Transportation Security Administration

Airport Access Control Pilot Project

Privacy Impact Assessment

June 18, 2004

Contact Point:

Lisa S. Dean
Privacy Officer
Transportation Security Administration
571.227.3947

Reviewing Official:

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security
202.772.9848

Airport Access Control
Pilot Project
Privacy Impact Assessment

I. Introduction

On November 18, 2001 Congress passed the Aviation and Transportation Security Act (PL 107-71). The statute directed the newly-formed Transportation Security Administration (TSA) to "establish pilot programs in no fewer than 20 airports to test and evaluate new and emerging technologies for providing access control and other security protections for closed or secure areas of the airports. Such technology may include biometric or other technology that ensures only authorized access to secure areas." (See PL 107-71 Section 106(d)(3) codified at 49 U.S.C. 44903(c)(3)).

The purpose of TSA's Airport Access Control Pilot Program (AACPP) is to implement pilot projects at airports to evaluate and demonstrate applications of new and emerging technologies that enhance the performance of access control systems. Access controls are used to ensure that unauthorized persons cannot gain access to sensitive areas in airports or gain access to air cargo stored in sensitive areas in air transportation facilities (e.g: warehouses, hangers, and other buildings that are usually at an airport).

Since the focus of the project is on the testing of technologies with the voluntary collection of a limited amount of personal data being an incidental component needed to conduct the testing, the impact to personal privacy will be minimal. However, in the interest of transparency to the public, TSA decided to conduct this Privacy Impact Assessment (PIA) pursuant to the E-Government Act of 2002, P.L. 107-347, and the accompanying guidelines issued by the Office of Management and Budget (OMB) on September 26, 2003. This PIA is based on the current design of the program and the Privacy Act system of records notice, Transportation Security Technology Testing System (DHS/TSA 016), that was published in the Federal Register on July 1, 2004. This PIA provides further details about the collection of personally identifiable information for the purpose of evaluating and demonstrating applications of new and emerging technologies.

The AACPP received proposals from 55 airports that are interested in volunteering for the project. Altogether, the airports proposed 325 different technology vendors who market variations of certain technologies. Of the different technologies proposed, the AACPP grouped them into 5 general categories: Biometric devices (including fingerprint recognition, voice or word recognition, iris scans, hand geometry recognition), intrusion surveillance and tracking (including Radio Frequency ID tags and intelligent video systems), door controls (including access control card readers), anti-tailgating (preventing persons from sneaking in behind authorized people by using intelligent video, and optical license plate readers to detect automobiles) and "other," which consisted of interesting but difficult to categorize ideas.

During the period of the pilot project, TSA will choose which technologies it would like to assess for access control purposes, and the AACPP will set up the access point and demonstrate the effectiveness of the chosen technologies. The demonstration will rely on the participation of volunteers who work at the airport and will use the access technology being tested. The program will monitor the experience of these volunteers and will utilize surveys to request feedback on the technology. Limited personal information about the volunteers will be collected and used during this pilot; however, none of this information will be collected or used to make determinations that will affect individual rights. The program will also not have an impact on anyone who does not volunteer to participate.

The end result of the project will be a report to TSA that will describe all of the technologies that were tested in at least 20 airports. The report will serve a threefold purpose:

- For TSA, the AACPP report will contain a body of field-proven knowledge to assist in developing performance standards and in determining what kinds of access control technology are acceptable for use in sensitive areas in airports or other air transportation facilities. Aviation security solutions need to vary in order to accommodate the needs of a large number of airports of various sizes and vulnerabilities. The body of field-proven knowledge that results from this project will enable TSA to approve security systems and designs that can be tailored to individual airport needs.

- For stakeholders (airports in particular), the AACPP report will facilitate the deployment of advanced access control technology. The results of this project will enable stakeholders to confidently design security solutions tailored to their individual needs and budgets, drawing upon the field-proven technology that was demonstrated under this project. This flexibility in meeting regulatory security standards is a high priority for stakeholders.

- For manufacturers of emerging technologies, portions of the AACPP report can be used as a guide for tailoring advanced access control technologies to meet the demands of the airport environment.

II. System Overview

• What information will be collected and used for this pilot project?

The information to be used and collected under this project consists of: full name, year of birth, gender, ethnic background, primary language, employer, and airport identification badge number of a select group of volunteer participants (airport or air carrier employees and contractors, airport users, and federal workers) who have access to secure areas of an airport (and in two cases, access to air cargo stored in secure areas of air cargo storage facilities).

