Privacy Impact Assessment for the

Screening of Passengers by Observation Techniques (SPOT) Program

August 5, 2008

Contact Point
Michael Kimlick, Branch Chief,
Behavior Detection and Travel Document Validation Branch, Screening Operations Division
Transportation Security Administration

Reviewing Officials
Peter Pietra, Director
Privacy Policy & Compliance
Transportation Security Administration

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Abstract

The Screening of Passengers by Observation Techniques (SPOT) program is a behavior observation and analysis program designed to provide the Transportation Security Administration (TSA) Behavior Detection Officers (BDOs) with a means of identifying persons who pose or may pose potential transportation security risks by focusing on behaviors indicative of high levels of stress, fear, or deception. The SPOT program is a derivative of other behavioral analysis programs that have been successfully employed by law enforcement and security personnel both in the U.S. and around the world.

Overview

Section 114 of the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, November 19, 2001, 115 Stat. 597) grants TSA the responsibility for security in all modes of transportation. Specifically, Section 114(f) grants the TSA Administrator authority to "receive, assess, and distribute intelligence information related to transportation security" as well as to "assess threats to transportation." SPOT is one means by which TSA fulfills that responsibility by enabling BDOs in the field to report individuals exhibiting behaviors possibly indicative of terrorist activity for referral to selectee screening or Law Enforcement Officer (LEO) intervention. The SPOT program relies on BDOs trained to detect involuntary physical and physiological reactions that may indicate stress, fear or deception regardless of race, gender, age, or religion.

TSA will collect two categories of information. Under the first category, BDOs will enter observations of behavior into a SPOT report (hard-copy or through a personal digital assistant (PDA)) that will be entered into the SPOT database that may reveal trends across airports or over time within a single airport. These reports will not contain personally identifiable information (PII) and the reports will be destroyed once the information is entered into the SPOT database. Under the second category, individuals whose behavior exceeds a threshold of behavioral indicators may be referred for additional screening or LEO intervention. In these instances, the BDO may collect personally identifiable information to check the individual's identity against intelligence, terrorist, and law enforcement databases, and to provide information for use in trend analysis. Terrorist acts that threaten transportation security are most vulnerable in the planning stages and the timely passage of SPOT referral information may assist in identifying such efforts before they become operational. Accordingly, BDOs may submit information (observations or PII based reports) to the Federal Air Marshal Service for analysis within the Transportation Information Security System (TISS) as discussed in the TISS PIA. TISS incidents are not input to the SPOT database since it does not contain PII .

Because this system entails the collection of information about members of the public in identifiable form, TSA is conducting this Privacy Impact Assessment (PIA) under the E-Government Act of 2002, Public Law 107-347 Section 208.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

TSA will collect two categories of information. The first is information about observed behaviors. The information is anonymous since BDOs do not have PII at the time that the observed behaviors are detected. The information is recorded either on a hard-copy or electronic SPOT report that is then inputted into a TSA SPOT database. Hardcopy reports are destroyed after the information is entered into the database. Information fields within the SPOT report include general information such as time, date, airport, geographical location, flight information, departure and arrival destinations, reason(s) for referral, LEO actions, and detected behaviors.

The second category is information collected when observed behaviors exceed certain thresholds. In this event, PII will be collected and reported in accordance with normal checkpoint incident reporting protocols including TSA headquarters and field location systems. TSA may collect:

- first, middle, and last names;
- aliases and nicknames;
- home and business addresses and phone numbers;
- employer information;
- identification numbers such as Social Security Number, drivers license number or passport number;
- date and place of birth;
- languages spoken;
- nationality;
- age;
- sex;
- race;
- height and weight;
- eye color;
- hair color, style and length; and
- facial hair, scars, tattoos and piercings, clothing (including colors and patterns) and eyewear;
- purpose for travel and contact information;
- photographs of any prohibited items, associated carry-on bags, and boarding documents;
- identifying information for traveling companion.

