follow-up research on passengers referred to secondary for additional scrutiny. Importantly, however, under no circumstances does ATS-P itself obtain information from or run queries against publicly available commercial databases.

Questions:

1(d) If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

Response:

No. ATS-P does not, in and of itself, bar a non-watchlisted/selectee passenger from boarding a flight. Nor does it automatically place a passenger on such a watchlist. As explained above, ATS-P is only a decision support tool CBP officers use to help identify passengers who may require further scrutiny.

However, there are two situations in which an ATS-P risk assessment could be one of many factors that contributes to a non-watchlisted passenger being prohibited from flying:

1. The passenger is the subject of predeparture screening conducted by CBP officers assigned to U.S. preclearance stations located at foreign airports. During foreign preclearance (for example, in Ottawa, Canada), a passenger undergoes Customs and Immigration clearance before departing for the United States. If a passenger is identified for further examination as a result of an ATS-P risk assessment, and if further investigation uncovers derogatory information, the passenger may be determined to be inadmissible to the U.S. (if an alien) or detained or arrested by Canadian authorities. In either case, the passenger would be prevented from boarding a flight to the U.S.
2. The passenger is the subject of predeparture screening through CBP's Immigration Advisory Program (IAP). CBP IAP officers are assigned, by arrangement with the foreign host government, to designated overseas locations and use ATS-P to identify travelers who may be potentially higher-risk for terrorism, human smuggling, or other criminal offenses or aliens who may otherwise be denied admission to the United States. In contrast to preclearance, IAP officers in the host country have no authority to prevent travelers from boarding. If a person is identified as a person of concern after further scrutiny or investigation (which may be triggered in part by the ATS-P assessment) an IAP officer's role is only to advise the appropriate foreign host government authorities. This process may result in the prevention of a passenger from flying, but it is not a direct result of an ATS-P assessment.

An ATS-P risk assessment will not cause a person to be placed on any U.S. government watchlist, regardless of citizenship. Changes to the watchlists are the responsibility the Terrorist Screening Center (TSC), not CBP. Moreover, a risk assessment developed through ATS-P is not the basis upon which TSC would make such amendments.

Question:

1(e) Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

Response:

Yes. ATS-P has mechanisms in place to block the use of passenger's health, race, religion, sexual preference, or political beliefs in assessing risk. Additionally, pursuant to an agreement with the European Union, certain sensitive terms (related to the categories noted above) that may appear in the PNR of travelers on flights between the US and EU are blocked from the view by CBP officers with access to PNR data, regardless of where those terms may appear in the PNR. Such terms can be unblocked only on a case-by-case basis in rare circumstances, upon a showing of particular need and with the approval of the CBP Deputy Commissioner. To date, there have been no requests to view sensitive terms that have been blocked in PNR.

Question:

1(f) Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on factors such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

Response:

CBP does not engage in racial, ethnic, or religious profiling, nor does it discriminate based on race, ethnicity, or religion. Furthermore, CBP does not use any of these factors to determine potential risk. CBP officers undergo extensive training, and CBP has policies in place, including Standards of Conduct and a Table of Offenses, prohibiting such discrimination and profiling.

Additionally, as mentioned above ATS-P does not consider factors such as language, dietary restrictions, or the presence of other sensitive information in a traveler's PNR.

Question:

1(g) The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances. Please provide specific examples that illustrate under what circumstances this provision would be applicable.

Response:

CBP enforces all federal laws and regulations at the border and between the ports of entry. (See, for example, 18 U.S.C. 545 and 19 U.S.C. 1595a, providing CBP with broad authority to take enforcement action with regard to merchandise that is imported

contrary to U.S. law.) CBP officers also assist a wide variety of state, local, and tribal agencies with an interest in border security and in the enforcement of their laws. Such support could include, for example, intercepting fugitives wanted on state-issued felony warrants identified through the National Crime Information Center network. Furthermore, under the Immigration and Nationality Act (INA), CBP is responsible for determining the admissibility of aliens attempting to enter the United States. The term "engaged", as used in the SORN, indicates that the person may be involved in conduct that is in violation of U.S. law.

