PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

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

COMMENTS OF
REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN-DESIGNATE
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES
ON
DEPARTMENT OF HOMELAND SECURITY
PRIVACY OFFICE
PRIVACY ACT SYSTEM OF RECORDS NOTICE
FOR THE U.S. CUSTOMS AND BORDER PROTECION
AUTOMATED TARGETING SYSTEM

Docket No. DHS-2006-0060, Published Nov. 2, 2006,
Extended December 8, 2006

As Chairman-designate of the Homeland Security Committee, I am pleased to submit these comments on the November 2, 2006 Privacy Act System of Notice (SORN) regarding the Automated Targeting System, known as ATS.[1] These comments specifically concern the screening program for passengers, or ATS-P. In the SORN, the Department describes ATS-P as the screening system employed by U.S. Customs and Border Protection (CBP) for "identifying persons who 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."[2]

I appreciate the Department's decision to extend the comment period to December 29, 2006,[3] as I requested in my letter to the Secretary of December 4, 2006.[4] As explained in that letter, I am concerned that some elements of ATS-P may constitute violations of the privacy and civil liberties of U.S. citizens and lawful permanent residents (LPRs). A detailed staff briefing by CBP officers on December 11, 2006, has resolved some of those concerns, but I believe there remain several aspects of ATS-P itself that require further elaboration or revision. In addition to these comments, I have

[1] Department of Homeland Security, Privacy Office, Notice of Privacy Act System of Records, 71 Fed. Reg. 64543-46 (Nov. 2, 2006).
[2] Id. at 64545.
[3] Extension of comment period, 71 Fed. Reg. 71182.
[4] Letter from Rep. Bennie G. Thompson, Ranking Member of the House Homeland Security Committee, to Secretary Michael Chertoff (Dec 4, 2006).

also sent a letter to CBP Commissioner W. Ralph Basham with specific questions that I hope will clarify of number of issues regarding the program.[5]

At the outset, I want to state clearly that I value and strongly support CBP's efforts to screen passengers bound for the U.S. from abroad in order to identify persons "who 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."[6] Indeed, Congress has mandated that CBP conduct passenger screening, both under the Aviation and Transportation Security Act of 2001[7] and the Intelligence Reform and Terrorism Prevention Act of 2004.[8] The purpose of the screening is to ensure aviation security and, in the case of foreign citizens, to ensure that those who would do us harm or would engage in terrorist, criminal or other illegal activity are not admitted to the United States. However, any passenger screening systems utilized by CBP to achieve these legislative goals must not go beyond the letter or intent of the law by infringing upon the guaranteed rights of U.S. citizens.

I also have no objections to using automated systems for conducting name checks and performing identity-matching, as long as those systems adequately protect and control data against breaches of confidentiality and security. However, I do have some concerns about the type of data collected from passenger name records (PNR), as discussed below and with how the data collected on U.S. citizens and LPRs is analyzed, protected, shared, controlled and retained.

It has long been an established principle that when a Federal agency creates and maintains a system of records on U.S. citizens and LPRs, the Privacy Act requires that the agency must collect, use, disseminate and retain those records in the least invasive manner possible to accomplish the agency's mission.[9] In the case of CBP, that mission is border security, generally, and includes preventing terrorists from entering the United States, preventing terrorist attacks upon the United States or upon ships and airplanes traveling to the United States, and the enforcement of U.S. customs and immigration laws.

Without clear justification, however, CBP has exempted ATS-P from the Privacy Act provision that states that an agency shall only collect and maintain information about an individual that is "relevant and necessary" to accomplish a purpose required by statute or by executive order of the President to be accomplished by that agency. [10] Any government collection or record-keeping of personal data must be limited only to what is relevant and necessary to accomplish the government's authorized purpose, and that any exemptions to this rule must be narrowly applied.