BDOs may also receive information alerts from a variety of sources, including such sources as the DHS Daily Operations Report, the FBI Most Wanted List, the ICE Most Wanted List, and the National Center for Missing and Exploited Children (NCMEC) alerts.

1.2 What are the sources of the information in the system?

The sources are BDOs who either observe behaviors or collect information directly from individuals, law enforcement officers, airport stakeholders, airline personnel and witnesses to the event(s). A source may also be information alerts passed to BDOs, as mentioned above.

1.3 Why is the information being collected, used, disseminated, or maintained?

This information is collected to identify threats to transportation security. The information is used to identify individuals, actions, patterns, or trends that may indicate preoperational terrorist activity.

1.4 How is the information collected?

BDOs directly input their observations onto SPOT reports and into the SPOT database, which does not contain PII. It is also collected from LEOs who obtain it directly from the individual during the preparation of an incident report. BDOs may also receive information alerts during briefings or through electronic means.

1.5 How will the information be checked for accuracy?

BDOs undergo extensive training in the behaviors they are observing prior to being assigned to BDO duties. BDO training emphasizes the importance of accurate data collection to the integrity of the system. Information regarding behavior is input directly by the BDO observing the behaviors. PII may be collected directly from the individual or from a LEO.

1.6 What specific legal authorities/arrangements/agreements define the collection of information?

TSA has broad responsibility for transportation security across all transportation modes and to assess threats to transportation under the Aviation and Transportation Security Act (ATSA) 49 USC §114. TSA is also responsible for screening persons and property carried aboard passenger aircraft by an air carrier or foreign air carrier under 49 USC §44901, and promulgated certain regulations at 49 CFR § 1540.105, 1540.107.

1.7 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The SPOT program is designed to identify individuals who may pose a threat to transportation security. This requires the collection of information that varies depending on the circumstances. Privacy risks are mitigated by 1) conducting surveillance in public places on behaviors that are generally evident to any observer; 2) not collecting PII unless certain thresholds of suspicious activity are met; and 3) strictly limiting system access to authorized program personnel. PII collected for purposes of preparing an incident report is not entered into the SPOT database, but is maintained by TSA for enforcement or analysis purposes. The SPOT database does not contain any PII (including demographic information such as age, sex, or race).

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

Information collected will be used to evaluate whether the individual should undergo secondary screening. If warranted, TSA may identify the individual to a LEO for a law enforcement interview or other action. BDOs use the information to create SPOT reports and input the data into the SPOT database. Information may be communicated within TSA to respond operationally, evaluate for trends or patterns, or for matching against intelligence, law enforcement, or immigration databases. This may include forwarding pertinent information to units within the Federal Air Marshal Service (FAMS) or to federal, state, or local entities for further analysis or information purposes in accordance with the Transportation Information Sharing System (TISS) PIA. PII may also be maintained in databases within TSA field offices or the Office of Security Operations for analysis or enforcement action.

2.2 What types of tools are used to analyze the data and what type of data may be produced?

The SPOT program will perform statistical analysis of the data for purposes of preparing reports. In addition, data may be input into TISS for pattern identification as discussed in the TISS PIA.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Commercial or publicly available data is not used.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Access to the SPOT database is limited to authorized program personnel. Statistical reports are prepared and provided to TSA personnel with a need for the information in the performance of their duties. SPOT information is protected and handled as Sensitive Security Information (SSI) under 49 CFR Part 1520. All users that have access to the system have unique user names and passwords, and must sign User Account Authorization acknowledging user obligations for safeguarding materials and monitoring of use. Audits of the system are conducted periodically to ensure proper use of the system.

Section 3.0 Retention

3.1 What information is retained?

All SPOT report information and PII obtained during the preparation of an incident report is retained.

3.2 How long is information retained?

Hard copy SPOT reports are retained only so long as required to input the data electronically into the SPOT database Electronic records in the SPOT database are expected to be retained for 15 years. Information from encounters that generate an incident report are entered into TISS or other TSA headquarters or field office systems and will be retained in accordance with that system's National Archives and Records Administration (NARA) approved retention schedule.

