Privacy Impact Assessment
for the

Rail Security Pilot Study Phase II at PATH

July 12, 2006

Contact Point
Joe Foster
Department of Homeland Security
Science & Technology
(202) 254-5314

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

Transit systems are attractive and visible targets for terrorism because they carry large numbers of people in concentrated, highly repetitious, and predictable patterns that are designed for easy access. In response to events in Madrid and London that demonstrated that commuter rail and mass transit are realistic terrorist targets, the Department of Homeland Security (DHS) Office of Science and Technology is implementing a Rail Security Pilot (RSP) under the auspices of congressional mandate found in Conference Report (H. Rep 108-774), "Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 20, 2005, and for Other Purposes (pg. 79).

The RSP objective is to develop a credible "response package" that could be quickly and efficiently implemented in response to an event or as the result of intelligence indicating a possible threat exists where explosives would be used in a commuter rail or mass transit venue. At a minimum, the resultant response package will consist of a set of validated concepts of operations (CONOPS), the endorsement of equipment, and a targeted and refined training package. To develop the response package, the RSP will evaluate the effectiveness of off-the-shelf and prototype explosives detection and mitigation capabilities to counter two distinct threats: 1) the suicide bomber and 2) the leave-behind bomb. An important feature of this pilot is the ability to rapidly deploy operational capabilities with minimal set-up costs, which is ideal for responding to intelligence-based monitoring or establishing high-visibility operations for deterrence.

The RSP is divided into two phases. Phase I, conducted in February 2006, did not require the collection of personally identifiable information and evaluated existing countermeasures using aviation security methods that could be implemented immediately. Phase I technologies included walk through metal detectors and dual-energy X-ray machines that were calibrated for the rail threat basis (i.e., large amounts of metal typical of that found in suicide bomber vests and large quantities of explosive capable of damaging key infrastructure).

Phase II is evaluating emerging technologies with varying technological maturity. Phase II activities will occur in several locations and this Privacy Impact Assessment only covers the activities to occur at the Port Authority Trans-Hudson New York New Jersey (PATH NY/NJ). Successful completion of the RSP will provide a combination of technologies, routine operating protocols, and appropriate training curriculum that minimizes the burden of responding to an explosive attack on the rail sector. Ideally, the RSP will offset the increased security burden on law enforcement personnel through increased police effectiveness in their traditional mission areas.

The specific technologies to be fielded with a potential privacy impact include: 1) motion video surveillance cameras, 2) still photography, 3) whole-body infrared images, 4) whole-body

millimeter-wave, and 4) whole body terahertz images. Additionally, personal articles may be inspected, either by law enforcement officers (LEO) or by trained test conductors. A summary of the Phase II screening equipment with potential privacy issues is provided in Table 1 below.

Table 1. Summary of Phase II Screening Equipment with Potential Privacy Issues

Port Authority/ Station	Technology	Operations
Port-Authority Trans Hudson (PATH)/ Exchange Place Station	• Passive[1] millimeter wave imaging • Active[2] millimeter wave imaging • Passive terahertz imaging • Infra red imaging • Standard still and surveillance camera images	• Imaging and detection technology identifies objects hidden beneath clothing • Still and motion video technology show facial images

Section 1.0 Information collected and maintained

1.1 What information is to be collected?

Collected information will be in the form of images of individual commuters traversing the detection area to assess the potential presence of concealed explosive threats. Technologies will include traditional motion video and still photography images, infrared (IR) thermography images, millimeter-wave (MMW) images, and terahertz (THz) images. Both whole body and facial images will be collected depending on the technology system/concept of operations (CONOPS).

- IR Thermography images (passive): Imaging using IR thermography relies upon the IR energy naturally emitted and reflected by the human body. IR energy emitted from the body is absorbed and then re-emitted by clothing. Concealed objects between the body and clothing are observed with IR imaging systems as a thermal contrast (temperature difference).

[1] Passive means the imaging technology uses only what is available to create the image (like non-flash photography)
[2] Active means the imaging technology illuminates the subject to create the image (like flash photography)

- Millimeter-wave images (active and passive): Passive MMW technology uses natural MMW illumination emitted and reflected from a person and the surrounding environment to produce an image. Active MMW illuminates a subject with MMW energy and produces images due to reflections from the body.
- Terahertz images (passive): Passive terahertz imaging is very similar to millimeter wave imaging with a slight shift in measured electromagnetic energy naturally emitted from the human body

Images will only contain date/time or sequence number labels – no other identifying information will be collected.

