



**One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515**

January 17, 2007

Commissioner W. Ralph Basham
U.S. Department of Homeland Security
U.S. Customs & Border Protection
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20229

Re: Automated Targeting System

Dear Commissioner Basham:

On November 2, 2006, the Department of Homeland Security's Privacy Office published a Federal Register Notice, hereinafter referred to as the "SORN" (71 Fed. Reg. 64543) in an effort to provide expanded notice and transparency to the public regarding Custom and Border Protection's intention to continue utilizing the Automated Targeting System - Passenger (ATS-P) to screen passengers traveling in and out of the United States. I have since learned that this system, built on its predecessor the Treasury Enforcement Communications System (TECS), has been in existence, with respect to individuals, since approximately 1999, without any prior public notice. Following this revelation, several concerns arose with respect to the program which resulted in my staff traveling to the National Targeting Center to tour its facilities, meeting with representatives from the Government Accountability Office and the DHS Privacy Officer and a subsequent meeting with CBP representatives to further explore possible privacy and civil liberties violations arising out of the use of ATS-P. I appreciate CBP's assistance throughout this process, including its cooperation with my request to extend the public comment period to allow for further evaluation.

Although some of our concerns were alleviated following the afore-mentioned meetings, there still remain questions concerning the operation of ATS-P. I believe that the answers to the following questions are vital to further understanding the nature and implications of ATS-P. My questions fall under four main areas.

1. The "risk assessment" portion of the process

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.

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?

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

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?

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?

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 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?

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.* (emphasis added) 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?

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?

2. *Accessibility of Information Contained within the System*

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

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.

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

January 17, 2007

Page 3

working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

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?

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?

3. *Process for Correcting and Detecting Mistakes*

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?

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?

4. *Retention of Information*

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?

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?

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?

Thank you, in advance, for taking the time to answer these timely questions and for your cooperation on this matter. If you have any questions, please do not hesitate to contact Jessica Herrera-Flanigan, Democratic Staff Director & General Counsel, at (202) 226-2616.

January 17, 2007
Page 4

Sincerely,

A handwritten signature in black ink that reads "Bennie G. Thompson". The signature is written in a cursive style with a large, prominent initial "B".

Bennie G. Thompson
Chairman-elect
Committee on Homeland Security