---

[5] Letter from Rep. Bennie G. Thompson, Chairman-Designate of the House Homeland Security Committee, to Commissioner Basham (Dec. 28, 2006).
[6] 71 Fed. Reg. at 64544-45.
[7] 49 U.S.C 40101 et seq. *See also*,19 C.F.R. 122.
[8] 6 U.S.C. 101 et seq.
[9] See, generally, *Doe v. Chao*, 540 U.S. 614 (2004).
[10] 5 U.S.C. 552a(e)(1).

In the SORN, the Department states that ATS was built upon the predecessor database and screening system, the Treasury Enforcement Communications System (TECS), that was covered by a previous SORN.[11] CBP has explained that TECS was originally designed as a cargo screening system for the former U.S. Customs Service, but for many years has included a comprehensive database for screening passengers as well, known as the Interagency Border Inspection System (IBIS), used by the U.S. Border Patrol. Records contained in TECS are linked to individuals and retrievable from biographical information and therefore fall within the scope of the Privacy Act. According to the "IBIS Fact Sheet," attached to the Department's ATS Privacy Impact Assessment (PIA), IBIS provides CBP access not only to CBP records but also to the FBI's National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications Systems (NLETS), a law enforcement database used by all fifty states.[12] Moreover, the PIA explains that, in addition to CBP, law enforcement and regulatory personnel from 20 other federal agencies use IBIS, including the FBI, Interpol, DEA, ATF, the IRS, the Coast Guard, the FAA, the Secret Service and the Animal Plant Health Inspection Service.[13] IBIS is also shared with Department of State consular officers for purposes of visa adjudication.[14] From this description, it is fair to conclude that the TECS/IBIS database is a comprehensive tool used not only for screening people and cargo at the border, but also for general law enforcement.

ATS-P apparently differs from TECS in that it automatically screens passengers based on information already contained in the TECS/IBIS database, plus the PNRs collected by airlines in the normal course of making a reservation and APIS, currently submitted within 15 minutes of takeoff.[15] I understand that ATS automatically performs two critical screening functions: 1) it checks the identity of a passenger against government watch lists, including terrorist watch lists, and 2) it performs a risk assessment of every passenger to determine if he or she "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." If ATS finds a possible watch list match or determines from its risk assessment that the passenger may pose a possible risk to the flight or for other terrorist or criminal activity, the record is flagged for a personal review by a CBP officer at the National Targeting Center (NTC). The reviewing CBP officer then makes a determination as to whether the passenger should receive additional scrutiny, either before he or she boards a vessel bound for the U.S. or at the U.S. port of entry upon arrival. According to CBP, the additional scrutiny may include a more rigorous screening, such as more thorough questioning or a search of the passenger's person or possessions or increased examination of his or her travel documents. The result of this additional screening may include, depending on the circumstances, refusal to board, diverting or returning an airplane already in flight, refusal to admit the passenger (if a foreign citizen) into the United States or admission and arrest of the passenger. In the case of a passenger who may be of interest to law enforcement but determined not to be a

[11] 71 Fed. Reg. at 64544.
[12] Privacy Impact Assessment, p, 29, Appendix C IBIS Fact Sheet.
[13] Id.
[14] Id.
[15] 71 Fed. Reg. 64544; Privacy Impact Assessment at p. 4.

risk to the flight itself, CBP may take other appropriate action as a "routine use" of that information, to include sharing its ATS results and underlying information with any other Federal, State or local law enforcement, regulatory, or intelligence agency. The "routine uses" listed in the SORN indicate that CBP may either push the information to another agency on its own initiative, or it may respond to any request from another agency.[16]

The SORN is overly vague in its description of which authority allows CBP to conduct this risk assessment screening. The SORN sets forth CBP's authority over border security only in the most general way. It does not adequately distinguish between CBP's legal authority and processes to use ATS to screen cargo from its legal authority and processes to screen passengers. Further, it does not distinguish between its different treatment options for foreign citizens flagged as high risk and high risk U.S. citizens, whom CBP has no authority to exclude from the United States.

