Privacy Impact Assessment for the Airport Access Authorization To Commercial Establishments Beyond The Screening Checkpoint (AAACE) Program

April 5, 2007

Contact Point
Robert J. Cammaroto
Manager, Airports Policy Branch
Commercial Airports
Transportation Sector Network Management
Transportation Security Administration
Bob.Cammaroto@dhs.gov

Reviewing Official
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov

Approving Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
privacy@dhs.gov

Abstract

The airport operating authorities at Dallas-Fort Worth International Airport (DFW) and Detroit Metropolitan Wayne County Airport (DTW) have established the Airport Access Authorization To Commercial Establishments Beyond The Screening Checkpoint (AAACE) Program. Under this pilot program, each airport operator may issue an Authorization Form to current registered overnight hotel guests (Registered Guest) at certain hotels physically connected to the airport terminal, who have requested access to commercial establishments beyond the screening checkpoint in the sterile area of the airport if they meet the requirements of the program. This Privacy Impact Assessment (PIA) is being amended to reflect that additional airports may participate in the pilot under the same conditions described in the original PIA. The additional airports will be identified in Appendix B but will otherwise not be identified in the text.

Introduction

TSA has broad authority under 49 United States Code (U.S.C.) §§ 114(f) and 40113(a) to assess threats and threat information and to plan and execute such actions as may be appropriate to address threats to transportation. TSA has determined that the implementation of certain security measures, briefly discussed herein, is necessary to permit registered guests to access beyond the screening checkpoints at DFW and DTW, in order to visit commercial establishments.

Each adult and any minor, under 18 years old and staying with an adult, must be a registered guest to be eligible to participate in the AAACE Program. Upon registration at a participating airport hotel, the hotel front desk staff will inform the guest about the AAACE Program. If the guest elects to participate, the hotel will arrange for the guest to meet with an airport law enforcement officer (LEO). The LEO will provide the guest with an information document which explains the program and contains a Privacy Act Statement. The guest must provide the LEO with his/her full name and date of birth. The LEO will examine the guest's government-issued photographic identification (ID) to verify the individual's identity and confirm that the guest is registered at the hotel as well as obtain the guest's room number. The LEO will record the guest's name, hotel room number, and date of birth on an Authorization Form, made up of two sections.

At both airports, the registered guest's name will be compared against the No-Fly List. The No-Fly List is maintained by the Terrorist Screening Center (TSC). The TSC maintains responsibility over the Federal Government's consolidated terrorist watch lists, including the No-Fly List, in an integrated database known as the Terrorist Screening Database (TSDB). The No-Fly component of the TSDB is the basis for the checks conducted by the airport operators. Under this pilot program, TSA will allow DFW and DTW airport operators access to the No Fly List in order to carry out the watch list screening function for registered hotel overnight guests who desire to participate in the AAACE Program. The airport will report any matches to TSA.

At DFW and DTW, those individuals who meet the program's participation requirements will be issued the date-stamped upper portion of an Authorization Form by the LEO in order to pass through security. The upper portion of the form contains the individual's name, date of birth, room number, the date of issuance and, in the case of a minor, the name(s)of the adult(s) who may accompany the minor. [1] The registered

[1] For minors participating in the pilot program, a registered overnight adult hotel guest, whose name appears on the

guests must surrender the upper portion of the Authorization Form to a Transportation Security Officer (TSO) at the security screening checkpoint prior to the commencement of the screening process. The LEO will complete the bottom portion of the Authorization form certifying that the individual is/is not authorized to participate in the AAACE Program, date-stamp the form, and provide this bottom portion of the form to TSA.

If there is a possible match to the No-Fly List, in accordance with current protocols applying to air carriers, airport operators may request additional information to resolve any possible matches. If the airport operator determines that there may be a match to the No-Fly List, the operator will refer the name to TSA for resolution of the possible match and/or for operational response. No Authorization Forms will be issued where there is a positive match to the No Fly List, the guest status has not been verified, or the ID found unacceptable.

