Before the

PRIVACY OFFICE
DEPARTMENT OF HOMELAND SECURITY

Washington, DC 20528

Privacy Act of 1974, System of Records Notice (SORN), DHS/CBP–006, "Automated Targeting System (ATS)"	DHS-2006-0060 **COMMENTS OF** **THE IDENTITY PROJECT (IDP)** **AND JOHN GILMORE**

The Identity Project (IDP)

<http://www.PapersPlease.org>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

The Identity Project submits these comments in response to the Privacy Act of 1974, System of Records Notice (SORN) for records system DHS/CBP–006, the Automated Targeting System (ATS), published at 71 Federal Register 64543-64546 (November 2, 2006), docket number DHS–2006–0060.

The stated purpose of the system of records is expressly forbidden by the Department of Homeland Security Appropriations Act, 2007, Title V, Sec. 514. The SORN would impermissibly include records describing how individuals exercise rights of assembly and other rights guaranteed by the First Amendment, is factually inaccurate, omits many of the categories of individuals about whom information would be (and perhaps already is being) collected and fails to give the required notice to data subjects, and would constitute a criminal violation of the Privacy Act by the responsible agency officers or employees.

The Identity Project respectfully requests that the proposed system of records not be created or, if it has been created already, that the data contained in it and in all backups and copies be destroyed.

I. ABOUT THE IDENTITY PROJECT

The Identity Project (IDP), <http://www.PapersPlease.org>, provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

II. THE STATED PURPOSE OF THE AUTOMATED TARGETING SYSTEM (ATS) SYSTEM OF RECORDS IS EXPRESSLY FORBIDDEN BY CONGRESS.

The Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441), provides in Title V, Sec. 514 (e), a copy of which is attached as an appendix to these comments, "None of the funds provided in this or previous appropriations Acts may be utilized to develop or test algorithms assigning risk to passengers whose names are not on Government watch lists." Previous DHS appropriations acts have similar provisions. This SORN violates that prohibition. While Sec. 514(a) prohibits "the deployment or implementation, on other than a test basis, of the Secure Flight program or any other follow on or successor passenger prescreening program" until "all of the conditions contained in paragraphs (1) through (10) of section 522(a) of Public Law 108-334 (118 Stat. 1319) have been successfully met," which they to date have not, Sec. 514(e) unequivocally and without limitation to the Secure Flight program prohibits the development or testing of "algorithms assigning risk to passengers whose names are not on Government watch lists." The prohibition is placed upon the Department of Homeland Security and not limited to domestic passenger data. In fact, because Sec. 514(e) stands separate from 514(a), prohibits testing where 514(a) does not, and makes no mention of Secure Flight, 514(e) is much broader in scope than 514(a).

The proposed ATS system of records would violate this prohibition. According to the SORN, the "ATS builds a risk assessment for ... travelers based on criteria and rules developed by CBP [DHS Bureau of customs and Border Protection]. ATS maintains the resulting assessment.... This assessment

and related rules history associated with developing a risk assessment for an individual are maintained for up to forty years to support ongoing targeting requirements." 71 Federal Register 64544. There is no indication in the SORN that these records or risk assessments are limited to individuals whose names appear on Government watch lists.

Even if one were to argue that Sec. 514(e) does not apply to ATS, or that ATS is not within the meaning of "any other follow on or successor passenger prescreening program" as defined in Sec. 514(a), the algorithms assigning risk to passengers in the Secure Flight program are arguably the same as those contemplated by this SORN. By cloaking this prohibited action in a border issue, and by not even publicly recognizing the manifest operational overlap here, the Department of Homeland Security directly and openly contravenes Congress' clear intent. Further, in the routine uses section of the SORN, sub-section N, DHS is specifically describing what Sec. 514(e) prohibits.

Since the function of this records system is expressly forbidden by Congress, the SORN should be immediately and expressly withdrawn, and any records or data already collected or being maintained pursuant to it, or for this forbidden purpose, along with any copies or backups, should be immediately destroyed.