The SORN also does not describe CBP's legal authority to share an ATS-P risk assessment result performed on a U.S. citizen with any Federal, State, and local law enforcement, regulatory or intelligence agency as a routine use, even in cases where CBP has determined that the citizen or LPR poses *no risk* to a flight or ship and has admitted him or her into the United States. Such a practice of routinely sharing any and all information CBP has collected on U.S. citizens and LPRs for border screening and aviation safety purposes appears to go far beyond CBP's border security mission, especially in view of CBP's decision to retain this information for up to 40 years.[17] If there are other legal authorities that permit this routine sharing of personal data of U.S. citizens and LPRs, I believe all these authorities must be specified in the SORN so citizens and LPRs, Congress and courts can better assess whether CBP or its other agency partners have exceeded that authority.

Even if such broad authority beyond border security does exist, the apparent lack of any controls or protections on the sharing of ATS-P personal data, at least as the routine uses are described in the SORN, is troubling. During the aforementioned briefings, CBP officials specifically stated that ATS-P data is only shared with other agencies at the request of the agency and only on an individual passenger or specific route basis. It was further stated that the data is not accessed on an aggregate or large-scale basis by other agencies. Notwithstanding these assurances, at a minimum, any further dissemination of this extensive personal data, either on CBP's initiative or upon request, must be documented regarding who is the requestor, what is the legal justification for receiving the data, for what purpose will the data be used, and how it will be protected from further disclosure. No such safeguards appear in the SORN. Without an established, authorized and transparent legal process to share personal data of persons protected under the Privacy Act, all the ATS data and indeed the entire TECS/IBIS database could be used as a warrantless well of evidence from which any law enforcement, regulatory or intelligence agency could dip at will -- without any probable cause, reasonable suspicion, or judicial oversight. The PIA says that Memoranda of Understanding (MOU) and other agreements are in place to govern further dissemination

[16] 71 Fed. Reg. at 64545.
[17] Id. at 64546.

outside of DHS, but, at least with respect to law enforcement, intelligence and regulatory agencies, no details of these agreements are provided.[18] Without adequate safeguards, these routine uses as described in the SORN may constitute violations of the U.S. Constitution's Fourth Amendment guarantee against unreasonable searches and seizures.

CBP has maintained, however, that U.S. citizens and LPRs should have no constitutionally protected expectations of privacy in PNR and APIS data since they freely give PNR information over to airlines when they make reservations, and APIS biographical data from passports already exist in the U.S. Government's records, such as passport records. I strongly disagree. Looking at all the many data points contained in PNR, as set out in the SORN, it is obvious that much of the collected data is exactly the kind of information that passengers desire to keep private, for example, credit card information, frequent flyer numbers, email addresses, billing and telephone numbers.[19] That this information is given to reservation agents for the sole purpose of buying a ticket in a secure business transaction does not abolish this expectation. Nor does the fact that airlines must, by law, give PNR and APIS data to CBP for the purpose of security screening change the fact that the passenger should be able to control who sees this data beyond those necessary to permit the completion of his or her travel.

In submitting a reservation request, the passenger is not relinquishing all control of their private data nor signaling that he or she wants to make this data public knowledge for all purposes. Americans and LPRs have an expectation that this information is being utilized for a discrete purpose. An expectation of privacy exists in the PNR and APIS data, and CBP is obligated to safeguard it against unwarranted disclosures. Indeed, CBP seems to acknowledge this in the SORN's description of internal safeguards it has imposed for its own personnel. There is no indication, however, that any of these safeguards apply to non-DHS law enforcement or regulatory agencies who may be tempted to troll through an individual's personal data for evidence rather than to request a proper subpoena for the information. If CBP does employs safeguards on outside disclosures as a routine use, those procedures need to be spelled out in the SORN so the public can be assured their privacy rights are not being violated.