The information collection in this program is paper-based. Technical access and security considerations do not apply to this collection; however, appropriate paper-based security measure will be taken with this information. Because this program entails a new collection of information about members of the public in an identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 requires that TSA conduct a Privacy Impact Assessment (PIA).

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

A LEO will collect the registered overnight hotel guest's name, room number, and date of birth and compare the name, date of birth, and the individual's identification against the No-Fly List. Adult registered guests will be required to present valid government-issued photo identification to the LEO or airport operator representative in order to verify the individual's identity. In most cases, the personal information provided on the government-issued identification will be sufficient to allow the LEO to eliminate the possibility that the individual is a person on the No–Fly List.

1.2 From whom is information collected?

The LEO will collect the personally identifying data directly from the registered guest and will provide TSA with the name and personal identifying information of any individual who is a match to the No-Fly List.

The LEO will provide TSA with the bottom portion of all Authorization Forms.

1.3 Why is the information being collected?

The purpose of collecting this information is to enable security measures to be undertaken with respect to the issuance of an Authorization Form that allows individuals, who are registered guests at certain hotels

---

minor's Authorization Form, must accompany the minor to the security screening checkpoint and wait until notified by TSA that the minor has successfully completed the screening process. Minors need only present the Authorization Form and surrender it to the TSO.

that are physically connected to the airport terminal, to access the sterile areas of the airport in order to visit commercial establishments beyond the screening checkpoint. TSA is also collecting the information to audit the performance of the airport operator under this program.

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

Under 49 U.S.C. §§ 114(f) and 40113(a), TSA has broad authority to issue regulations to carry out its statutory functions. TSA has issued Transportation Security regulations (TSRs) which, among other things, establish security obligations of airport operators. Airport operator security requirements contained at 49 CFR Part 1542 apply to airport operators identified at 49 CFR § 1542.1. Pursuant to this authority, TSA is requiring airport operators at DFW and DTW to collect and compare the names and personally identifying data of individuals who are registered guests at designated hotels and are seeking access to commercial establishments beyond the screening checkpoint against the No-Fly List.

1.5 Privacy Impact Analysis:

For purposes of conducting No-Fly List comparisons, TSA will receive the names and personally identifying data of positive or potential matches to the TSA No-Fly List. This process is consistent with the current protocols applicable to air carriers. Because the registered guests will be able to provide any additional identifying information, it is expected that positive matches reported to TSA will be rare. Additionally, TSA will receive the guest's name and date of birth by retaining the upper portion of the Authorization Forms that registered guests present prior to entering the screening checkpoint as well as the bottom portion of those form that are provided by the LEO and Airport Representative. For purposes of program auditing, TSA will retain both portions of each Authorization Form for not more than seven days after the Authorization Form's issuance date. TSA will retain each Authorization Form of those individuals who are positive or potential matches to the No-Fly List for one year after the conclusion of the pilot program. Limiting the information received by TSA serves the agency's operational purposes while minimizing the privacy risks for individuals who use this means for access to the sterile areas of an airport.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

The information collected is used to determine whether an individual is eligible to participate in the AAACE Program.

If, after comparing the registered guest's name against the No-Fly List the LEO determines there is a possible match, TSA will be notified for resolution and/or possible operational response. Any individual who is a positive match will not be issued an Authorization Form. TSA will use the information concerning registered guests who are positive matches to the No-Fly List for the purpose of identifying actual or potential threats to transportation security, as well as individuals who seek to test access controls to the sterile area.

The Authorization Form may also be used to audit the performance of the airport operator by periodically reviewing the Authorization Forms from all individuals admitted to the sterile area under this program. TSA will discard the Authorization Forms after seven days (see Section 3.1).

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The LEO will collect information directly from the registered guest. Adult registered guests must present valid government-issued photo identification in order to obtain an Authorization Form to allow them access to commercial establishments beyond the TSA security checkpoint. Further, prior to undergoing screening, they must also present, at the screening checkpoint, a valid government-issued photo identification that matches the information on the Authorization Form which is an added assurance that the information is accurate. The LEO will transmit the identifying information concerning suspected No-Fly List matches directly to TSA in order to resolve the suspected match.