Additionally, at sites that are testing biometric devices, a biometric identifier will be collected from participants in the program. In order for AACPP to analyze the performance of the devices at access points leading into secure areas of an airport, the participants will use the device whenever they attempt to enter these areas. The AACPP will then review how well the device works and how well the participants adjusted to the device. In conducting such a review, the AACPP may have reason to contact the participant for information. As a result, the AACPP needs to have a method of identifying who the participants are. Normally, this will be done through the participant's airport identification badge number, which will be recorded every time a participant uses the device. The AACPP may need to contact the participant for a number of reasons, including the following:

- If, during the pilot, the technical data collected indicates to the AACPP that a participant has experienced unique difficulties while interacting with a device, the AACPP can use the participant's identifying information in order to contact the participant to get more specific information about the difficulties that were experienced. For example, in a project demonstrating the effectiveness of a fingerprint reader, participants will enroll in the project by submitting a fingerprint sample to the system. If technical data later indicates that one participant continues to experience a "bad read" by the fingerprint reader, the AACPP can extract the participant's badge number from the raw data collected and ask the airport to use the badge number to identify the participant. AACPP can then contact the participant to determine why the fingerprint reader is having trouble recognizing that participant's fingerprint sample (the participant's fingerprint sample may have been enrolled improperly). In all cases, submission of identifying data to the AACPP is voluntary, and anyone who has been invited to be a participant in the pilot project is free to decline.

- Midway through the project, the AACPP may want to interview some participants to determine their perceptions of the project. While perceptions do not indicate how well a device actually works, they can shed light on the acceptability of a device by the persons using it. In some cases, if the participants have to follow a few extra steps before gaining access to a secure area, but they feel that the added steps are worth the effort to keep the area safe, a particular device may be easier to introduce at an airport for widespread use.

- Some technologies do not effectively identify people with certain physical characteristics. It is well documented, for instance, that certain fingerprint technologies do not effectively recognize the fingerprints of certain ethnic groups. If a pilot device indicates an unusually high number of "bad reads" for one participant, the AACPP may want to look at the participant's voluntarily-submitted demographic information to determine whether he or she falls into a known category of persons for which that particular technology isn't best suited. This is also seen in word recognition technology being used by persons who speak English as a second language. Use of this personal information will help AACPP determine whether the device being demonstrated is malfunctioning, or whether it is not performing well because of outside influences such as ethnic background or language barriers.

In all instances when personal information is used, the AACPP is using the information to determine how well a device is functioning as well as the pros and cons of deploying a device in a location that must accommodate a large number of persons. The AACPP's interest, then, is to determine the ultimate operational suitability of a technology for use by many people; other than determining how well a device works, or whether a device is malfunctioning or simply reacting to a demographic anomaly, AACPP has no other interest in personal information of participants, and will not use it for any other purpose.

- **Why is the information being collected and how are participants affected?**

The information is being collected in order to evaluate the performance of the access control systems being demonstrated at each site. Participants are not affected personally, except that they may be contacted by AACPP and asked their opinions about the device being demonstrated and whether they find it easy to use.

- **What information technology system(s) will be used for this program and how will they be integrated?**

The AACPP will deploy Data Observation Collection Kits (DOCKs) at all airport sites where technologies are being demonstrated. These kits receive highly technical operational data (raw data, such as mean-time between failures, temperature, and the date and time a device was used) from an integration panel connected to the devices being demonstrated. The DOCKs at every location record the raw data received and transmit it to a central data repository located at the AACPP headquarters in Reston, Virginia. AACPP personnel then review the raw data to determine how well the devices are working. The system also records such things as whether a device would have permitted access to a participant if it were actually deployed by an airport as part of its security system, and how long it took for the transaction to take place. Malfunctions of any devices will also be recorded and analyzed.

Neither the DOCKs nor the Central Repository are integrated into any other information system. No information from the DOCKs or from the Central Repository can be obtained from any outside system. Only AACPP personnel with a need to know will have access to the information recorded by the DOCKs or stored in the Central Repository

- **What notice or opportunities for consent are provided to individuals regarding what information is collected, and how that information is shared?**

In its Privacy Act System of Records Notice, Transportation Security Technology Testing System (DHS/TSA 016), TSA provided notice that it will collect personally-identifying information. relating to the Transportation Security Technology Testing System. This PIA provides additional notice about the program. TSA intends to provide further notices to individuals at the time the information is collected. Individuals' participation in the AACPP program is entirely voluntary.

- **Does this program create a new system of records under the Privacy Act?**

Yes. This program is covered under a Privacy Act system of records that is being established concurrent with this notice, called the "Transportation Security Technology Testing System," or DHS/TSA 016.

- **With whom will the collected information be shared?**

The collection, maintenance, and disclosure of information will be in compliance with the Privacy Act and the published system of records notice. TSA's contractor is likewise obliged to comply with the Privacy Act pursuant to 5 U.S.C. 552a(m).