3.3 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The SPOT database retention schedule is pending approval by NARA. No records will be destroyed until the retention schedule is approved by NARA.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Information collected by SPOT is kept for a reasonable time considering the need to develop statistical data on potential threats to transportation security. Hard copy records are retained only so long as necessary to input the information into a secure restricted access database. Encounters that generate incident reports are retained for varying periods of time tailored to the purposes for which the systems were created. They range from 3 years for certain aviation security systems to 25 years in the TISS system.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations are the information shared, what information is shared and for what purpose?

Information contained in the SPOT database is expected to be shared with the Transportation Security Operations Center (TSOC), TISS, Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS), and the Office of Intelligence (OI). It will also be used to generate statistical reports for TSA leadership and supervisors. Information may also be shared with other offices that have a need for the information in the performance of their duties, such as the Office of Chief Counsel, Office of Security Operations, Office of Civil Rights and Liberties, Office of Legislative Affairs, Office of Inspection, and the Privacy Office. Suspicious activity reports, including PII where it is available, would be shared with TSOC, TISS, and OI for purposes of identifying suspicious activity trends across airports or over time. It may be shared with other offices to respond to complaints or inquiries, perform oversight or audit functions, or as part of the civil/criminal enforcement process.

Information contained in the SPOT database may be shared with DHS employees and contractors who have a need for the record in the performance of their duties, including but not limited to law enforcement or intelligence operations. This information will be shared in accordance with the Privacy Act of 1974, 5 USC § 552a.

4.2 How is the information transmitted or disclosed?

Information is shared subject to SSI handling restrictions, including password-protection of email, but may also be transmitted by telephone or fax.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy risks associated with internal sharing include security of the information and limiting access to individuals with a need to know. The risk of sharing this information with an individual without a need to know has been mitigated by access controls, including passwords and real-time auditing that tracks access to electronic information. The risk has also been mitigated by collecting PII from only a small proportion of individuals; that is, only those individuals identified by BDOs as exceeding certain thresholds of suspect behaviors.

Section 5.0 External sharing and disclosure

5.1 With which external organizations are the information shared, what information is shared, and for what purpose?

Information may be shared with local enforcement if the individual is identified as someone in a law enforcement, intelligence or immigration database. The information will be shared for purposes of identifying threats or individuals who are sought by law enforcement or immigration authorities.

5.2 Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DHS?

Yes, PII collected as part of the SPOT program is covered by TSA's Privacy Act system of records, DHS/TSA 001 Transportation Enforcement Records System (TSERS). This system of records has several routine uses which allow TSA to share information outside of the Department. For example, routine use 3 permits TSA to share information with appropriate outside agencies regarding individuals who pose or are suspected of posing a risk to transportation or national security.

5.3 How is the information shared outside the department and what security measures safeguard its transmission?

Information is shared outside DHS by voice or electronic transmission directly to the LEO investigating the incident. The information is Sensitive Security Information (SSI) and is subject to handling safeguards in 49 CFR Part 1520.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and how they were mitigated.

Misidentification of the individual is a risk associated with external sharing. Given the involvement of a LEO, however, it is expected that sufficient information will be collected to mitigate this risk.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

No. BDO observations of suspicious behaviors or activity are contemporaneously recorded so there is no opportunity to give notice. The BDO has no prior knowledge that the behavior or activity is going to occur, and has no ability to give notice that the information is going to be gathered. PII will only be collected from individuals whose actions exceed specified thresholds delineated in the SPOT Standard Operating Procedures and notice under these circumstances is exempt under the Privacy Act.

6.2 Do individuals have an opportunity and / or right to decline to provide information?

Information contained in the SPOT database is based primarily upon observations which are not susceptible to an opportunity to decline, and casual conversation which may be terminated at any time by the individual without consequence to the individual. If an individual is referred to a LEO, their ability to decline is subject to law enforcement protocols.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is not provided to the individual during the behavior observation. Risks are mitigated by not collecting PII unless the behaviors rise to certain levels.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their own information?