2.4 Privacy Impact Analysis:

Because the personal information is collected directly from the individual in person at the airport, and the individual must present a valid government-issued photo identification, the risk of collecting inaccurate information is minimized. Individuals who feel they have been wrongly identified as a positive match to the No-Fly List can seek redress through TSA.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

TSA will retain the data it receives in accordance with record schedules to be approved by the National Archives and Records Administration (NARA). TSA proposes to retain any issued Authorization Forms for individuals who are not found to be a match to the No-Fly List for not less than three and no more than seven days, which it has determined is a sufficient retention period for purposes of program auditing and incident response. TSA proposes to retain any Authorization Forms which are generated but not issued for individuals who are found to be a match to the No-Fly List for one year after collection of the information. Data on positive or suspected No-Fly and other watch list matches will be kept in accordance with TSA's proposed retention schedule for these records. Until these schedules are approved, TSA will not destroy any records.

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

The applicable record retention schedule covering data on positive or suspected No-Fly and other watch list matches is pending approval by NARA. The applicable record retention schedule for information obtained from individuals for audit and incident response purposes will be submitted to NARA.

3.3 Privacy Impact Analysis:

Information collected through this program will be maintained in accordance with NARA-approved record retention schedules in furtherance of TSA's mission to ensure the security of the Nation's transportation system. The expected retention schedule for Authorization Forms will allow only for a minimal retention period for program audit purposes. The expected retention schedule for data on positive or suspected No-Fly and other watch list matches will be the minimal period necessary to facilitate litigation and intelligence needs. The privacy interest is furthered by minimal data retention.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

This information is generally not shared outside of TSA, however, as noted in Section 4.2, the information TSA receives 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 provisions of the Privacy Act, 5 U.S.C. § 552a.

4.2 For each organization, what information is shared and for what purpose?

TSA will receive the registered guest's name and date of birth by retaining the Authorization Form that the guest presents prior to entering the screening checkpoint. TSA will also receive information on any registered guest seeking access to commercial establishments beyond the screening checkpoint at the airport when information matches the No-Fly List and the LEO contacts TSA for operational response. If there is a match or possible match against the No-Fly list, TSA may share the registered guest's name and date of birth within DHS for intelligence, counterintelligence, law enforcement, or other official purposes related to transportation or national security in accordance with the provisions of the Privacy Act.

4.3 How is the information transmitted or disclosed?

Depending on the specific situation and need, TSA may transmit this data to DHS employees and contractors who have a need for the record in the performance of their duties in person, in paper format, via facsimile, telephonically, or electronically via a secure data network. This method of transmission may

vary according to specific circumstances. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

4.4 Privacy Impact Analysis:

Information may be shared with DHS employees and contractors who have a need for the record in the performance of their duties in accordance with the Privacy Act. Privacy protections may include strict access controls and audit trails to track user access, unauthorized access attempts, and mandated training for all employees and contractors.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

Under this pilot program, TSA will enable the DFW and DTW airport operators access to the No Fly List in order to carry out the watch list screening function for registered guests who wish to access commercial establishments beyond the TSA security checkpoints of these airports. If a registered guest's name comes up a match on the No Fly List, TSA will share information with the Terrorist Screening Center (TSC) and other agencies in connection with the resolution of possible name matches and any operational response. TSA may share the information it receives on individuals who are matches to the No-Fly List with Federal, state, or local law enforcement, intelligence agencies, with the airport operator, or other entities pursuant to the Privacy Act and in accordance with the routine uses identified in the applicable Privacy Act system of records notices (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS), and DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operations Files. These SORNs were last published in the Federal Register, respectively, on November 8, 2005, and can be found at 70 FR 67731-67735, and on December 10, 2004, and can be found at 69 FR 71828, 71835.