III. THE DATA COLLECTED IMPERMISSIBLY INCLUDES THAT OF DOMESTIC TRAVEL.

PNR's for international flights can, and often do, contain data about domestic travel within the USA. According to the SORN, the ATS may include the entire PNR, including "All travel itinerary for specific PNR". A PNR can contain data on any number of sequential flights, including connecting flights as well as flights separated by surface ("ARNK") segments. This could include multiple domestic flights prior or subsequent to the international leg in the same PNR, including flights that do not connect from or to international flights and neither originate nor terminate at international gateways.

In addition, information in PNR's for purely domestic journeys within the USA could be included in "Split/Divided PNR information" in ATS records, if the person(s) making such a domestic journey was originally included in the same PNR as, and was then split or divided into a separate (cross-referenced) PNR from, someone whose journey included an international leg.

The Government's collection of domestic PNR information, as envisioned by the long shelved Secure Flight program, is clearly impermissible (see again Sec. 514(a)). Because the collection of international PNR information would be inextricably intertwined with the domestic PNR information, the collection of either is impermissible.

IV. THE ATS SYSTEM WOULD INCLUDE RECORDS DESCRIBING HOW INDIVIDUALS EXERCISE RIGHTS OF ASSEMBLY AND OTHER RIGHTS GUARANTEED BY THE FIRST AMENDMENT, WITHOUT STATUTORY AUTHORIZATION.

The Privacy Act of 1974, 5 U.S.C. 552a(e)(7), provides that:

> Each agency that maintains a system of records shall - ... maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

As we have explained in comments filed with this Department in other rulemaking proceedings, travel necessarily incorporates the act of assembly, a right specifically protected by the First Amendment. See "Passenger Manifests for Commercial Aircraft Arriving in and Departing From the United States; Passenger and Crew Manifests for Commercial Vessels Departing From the United States", Comments of the Identity Project, et al., before the Bureau of Customs and Border Protection, Department of Homeland Security, docket USCBP-2005-0003 (October 12, 2006), available at <http://hasbrouck.org/IDP/IDP-APIS-comments.pdf>. Travel records such as Passenger Name Records (PNR's) thus are, directly and by definition, records of our acts of assembly.

PNR's "describe how any individual exercises rights guaranteed by the First Amendment" in numerous ways. One PNR can contain reservations for an entire group of people traveling and assembling together. Multiple PNR's for people traveling and assembling together can be cross-referenced to indicate their association, even when they are traveling from different places. PNR's for travel by members of organizations frequently identify their organizational affiliations through discount eligibility codes, particularly through unique meeting codes (included in ticketing information and other PNR data categories) that identify a specific assembly. PNR's record with whom we assemble, when and for how long we assemble, where and from where we assemble, and how (by exactly what means of transport) we assemble, among other details of our acts of assembly.

None of the exceptions to the Privacy Act's prohibition on keeping of records about the exercise of rights protected by the First Amendment applies in this case. First, any claimed statutory authorization for the maintenance of such a system of records is, at most, implied, not express. No statute mandates the collection or retention by the DHS of PNR data. In fact, as detailed earlier in these comments, the claimed purpose of the ATS system is expressly forbidden by the most recent Department of Homeland Security Appropriations Act, as well as by multiple similar prior acts. Second, the maintenance of these records could hardly be considered authorized by the individuals about whom the records are maintained. The DHS has provided no mechanism to obtain consent, or to permit individuals to "opt out" or prevent the inclusion of records about them in the system. On the contrary, the DHS has proposed to exempt this system of records from even the limited requirements of the Privacy Act for accuracy, relevance, access, and so forth. Third, the system expressly includes all travelers (and, although it fails to give them notice, many other categories of individuals), without any limitation to those who are the target of any law enforcement activity.

To invoke the law enforcement exemption to the protections of the Privacy Act, there must exist some degree of individualized suspicion. A blanket requests for all records of a particular type is not permissible. Therefore, DHS is generally, and specifically regarding the collection of data concerning how individuals exercise First Amendment rights, violating the Privacy Act if their stated exemption to its protections here is "law enforcement".