While much of the information in the system is exempt from release under the FOIA and Privacy Act, individuals may request access to their information pursuant to the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 CFR Section 5.21 by submitting a Freedom of Information Act / Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20, West Tower
FOIA Division
601 South 12th Street
Arlington, VA 22202-4220

FOIA / PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: http://www.tsa.gov/public/contactus). The FOIA / PA request must contain the following information: Full Name, current address, date and place of birth, telephone number, and email address (optional). Privacy Act requesters must either provide a notarized and signed request or sign the request pursuant to penalty of perjury, 28 U.S.C. §1746. Please refer to the TSA FOIA web site (http://www.tsa.gov/public).

7.2 What are the procedures for correcting inaccurate or erroneous information?

To the extent record access is granted under the FOIA/PA, individuals may request correction of their personal information in this system of records in accordance with the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 CFR Section 5.26.

7.3 How are individuals notified of the procedures for correcting their information?

DHS has published procedures to request amendment of records at 6 CFR Section 5.26.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Individuals may request access or amendment of their records in the SPOT database in accordance with the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 CFR Section 5.21.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to the individual and how those risks are mitigated.

Individuals may request access to and amendment of their personal information contained in this system in accordance with the Privacy Act and the DHS Privacy Act regulation, however, much of the information in the system is exempt from release under the FOIA and Privacy Act as law enforcement or intelligence information, and may also be SSI exempt from disclosure under 49 USC §114(s).

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

Only designated employees of TSA's TSOC, OLE/FAMS, and OI have "view only" access to the SPOT database for trend analysis and risk assessment or other need-to-know purposes. This includes system administrators, security administrators, and other persons within TSA or DHS who have a need-to-know access to the system or information contained in the system in the performance of their duties. The procedures are not documented but are strictly controlled by the SPOT program Branch Chief or his designees. Incident reports that are entered into other systems are also limited to authorized users.

8.2 Will Department contractors have access to the system?

Yes. Contractors have access to the system for system maintenance and security assessments, but not as SPOT database users. Contractors have signed appropriate non-disclosure agreements and agreed to handle the information in accordance with the Privacy Act of 1974, as amended.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

DHS privacy training is mandated for all TSA employees and contractors. In addition, privacy and civil rights training tailored to the program is part of the training provided to all BDOs.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Information in the SPOT database system is safeguarded in accordance with the Federal Information Security Management Act of 2002 (Pub. L. 107-347) (FISMA), which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. Authority to Operate was granted on August 9, 2006.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Systematic network and system monitoring is in place to detect intrusions. Role-based security is used to prevent unauthorized use of the information, including improper printing or editing of data.

The TSA Office of the Chief Information Security Officer (OCISO) performed a formal risk assessment on the SPOT database system against the information asset data, i.e., the information held within the SPOT database system, in accordance with NIST Special Publication, 800-30, Risk Management Guide for Information Technology Systems. A formal risk assessment was completed by the TSA OCISO on July 24, 2006.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do security controls mitigate them?

Data in the SPOT database system is secured in accordance with applicable federal standards, including systematic network and system monitoring is in place to detect intrusions. Security controls are in place to protect the confidentiality, availability, and integrity of the data, including role-based access controls to that enforce a strict need to know policy. Each user is given a unique login name and password and audit trails are maintained and monitored to track user access and detect any unauthorized use.

Section 9.0 Technology

9.1 What type of project is the program or system?

The project is a security system based on human observation of suspicious behaviors.

9.2 What stage of development is the system in and what project development lifecycle was used?

The project is operational.

9.3 Does the project employ technology which may raise privacy concerns? If so please describe their implementation.

No.

Responsible Officials

Michael Kimlick, SPOT Program Manager
Behavior Detection and Travel Document Validation Branch
Screening Operations Division,
Office of Security Operations

Approval Signature Page

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security