- **How will the information be secured against unauthorized use? (What technological mechanism will be used to ensure security against hackers or malicious intent?)**

TSA will secure personal information against unauthorized use through the use of a layered security approach involving procedural and information security safeguards. The data will be encrypted using National Institute of Science and Technology (NIST) and Federal Information Security Management Act (FISMA) standards and industry best practices when being transferred between secure workstations.

When transferring information between the end user's browser and the web, TSA will use Secure Socket Layer (SSL) 128-bit encrypted sessions for data integrity and privacy. Once user data has been obtained at the web server, it will be transferred to a TSA database server over an encrypted session.

Specific privacy safeguards can be categorized by the following means, which are described in greater detail elsewhere in this document:

- Technical limitations on, and tracking of, data access and use;
- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

This approach protects the information in accordance with the following requirements:

- The Privacy Act of 1974, as amended (5 USC 552a), which affords individuals the right to privacy in records that are maintained and used by Federal agencies.
- Federal Information Security Management Act of 2002, (Public Law 107-347), which establishes minimum security practices for Federal security systems.

- **Will the information be retained and if so, for what period of time?**

TSA proposes to maintain the raw data and accompanying records generated by the AACPP for 10 years, pending approval by the National Archives and Records Administration (NARA). The records being retained, however, will not contain any personal identifiers of the participants. AACPP will remove and destroy personal identifiers form the data at the end of the project.

- **Will the information collected be used for any other purpose other than the one intended?**

Information collected will only be used for the purpose of evaluating the technology being tested at each site under the AACPP pilot program.

- **How will the pilot participants be able to seek redress?**

For purposes of this pilot, TSA will not make any determinations that affect individual rights for which redress is required; additionally, all participants are volunteers. Procedures for Privacy Act requests for access to information in the system are as follows:

To determine if this system contains a record relating to you, write to the system manager at the following address: Director of the Security Technology Office, TSA Headquarters, TSA-16, 601 S. 12th Street, Arlington, VA 22202-4220. Please provide your full name, current address, date of birth, place of birth, and a description of information that you seek, including the time frame during which the record(s) may have been generated. You may also provide your Social Security Number or other unique identifier(s) but you are not required to do so. Individuals requesting access must comply with the Department of Homeland Security's Privacy Act regulations on verification of identity (6 CFR 5.21(d)).

- **What databases will the names be run against?**

DHS will not run the names of pilot participants against any database.

- **What is the step by step process through which the systems will work once the data has been input and what is the process for generating a response?**

AACPP will input the participant information (an airport badge number, along with a biometric identifier in places where a biometric device is being demonstrated) into the system being demonstrated at each site. For a period of 90 days per site, the participant will present his or her biometric identifier (a fingerprint, for instance) to a reader, and then follow regular airport procedures in order to gain access to a secure area. Because the devices in this program are being demonstrated, they are not connected to an airport's actual access control system. In this way, if the device cannot read a fingerprint, or an iris scan, or whatever biometric identifier is needed for the demonstration, a participant will not be prevented from entering an area if he or she otherwise is granted access by the airport's system. In most cases where a device cannot read a biometric identifier, the device will prompt the participant to try again. Even if the device cannot identify the participant, the participant ultimately will be given a signal (usually a green light or an audible tone) indicating that the participant may proceed into a secure area after following the airport's standard access procedures.

AACPP has an interest in the number of times a device fails to read a biometric identifier as well as the number of times it recognizes them. Therefore, all of the attempts to use the device are recorded by the DOCK and sent to the Central Repository. AACPP will review the raw data to

evaluate the performance of the device. Participants can expect to be contacted by AACPP during the 90-day period of the demonstration and asked their opinions of the device being demonstrated. At the end of the pilot period, any leftover equipment (not clear what this refers to), the AACPP report, and associated raw data (with personal identifiers removed) will be provided to TSA.

- **What technical safeguards are in place to secure the data?**

DHS employs the following technical safeguards to secure data:

- Use of advanced encryption technology to prevent internal and external tampering of the raw data.
- Secure data transmission including the use of password-protected e-mail for sending files between the AACPP contractor and TSA headquarters.
- Password protection for files containing personal or sensitive security information to prevent unauthorized internal and external access.
- Network firewalls to prevent intrusion into DHS network and AACPP databases.
- User identification and password authentication to prevent access to sensitive security information by unauthorized users.

- **Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?**

All DHS and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of personal data. Additionally, training has been conducted that relates to the handling of personal data and sensitive security information.

FOR QUESTIONS OR COMMENTS, PLEASE CONTACT:

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 202-772-9848