Question:

1(h) To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

Response:

Overall, ATS-P is only a decision support tool and a part of the larger admissibility process. It is not solely responsible for making any determinations; a CBP officer makes these determinations, taking into account several factors -- sometimes one of those factors is an ATS-P risk assessment. ATS-P does not produce an arrest or a denial of admission; those are a result of a CBP Officer's judgement and actions. In the past, CBP has provided to Congress and the general public statistics on arrests, contraband seizures, and persons refused admission to the country. It will continue to do so moving forward. It is important to stress, however, that these statistics are not a direct result of ATS-P. They are the result of determinations made by CBP officers using a variety of tools, including ATS-P.

2. Accessibility of Information Contained within the System

Question:

2(a) Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

Response:

No agency other than CBP has full access to all of the information contained in ATS-P. At the same time, CBP is obliged by acts of Congress and Executive Order to share terrorism-related information with other agencies. CBP meets these obligations by judiciously providing access to information in ATS-P to appropriate government personnel. CBP provides such access to other agencies only for a limited time and purpose, and usually related to a particular case, investigation, or threat. Personnel granted access must have proper, current clearances. Further, CBP regularly audits and reviews the process to ensure that access remains consistent with and relevant to stated purposes. See also CBP's answer to Question 2(e) for further discussions on MOUs and agreements in place governing access.

Question:

2(b) If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of

individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

Response:

CBP provides ATS-P information to sources outside of DHS to support security requests, and law enforcement and/or counterterrorism efforts. The information can be provided in reference to an individual passenger or a grouping of categories of individuals, depending upon the circumstances supporting the need for access. Some examples of groupings include all persons traveling on a specific flight on a specific date or range of dates; traveling to a specific city on a specific date or range of dates; or arriving at a specific port of entry at a specific date within a specific timeframe.

Question:

2(c) If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

Response:

The Privacy Act allows for information to be provided to contractors, grantees, experts, consultants, etc. "when [such access] is necessary to accomplish an agency function related to this system of record." As referenced in the ATS SORN, such sharing is considered a "routine use" pursuant to 5 U.S.C. 552a(b)(3). This reference was necessary to encompass non-government, contract employees who may need to receive limited access to assist in the development and maintenance of the system and its databases. Like DHS employees, these contractors complete fully adjudicated background investigations prior to beginning their contractual work. They also are required to sign a DHS non-disclosure agreement.

Question:

2(d) The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

Response:

This narrow routine use permits the effective sharing of data that could prove beneficial to law enforcement investigations. During the course of an investigation, it may become necessary for certain discrete information to be shared to obtain additional information from certain persons, such as informants and witnesses, without compromising the investigation. In most instances, information shared in such circumstances is covered by an appropriate non-disclosure agreement, which prohibits further use or dissemination of the subject information.

Question:

2(e) Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

Response:

As stated above, this routine use does not establish broad sharing arrangements or memoranda of understanding; instead, it authorizes the use of the information in the limited context of a law enforcement investigation. Without the exception, for example, it would be difficult to ask one member of a group under investigation whether he participated in past travel with another member of the group because the question would reveal information from ATS-P to a third party.

In the case of other government agencies, CBP (as well as its predecessor, the U.S. Customs Service) has MOUs and other formal mechanisms setting forth the conditions for access to, and use and dissemination of, CBP-provided data. Typical limitations applicable to other government authorities include "third agency rules" preventing disclosure of data without consent of the originating agency. Failure to abide by the terms of such agreements may result in CBP's revocation of access to such data, and depending upon the circumstances, could result in disciplinary, civil or criminal sanctions against an individual/entity. Furthermore, these agencies generally may only retain, store, or aggregate the data under the conditions and restrictions in those mechanisms described above.

For contractors and the like, access is covered by agreements that define the terms under which the data may be accessed and used (i.e., a non-disclosure agreement). To the extent access to ATS-P is provided, CBP insists, at a minimum, that an Interconnection Security Agreement (ISA) exists, describing how information must be secured and accessed.