Moreover, the breadth and detail of the PNR data raises another concern, namely, that particular data points collected and analyzed may lead to discrimination based on, for example, religion or disability, in violation of the civil rights of U.S. citizen and LPR passengers. For example, the PNR data described in the SORN would contain a request for a special meal to comply with religious dietary restrictions or a special accommodation for a disability. Both CBP officials and the DHS Chief Privacy Officer have ensured my staff that any data related to religion or disability is blocked, and thus not included in the ATS risk assessment, and the PIA supports this claim. There is nothing in the SORN, however, to indicate any restrictions on the collection of PNR data. Given the amount of detailed information that makes up PNRs, I strongly urge CBP in the interest of transparency, CBP should inform Americans which categories of data that are collected are blocked or excluded from the automated risk assessment.

[18] Privacy Impact Assessment, pp. 15-16.
[19] Id. at 64544.

The automated risk assessment process itself also suffers from lack of transparency. Beyond checking identities against watch lists, which would obviously flag a high risk passenger, the process and data points for flagging passengers for greater CBP scrutiny based on a computerized "risk assessment" that remains invisible to the public. As such, it has stirred understandable anxiety among citizens who have no way of assessing the objectivity or reliability of the process, which has been described as everything from data-mining to risk-scoring in the press. Oral briefings by DHS officials, have clarified that ATS-P is neither a scoring nor a data-mining process; they have described the assessment as a "flag/no flag" result based on a "links analysis," i.e., looking at links between data in the TECS, PNR and APIS data and known or suspected terrorist activity. They have explained that the relevant factors are determined by counterterrorism experts and as such, are constantly changing as facts on the ground change and more information becomes known. I was reassured that there is no indiscriminate "data-dumping" or "data-mining," but that the risk analysis evaluates each traveler for specific factors or combinations of factors that have been determined by experts to signal a need for a second look by CBP. While a good cause can be made for the non-disclosure of the relevant factors themselves, else they could be defeated, a more transparent description of the process itself would reassure Americans that their personal data is being evaluated narrowly and thoughtfully and not indiscriminately.

Another problem with the SORN is the lack of an adequate justification for retaining information collected in ATS for up to 40 years.[20] To date, no Department official has been able to provide a satisfactory explanation regarding CBP's conclusion that 40 years of data may be required "to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities."[21] Remembering that this data is collected for border security screening purposes, and not to serve as a general domestic law enforcement evidence repository, it seems patently excessive to assert that the data on every single citizen and LPR, no matter how many times they have entered and exited the country lawfully and not been "flagged," remains relevant because some link might exist between 40-year-old data and new travel.

With respect to the right to access information, the SORN seems to say that individuals will not be able to access ATS-P records on themselves to inspect them for accuracy and request modifications if inaccurate information exists.[22] This essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about his or herself, again without clearly stating the justification. The PIA explains that since ATS-P collects no new information, but only uses data from other sources, individuals should seek access and redress from the various agencies that provide source data upon which ATS-P operates, such as the PNR, TECS or APIS, for example.[23] The ATS-P SORN should incorporate this explanation because, as written, a citizen is left believing there is no way

[20] 71 Fed. Reg. at 64546.
[21] Id.
[22] 71 Fed. Reg. at 64546.
[23] Privacy Impact Assessment, Sec. 7.0, pp. 16-20.

to access and seek redress for erroneous information, and the instruction to send Privacy Act inquiries to the Customer Satisfaction Unit only adds to this confusion.

Finally, the SORN does not explain how ATS-P operates with respect to passengers exiting the United States, although it repeatedly describes ATS as a system to screen inbound and outbound persons and cargo.[24] The exit portion of ATS-P should be elucidated in any revision to the SORN.

Thank you for the opportunity to file these comments. If you have any questions about these comments, please contact Jessica Herrera-Flanigan, Democratic Staff Director and General Counsel of the Committee on Homeland Security at (202) 226-2616.

Bennie G. Thompson
Chairman-Designate
Committee on Homeland Security

[24] 711 Fed. Reg. 64543-44.