Accordingly, the inclusion in the ATS system of PNR's data or any other data concerning how individuals exercise rights of assembly or other rights protected by the First Amendment is forbidden by the Privacy Act. Any such data that has been collected, and any copies or backups, should be destroyed. The system of records should be modified to exclude such data, and a new SORN should be published.

V. THE SYSTEM OF RECORDS NOTICE IS FACTUALLY INACCURATE.

According to the SORN, "the Automated Targeting System ... was previously covered by the Treasury Enforcement Communications System 'System of Records Notice.' .... This system of records notice does not identify or create any new collection of information."

This claim is false.

The most recent SORN for the Treasury Enforcement Communications System (TECS) was published at 66 Federal Register 52983 at 53029 (October 18, 2001). There is no mention in that SORN for the TECS system of any use of this data to generate "risk assessments" or for "targetting", as disclosed for the first time in this SORN for the ATS records system.

In addition, the SORN for the TECS system describes the "categories of records in the system" as: "Every possible type of information from a variety of Federal, state and local sources." This reference to "Federal, state, and local sources" clearly implies Federal, state, and local *government* sources. There is no mention in the SORN for TECS of data from non-governmental, commercial sources such as the airline reservation systems that are the source of Passenger Name Records (PNR's), whose inclusion in these records is disclosed for the first time in the SORN for the ATS records system.

The false and misleading claim in the SORN for the ATS system that it does not identify or create any new collection of information appears designed to cover up the apparent fact that the previous SORN for the TECS system was deficient, and that the ongoing collection of categories of data such as commercial data, and uses of that data such as for creation of risk assessments and targeting, not disclosed in that SORN, have been in violation of the Privacy Act.

VI. THE ATS SORN FAILS TO GIVE THE NOTICE REQUIRED.

5 U.S.C. 552a(e)(4)(B), the Privacy Act of 1974, requires that the SORN include "the categories of individuals on whom records are maintained in the system". But the SORN for the ATS system of records omits large categories of individuals about whom the ATS system, as described in that SORN , would contain personally identifiable information.

The SORN discloses that the ATS system of records will cover "A. Persons seeking to enter or exit the United States; ... and D. Persons who serve as operators, crew, or passengers on any vessel, vehicle, aircraft, or train who enters or exits the United States."

But the SORN also discloses that the ATS will include airline Passenger Name Records (PNR's). PNR's contain personally identifiable information on numerous other categories of individuals, not mentioned in the SORN or given the required notice that they are included in the ATS system.

Among those additional categories of individuals not mentioned in the SORN, about whom PNR's and thus the ATS system would contain information, are the following:

A. Travel arrangers, personal assistants and administrative staff, travel managers, group coordinators, event organizers, and family members and friends assisting with travel arrangements, as identified by the “received from” field in the PNR (acknowledged in the SORN as one of the PNR data categories included in the ATS system) that records the person who requested the creation of the reservation or the most recent change to it.

B. People who pay for tickets for others, or who hold joint credit or debit cards with people who purchase travel for themselves or others – whether or not they travel themselves – as identified from the “form of payment” fields in ticketing records in PNR’s (again, a category of PNR data acknowledged in the SORN as included in the ATS system).

C. Friends, family members, hosts, housemates, domestic partners, and business associates of travellers, as identified from the "local contact" and "document delivery" information in PNR's (which may include phone numbers, descriptions of the relationship of the contact to the traveller, and in some cases addresses).

D. Travel industry personnel, including travel agents and airline reservation, check-in, and ticketing staff, as identified by the unique “agent sine” or log-in ID in the PNR and by the city or “pseudo-city” (airline office or travel agency branch or location) and the LNIATA or “set address” of the terminal or data connection on which the entry was made (the CRS or airline hosting system counterpart of an Internet IP address).

E. Clients, customers, and employers of travellers, even if they aren’t travelling, as identified by billing and accounting codes for travel by others undertaken on their behalf or at their expense. Corporate travel agencies routinely include codes in PNR’s to indicate to the traveller (or the traveller’s employer) to which department, project, or client the cost of the trip is to be billed. In the case of a law firm, these entries routinely identify the specific client, case, or matter on whose behalf or at whose expense the travel was undertaken. Thus clients of law firms, consultants, financial advisors, and other professionals are routinely the subject of data in PNR’s, and thus could be the subject of data (including legally privileged data) in the proposed system.