3. Process for Correcting and Detecting Mistakes**Question:**

3(a) The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

Response:

A number of options are available to passengers who seek redress. In general, information in ATS-P is used to conduct further inquiries during inspection. If the information is incorrect, it can be corrected during that process. Furthermore, although

the SORN itself does not provide individual access to records under the Privacy Act, passengers may seek access under the Freedom of Information Act (5 U.S.C. 552) to certain data (namely their own PNR data) that is stored in ATS.

The ATS Privacy Impact Assessment (PIA) indicates additional procedures available through CBP for persons seeking to correct data in the system. For example, CBP has recently implemented a mechanism within its systems that permits a CBP officer to remedy issues related to the misidentification or inappropriate matching of passengers relative to watchlists. This redress process can be initiated at the port of entry after an inspection is completed, and it has been determined that the initial match was an incorrect one (i.e., a match based solely on a similar name match, but other information such as date of birth, passport number, or biometrics, etc., are not the same).

Additionally, CBP continues to review this issue of access for personally identifiable information, which includes addressing comments provided during the SORN comment period. DHS recently announced a new initiative known as the DHS Traveler Redress Inquiry Program (TRIP). Once implemented, TRIP will provide a further avenue for passenger redress. DHS TRIP was developed to provide a central gateway to address watchlist misidentification issues, situations where individuals believe they have faced screening problems at points of entry, or have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at our Nation's transportation hubs.

Question:

3(b) The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

Response:

The mechanisms currently available to correct inaccuracies are described in the response to the preceding question. As stated there, passengers are able, under FOIA, to gain access to their PNR data and seek to correct it if necessary.

4. Retention of Information

Question:

4(a) Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

Response:

CBP has provided a records schedule for ATS-P to NARA, but NARA has yet to approve it.

Question:

4(b) What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

Response:

The determination is based upon CBP's historical encounters with watch-listed suspects as well as information from the law enforcement and intelligence communities. It is known, for instance, that potential terrorists are patient. Individuals may travel to the United States several times without attempting a terrorist attack. As documented in the 9/11 and Terrorist Travel Staff Report of the 9/11 Commission, the 9/11 conspirators attempted to enter the United States 34 times over 21 months, through nine airports.

As a hypothetical example, a youth who has attended a terrorist training camp in one country could travel without notice annually over the next several years, if not decades, to the United States to potentially build networks, identify resources, or isolate and survey possible targets. Then, one day, actionable intelligence becomes available that points to the fact that a terrorist cell may be active and has operatives traveling annually from X point to Y in the United States to coordinate efforts. With ATS-P, CBP could take that actionable intelligence to develop threshold targeting rules and see if a person who matches the travel from X point to Y in the United States has done so annually. ATS-P would then identify the person described above as a person that warranted further scrutiny by a CBP officer. As this example illustrates, a longer active lifespan is crucial for ATS-P to be effective.

CBP continually reviews the effectiveness, reasonableness, and benefits of such information. Finally, CBP works very closely with other law enforcement and counterterrorism agencies, including the Department of Justice, and must ensure that its policies effectively support the needs of fellow agencies engaged in the enforcement of U.S. laws.

Question:

4(c) The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

Response:

In the course of determining the admissibility of those seeking to enter the country, CBP must take into consideration all security and applicable law enforcement concerns. This includes the everyday process of verifying the purpose and intent of people seeking entry into the United States. The relevance of particular ATS-P information may not be

immediately apparent without the proper contextual data, yet may prove invaluable when placed in context with other available information or intelligence. The exemptions included in the Privacy Act recognize that the nature of law enforcement investigations often does not permit an agency to determine whether or not a particular piece of information is relevant and necessary to a mission purpose at the time of collection or dissemination (see definition of "maintain" in 5 U.S.C. 552a(a)(3)).

I hope this clarifies some of your questions and provides you a better understanding of ATS-P and its critical role as a decision support tool to CBP. We, along with the Department, would be happy to brief you further on any or all of these items related to ATS-P. As indicated above, however, many of these issues are under active consideration at the Department and may be subject to changes in connection with our response to the ATS SORN and received comments. I thank you for your questions and the opportunity to respond to them.

Sincerely,



W. Ralph Basham
Commissioner