1.2 From whom is information collected?

All rail commuters who pass into the detection area will be subject to image analyses for concealed body-borne explosive threats as they progress from entrance turnstiles toward subway platforms.

1.3 Why is the information being collected?

The purpose of the RSP is to assess the merits of available, emerging technologies with security system CONOPS to mitigate the threat of a body-borne explosive device or leave-behind bomb. The imaging information provides an indication of a potential threat that requires secondary assessment by law enforcement officers. These technologies and security systems must be evaluated in an actual commuter rail environment to collect operationally relevant data.

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

Pursuant to the Congressional Conference Report (H. Rep 108-774), "Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 20, 2005, and for Other Purposes (pg. 79). Congressional appropriation language stipulated that funds be spent for:

- conducting simulated, real-world exercises to validate a training program for the use of commercially available equipment against suicide bombers in commuter and passenger rail environments;
- improving the ability of law enforcement to detect and disrupt potential suicide bombers at a distance while minimizing risk to law enforcement and the general population; and,
- operationally evaluating commercially available systems for rail track surveillance.

1.5 Privacy Impact Analysis:

This pilot project is designed to evaluate the merits of commercial technology to identify suicide bombers among rail passengers in real-world exercises. The technologies capture traditional visible photographic images and emerging "invisible to the eye" images of body-borne concealed threats. There is a risk to privacy with imagery that contains facial and whole body photographs, and/or whole body scans. The risk of this type of privacy interference has been reduced by specifically not collecting additional personally identifiable information (such as name, thus individuals remain anonymous to DHS and the pilot program) and by ensuring that only blurred pictures are shared outside of the RSP.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

Information is collected in the form of passenger images as follows:

- Traditional motion video images will be obtained in the test areas to evaluate queue lengths at passenger inspection checkpoints and determine the impact of screening on the passenger.
- The infrared (IR), terahertz (THz) and millimeter wave (MMW) images of commuters will be used to evaluate technology and concept of operations effectiveness derived from pooled data.

All of the images collected are part of a primary screening process to identify concealed explosives or shrapnel carried on the commuter's person. If the system identifies a possible concealed explosive threat, an alarm will occur. Alarm resolution is required on all primary detection alerts and may include law enforcement interrogation and/or physical search. Any illegal contraband that is not evidence of an explosive threat found during secondary inspection/alarm resolution will be managed by local law enforcement authorities. The screening process may uncover other security risks such as concealed weapons or illegal drugs, which will be managed per PATH NY/NJ protocols. DHS will not collect any additional personal information other than the pictures. Local law enforcement may collect additional information, as needed. If requested, DHS may provide PATH NY/NJ a copy of the image photo that prompted the primary screening process.

Image information collected for this pilot project will be held within the project to derive statistical measures of performance for each system. Select images will be shared externally in a training package to disseminate the utility of each technology/CONOPS; however, any facial image shared will be obscured to prevent identification of an individual. If the technology detects a true threat during the pilot, the threat will be handled appropriately through law enforcement.

Images may also be used for training purposes. In this instance the facial features will be blurred.

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)?

There are no plans to use this data to search for or to establish patterns involving individuals. The information will be used to estimate measures of effectiveness derived from pooled data, such as probability of detection, false alarm rate, nuisance, alarm rate, impact on the individual and delay time. Data will be deleted within 90 days (per PATH NY/NJ legal). For the purpose of reporting to Congress, a limited number of images will be maintained; however, all identifying features of individuals will be blurred.

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

The accuracy of the information is determined by the detection that takes place. The pilot is seeking to detect a bomb which often consists of explosives, shrapnel, batteries and wires. All positive alarms from the surveillance technologies will require resolution to determine the nature of the alarm. This is performed by escorting the passenger to a partitioned secondary screening facility for questioning and/or physical inspection (such as performing a pat-down inspection). Alarms will be resolved as nuisance (the item causing the alert was appropriately found, but was not a threat), false (no item was found), and true (the item found was a true threat).

2.4 Privacy Impact Analysis

Technology has been deployed to blur the images that have personal information such as a face or other identifying features when shared outside of the RSP or used for training purposes. Individuals using the system have been trained on the appropriate use of the system and the collection of the information so as to decrease the risk of misuse of the clear image photos.