5.2 What information is shared and for what purpose?

TSA will share the No-Fly List with the airport operators to carry out the watch list screening function. If the airport operator determines that there may be a match to the No-Fly List, the operator will refer the name to TSA for resolution of the possible match and/or for operational response. It is expected that individually identifying data and No-Fly List status will be shared to communicate the access status with the airport operator and to facilitate an operational response. This information may also be shared for intelligence, counterintelligence, law enforcement, or other official purposes related to transportation or national security and in accordance with the routine uses identified in the applicable SORNs DHS/TSA 002, Transportation Threat Assessment System (T-STAS), and DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operations File.

5.3 How is the information transmitted or disclosed?

Depending on the recipient and the urgency of the request or disclosure, the information may be disclosed in person, in paper format, via facsimile, telephonically, or electronically via a secure data network.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

There is no MOU. The Privacy Act System of Records Notice described above provides the necessary guidance for sharing of the information.

5.5 How is the shared information secured by the recipient?

Any Federal agency receiving this information is required to handle it in accordance with the Privacy Act, the Federal Information Security Management Act (FISMA), and their applicable SORNs. Airport operators are required to treat No-Fly List information as Sensitive Security Information subject to the handling requirements under 49 CFR Part 1520.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No specific training is required by TSA. Federal agency employees typically are required to undergo Privacy Act training by their employing agencies

5.7 Privacy Impact Analysis:

TSA will share possible matches and matches to the No-Fly list under the applicable provisions of the SORNs and the Privacy Act. Privacy risks are mitigated by the protections offered by the Privacy Act and TSA policies on disclosure of personally identifying information.

Section 6.0
Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Individuals will receive a Privacy Act Statement included in an information document explaining the program from a LEO or airport operator representative at the time they wish to undergo the clearance process. If an individual believes that the decision by the airport operator representative is based upon inaccurate information, he or she will be informed of how to pursue redress from TSA. The publication of this PIA and of the SORNs for DHS/TSA 002, Transportation Threat Assessment System (T-STAS), and

DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operations Files, also serve to provide public notice of the collection, use and maintenance of this information.

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

Yes, this process is voluntary. Nevertheless, TSA will not allow registered guest to participate in the AAACE Program unless they meet participation requirements, which include showing a valid government issued ID, verifying that the individual is a registered overnight hotel guest at a specified hotel and comparing the individual's name against the No-Fly List

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:

The limitation on the information received by TSA serves the agency's operational purposes while minimizing the privacy risks for individuals who use this program for access to the sterile areas of the airport. Registered guests participating in this program will be able to provide any additional identifying information to the LEO, if necessary, to distinguish the individual from a name on the No-Fly List. Because the individual can contemporaneously provide this information, it is expected that positive matches reported to TSA will be rare.

Section 7.0
Individual Access, Redress and Correction

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

Individuals may request access to their information 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,
Freedom of Information Act Office, TSA-20
11th Floor, East Tower
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by email at FOIA.TSA@dhs.gov. The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA Web site (http://www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting erroneous information?

Individuals may request correction of their information in two ways. First, the LEO may request additional information directly from the participating registered guest in order to rule out a possible match to the No-Fly List. In addition, a TSA redress process will be available to assist individuals who feel that they have been wrongfully denied access beyond the TSA screening checkpoint. Individuals will be notified of the redress process on the information document explaining the program that they receive from the LEO. The individual may contact the TSA Contact Center at 1-866-289-9673 or TSA-ContactCenter@dhs.gov for assistance. During the redress process, it may be necessary for TSA to collect additional information from the individual in order to facilitate the redress process, including notarized copies of identification documents, such as a birth certificate or passport. If TSA needs such additional information in order to continue the process, the individual will be notified in writing. The information requested will be the minimum necessary to complete the redress process.

In addition to the redress process, the individual may also request correction of the records pursuant to the Privacy Act. While the system of records in which actual or potential matches to the No-Fly List are maintained is subject to certain exemptions under the Privacy Act, TSA may decide to amend these records when appropriate. Such requests should be sent to the address noted in paragraph 7.1 above.