In order to avoid a violation of the Privacy Act, or terminate the ongoing violation if the ATS system of records containing PNR's has already been created, a revised SORN should be published as soon as possible to give these categories of individuals the notice to which they are entitled.

VII. MAINTENANCE OF THE ATS SYSTEM OF RECORDS WOULD CONSTITUTE A CRIMINAL VIOLATION OF THE PRIVACY ACT ON THE PART OF THE RESPONSIBLE AGENCY OFFICERS OR EMPLOYEES.

The Privacy Act of 1974, 5 U.S.C. 552a(I)(2), provides that: "Any officer or employee of an agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor."

As discussed immediately above, the SORN for the ATS system does not meet the notice requirements of 5 U.S.C. 552a(e)(4) with respect to the categories of individuals on whom records are to be maintained in the system. As a result, willful maintenance of the ATS system containing data from PNR's concerning any categories of individuals other than individuals actually travelling, would be a criminal violation of the Privacy Act of 1974, 5 U.S.C. 552a(I)(2), on the part of each officer or employee of any agency willfully participating in such maintenance.

VIII. CONCLUSION AND RECOMMENDATIONS

The stated purpose of the system of records, the assignment of "risk" scores to all international air travellers to and from the USA, is expressly forbidden by the Department of Homeland Security Appropriations Act, 2007. The proposed system of records would impermissibly include records describing how individuals exercise rights of assembly and other rights guaranteed by the First Amendment, without express statutory authorization. The SORN is materially inaccurate, omits many of the categories of individuals about whom information would be (and perhaps already is being) collected and fails to give the notice to data subjects required by the Privacy Act, and maintenance of the proposed system of records would constitute a criminal violation of the Privacy Act on the part of the responsible agency officers or employees.

The Identity Project respectfully requests that the proposed system of records not be created and, if it has been created already, that the data contained in it and in all backups and copies be destroyed.

Respectfully submitted,

The Identity Project (IDP)

<http://www.PapersPlease.org>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

/s/

Edward Hasbrouck,

Consultant to IDP on travel-related issues

James P. Harrison

Staff Attorney, First Amendment Project

Director, IDP

John Gilmore

Post Office Box 170608

San Francisco, CA 94117

December 4, 2006

APPENDIX

Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441)

TITLE V: GENERAL PROVISIONS

SEC. 514. (a) None of the funds provided by this or previous appropriations Acts may be obligated for deployment or implementation, on other than a test basis, of the Secure Flight program or any other follow on or successor passenger prescreening program, until the Secretary of Homeland Security certifies, and the Government Accountability Office reports, to the Committees on Appropriations of the Senate and the House of Representatives, that all ten of the conditions contained in paragraphs (1) through (10) of section 522(a) of Public Law 108–334 (118 Stat. 1319) have been successfully met.

(b) The report required by subsection (a) shall be submitted within 90 days after the Secretary provides the requisite certification, and periodically thereafter, if necessary, until the Government Accountability Office confirms that all ten conditions have been successfully met.

(c) Within 90 days of enactment of this Act, the Secretary shall submit to the Committees on Appropriations of the Senate and the House of Representatives a detailed plan that describes: (1) the dates for achieving key milestones, including the date or time frames that the Secretary will certify the program under subsection (a); and (2) the methodology to be followed to support the Secretary's certification, as required under subsection (a).

(d) During the testing phase permitted by subsection (a), no information gathered from passengers, foreign or domestic air carriers, or reservation systems may be used to screen aviation passengers, or delay or deny boarding to such passengers, except in instances where passenger names are matched to a Government watch list.

(e) None of the funds provided in this or previous appropriations Acts may be utilized to develop or test algorithms assigning risk to passengers whose names are not on Government watch lists.

(f) None of the funds provided in this or previous appropriations Acts may be utilized for data or a database that is obtained from or remains under the control of a non-Federal entity: Provided, That this restriction shall not apply to Passenger Name Record data obtained from air carriers.