Section 3.0 Retention

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

The data will be analyzed by the DHS RSP for a period not to exceed ninety (90) day, after which the data will be archived or destroyed. Ninety (90) days provides adequate time to complete the RSP and develop follow on actions.

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

Yes. General Records System 20 covers the disposition of Electronic files or records

created solely to test system performance, as well as hard-copy printouts and related documentation for the electronic files/records.

3.3 Privacy Impact Analysis

The information needs to be retained for 90 days to ensure adequate time is available to assess the utility of the technologies being evaluated and develop the needed training materials.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

DHS/S&T will share the results of the study with the Transportation Security Administration (TSA), but the individual images will not be released unless facial features are obscured/blurred as discussed in other sections.

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

DHS/S&T will share the results and the obscured/blurred pictures with TSA to assess merits of technology systems/concepts of operations as requirements for mass transit authorities or for adaptation into other transportation environments.

4.3 How is the information transmitted or disclosed?

The study results and associated obscured/blurred pictures will be transmitted in electronic or print editions. All reports generated by the project will be designated For Official Use Only and will be appropriately maintained.

4.4 Privacy Impact Analysis

Internal information sharing is needed within the S&T technical team to understand and define the technology/CONOPS merits/demerits; and, external to provide summary results. All images shared within DHS/TSA will remain anonymous as no individual is named or otherwise identified. Any images shared external to the RSP team must have blurred facial features to ensure that the identity of the individual is not recognized in any display of the image.

Section 5.0 External sharing and disclosure

5.1 With which external organizations is the information shared?

Study results will be available to transit authorities in the form of a training package that describes technology options and select concepts of operation. Commercial vendors supplying equipment for the pilot will be provided subsets of images to support improvements in the technology. Any images supplied to vendors will protect individual privacy by blurring out the images before sending on to the vendors. The information may also be made available to

Congress.

When an alarm and secondary screening confirms presence of concealed weapons or illegal drugs, PATH NY/NJ will implement law enforcement protocols and RSP may provide the clear photo upon request by the law enforcement authority.

5.2 What information is shared and for what purpose?

Technology system performance results will be shared to enable the transit authorities to evaluate operational costs and benefits of technologies employed in the test. No personally identifiable commuter information will be shared.

If, during the course of the pilot test, the LEO detains a commuter based on concealed contraband or explosives detection, then law enforcement will have access to images collected from the pilot activities for use in legal proceedings. Possession of contraband or explosives may also be confirmed by subsequent search by the LEO, based on the LEO's determination of probable cause.

5.3 How is the information transmitted or disclosed?

Printed or electronic summary reports of the study will be provided without any personally identifiable information.

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?

The training package for transit authorities is intended to provide a current value assessment of technology/CONOPS for consideration of security system upgrades. Information shared with external organizations will not include sufficient detail to identify specific individuals. No specific MOU, contract or agreement is employed.

5.5 How is the shared information secured by the recipient?

Shared information does not include personally identifiable information. Sensitive security information resulting from the RSP will be protected according to DHS information security requirements.

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

Not applicable.

5.7 Privacy Impact Analysis

For study results and associated photos, the information will be obscured or blurred so that no personal information is provided to those looking at the efficacy of the information. For

law enforcement authorities, the clear image photo may be provided if requested after a search has been conducted.

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?

Notice that screening is taking place and what type of technology will be used will be provided prior to entrance to the transit area at PATH. The signage that will be used for the PATH pilot is provided in Appendix A.

Individual commuters will be able to render consent prior to entering the relevant area because sufficient notice will be provided. Given the nature of the information gathered, the RSP will not be collecting information that is considered a record under the Privacy Act. *See* 5 U.S.C. § 552a(a)(4)(defining a record as "any item . . . of information about an individual . . . that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.") Accordingly, we will not file a system of records notice in the Federal Register as indicated in 5 U.S.C § 552a(e)(4) .

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

The notice, as described in 6.0, will provide written notice to individuals of their options including the opportunity to enter the station where the test will take place or choose to enter via another station thereby opting out of the pilot study with no record of declination or penalty.

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. Once the passenger chooses to enter the inspection area by passing through the turnstiles, the person has consented to have images obtained by the RSP.

6.4 Privacy Impact Analysis

Individuals will be provided adequate notice, as described in 6.0, that security screening will occur upon entry through the turnstiles. An individual may choose not to consent by leaving the station and entering the rail system through a separate station. Sufficient notice of the location and type of screening has mitigated the risk of the individual being unaware of the collection of information.