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

Individuals will be notified of the redress process on the information document that they are given, which will provide the telephone number for the TSA Contact Center. Individuals may contact the TSA Contact Center for assistance, as noted in paragraph 7.2.

7.4 If no redress is provided, are alternatives available?

A redress process is provided for individuals who believe that they have been wrongfully denied access beyond the TSA security checkpoint based on the watch list screening process.

7.5 Privacy Impact Analysis:

Because the LEO will collect information directly from the individual, the risk of collecting inaccurate information is minimized. In addition, individuals may request access to or correction of their personal information pursuant to a redress process and pursuant to the Privacy Act.

Section 8.0
Technical Access and Security

The information collection in this program is paper-based. IT based technical access and security considerations do not apply to this collection.

8.1 Which user group(s) will have access to the system?

N/A.

8.2 Will contractors to DHS have access to the system?

N/A.

8.3 Does the system use "roles" to assign privileges to users of the system?

N/A.

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

N/A.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

N/A.

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

N/A.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

N/A.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

N/A.

8.9 Privacy Impact Analysis:

N/A.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

This program uses a paper-based system for collecting information on AAACE program participants. Because of the very limited personal information collected and the limitations on this pilot program in general, TSA does not have a need to use an electronic system.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

TSA made the conscious decision to collect only the minimum personal information necessary to conduct the No-Fly List comparison, and TSA will retain this information for the minimal retention period necessary for audit, intelligence and investigative purposes in accordance with the NARA-approved record retention schedules. Only the LEO collects and compares the participating registered guest's personal information to the No-Fly List. TSA receives information concerning positive matches to the No-Fly List, as well the Authorization Forms issued or generated in order to audit the performance of the airport operator. (The Authorization Forms are not part of, nor do they become a part of the system.) The TSA system is designed to allow for collection of only those data elements necessary to allow TSA to complete its tasks. Additional information is only requested as needed and in the vast majority of cases, a limited initial set of information will be sufficient to eliminate the possibility that the individual is a person on the No-Fly List.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA will collect the minimal personal information necessary to conduct the No-Fly List comparison. TSA will not transmit or otherwise share this information with entities outside of DHS that are not listed in the routine uses in the TSIS or T-STAS Privacy Act System of Records Notices, which were published in the Federal Register. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent abuses.

9.4 Privacy Impact Analysis:

The conscious design choices in section 9.3 will limit access to the personal information, thereby mitigating any possible privacy risks associated with this program.

Conclusion

TSA is establishing this program to accommodate requests from airport operating authorities to allow registered overnight hotel guests participating in this program access to commercial establishments beyond

the screening checkpoint that would not otherwise be readily available to them during their stay at the airport, while balancing security concerns associated with permitting such access. TSA will use this limited personal information provided to assist airport operators in the resolution of possible matches and to facilitate an operational response to actual matches to the No-Fly List. TSA will retain the Authorization Form according to the approved NARA record schedule for purposes of program auditing.

Responsible Official

Robert J. Cammaroto
Manager, Airports Policy Branch
Commercial Airports
Transportation Sector Network Management, TSA

Reviewing Official Signature

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

Approving Official Signature

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Privacy Act Statement

AUTHORITY: 49 U.S.C. § 114(f).

PRINCIPAL PURPOSE(S): This information is collected by airport operators or their representatives in order to conduct checks of TSA's No Fly List on individuals who are registered overnight guests at designated airport hotels who wish to access commercial establishments located beyond the screening checkpoint. TSA may receive this information from airport operators or their representatives in order to resolve suspected or actual matches to this database.

ROUTINE USE(S): TSA may share this information with aircraft and airport operators, foreign air carriers, or appropriate Federal, State, or other agency regarding individuals who pose or are suspected of posing a risk to transportation or national security, or for other routine uses identified in TSA system of records, DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS) and DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operations Files.

DISCLOSURE: Voluntary; failure to furnish the requested information may result in your inability to access facilities located in the airport beyond the screening checkpoint.

APPENDIX B

List of participating airports

Pittsburgh International