Section 7.0 Individual Access, Redress and Correction

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

None. No additional personally identifiable information is collected to associate an individual in an image, nor will the public have access to the image database. Nonetheless, if a person is arrested on the basis of the images, they may request copies of these images from PATH NY/NJ's Legal Department.

7.2 What are the procedures for correcting erroneous information?

If an alarm resolution is required, a physical search is conducted by trained personnel and if nothing is found then the individual is allowed to pass and no personal information is collected. If the wrong individual was brought over for secondary screening, this will be rectified by comparing the clear photo to the individual being screened.

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

There is no information to be corrected.

7.4 If no redress is provided, are alternatives are available?

Redress is provided at the time of the secondary screening.

7.5 Privacy Impact Analysis

Individuals will not have access to collected images because the information is not cataloged by retrievable personal information.

Section 8.0 Technical Access and Security

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

Rail Security Pilot S&T technical team consisting of members from Oak Ridge National Laboratory (ORNL), Lawrence Livermore National Laboratory (LLNL), Pacific Northwest Laboratory (PNL), Sandia National Laboratories (SNL) and DHS/S&T will have access to clear and blurred images collected while in the field, and later during data analysis/summary report preparation.

No other groups will have access to the clear images.

8.2 Will contractors to DHS have access to the system?

Yes. U.S. Government National Laboratories are considered DHS intramural laboratories, but may be considered external to the DHS. See 8.1. Commercial vendors supplying technology for the pilot will support the field operations, providing technical advice on optimum operation of the technologies.

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

No. There is a limited number of individuals who have access to the system, which will include only the S&T technical team.

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

S&T technical team members are the only individuals with access to the system. This is documented according to previously drafted Statements of Work.

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

The Project Manager will for the S&T technical team. The Project Manager will perform random inspection/auditing to ensure all collected images are managed per the privacy requirements of the project.

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

Given the small number of individuals with access to this pilot program, auditing has not been put in place. If this program is deployed on a larger basis appropriate auditing measures will be included.

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

Appropriate privacy training has been provided to the limited number of indivudals on the S&T technical team with actual access to the system.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed? This section is not applicable because data collected by the RSP is a stand alone system and will not be integrated into existing DHS systems.

8.9 <u>Privacy Impact Analysis</u>

The bulk of image data collected will be translated into statistical performance characteristics of the technology by the DHS technical team. Team members have been trained on the appropriate use of the clear image.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

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

All systems were selected, obtained and installed by the RSP project team.

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

The RSP CONOPS for the selected technologies were developed to meet the goals for detection/interruption of suicide bomb threats on individuals without specifically identifying an individual. Decisions to include specific technology/CONOPS into the RSP were based on merits to improve rail security balanced by impacts to transit authority operations.

9.3 What design choices were made to enhance privacy?

Design choices depended on the technology system. Full body imaging technologies were selected and configured so as to not show a revealing image of the screened individual. Video surveillance cameras were selected to be of lower resolution and wider angle viewing than required for individual identification. Furthermore, mount locations were chosen to provide views from above (also limiting individual identification) to assist in the identification of conduct of operations problems, the formation of queues, and time-motion information. The secondary screening location was located out of the main flow of passengers and is a relatively isolated location. Privacy partitions are planned to form discreet, individual secondary screening areas where the cause of the alarm can be identified through questioning, hand held metal detectors, and/or pat-down techniques.

Conclusion

Developing system performance factors to recommend credible suicide bomber rail protection systems and methodologies does not depend on identifying, classifying, or tracking the test participants. The RSP actually benefits from test participant anonymity both in minimizing obtrusiveness on the commuters, who are impacted by deployed systems, and in avoiding the potential for individual profiling. We have selected technologies and CONOPS that meet the goal of detecting threats on individuals without links to collect the identity of these individuals. Images collected will be used to determine threat detection technology performance

and impacts to transit authority operations. This information can not be mined to provide information about specific individuals and will be either archived at DHS or destroyed at the end of the pilot program.

Responsible Officials

Joe Foster

Department of Homeland Security

Approval Signature Page

_____ July 12, 2006

Maureen Cooney
Acting Chief Privacy Officer
Chief Freedom of Information Act Officer
Department of Homeland Security

Appendix A

Figure B.1. Security Inspection Notice For Rail Security Pilot At PATH