



Privacy Impact Assessment
for

Exit Lane Breach Control (ELBC) System

December 28, 2010

Contact Point

Robin Kane

**Operational Process and Technology
Transportation Security Administration**

Robin.Kane@dhs.gov

**Mary Ellen Callahan
Chief Privacy Officer**

Department of Homeland Security

Privacy@dhs.gov



Abstract

The Transportation Security Administration (TSA) is conducting an assessment of Exit Lane Breach Control (ELBC) systems for use in airports. The assessment will evaluate the ELBC systems' capability to monitor traffic flow at the exit lanes from the sterile areas of the airport and initiate an automated response if it appears that an individual is entering the sterile area through the exit lane. TSA will make results of the assessment available to airports seeking to implement such systems. This Privacy Impact Assessment (PIA) is being conducted to provide transparency into TSA testing affecting the public and the collection of images as part of the assessment. If TSA decides to implement such systems for its own use, a new PIA will be conducted.

Introduction

In response to Congressional requirements included in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, TSA is conducting an assessment of Exit Lane Breach Control (ELBC) systems.¹

Today, airports use closed-circuit television (CCTV) systems at many locations for a variety of loss prevention, law enforcement, and security purposes. TSA is testing the ELBC system, which consists of software that analyzes the movement of traffic through cameras placed to monitor the exit lane, and hardware consisting of sensors to monitor the exit lane, alarms (siren and/or flashing lights), and possibly barriers, such as doors. The ELBC system integrates video, sensor, alarm, and barrier technologies that support the automated or manual detection and response to unauthorized persons and objects entering the sterile area of an airport terminal from the non-sterile area via an exit lane. The ELBC system monitors the exit lane and the non-sterile area, and sterile area immediately abutting the exit lane. Using video analytics and sensor inputs, the ELBC identifies traffic anomalies at the exit lanes indicative of a breach or potential breach of the sterile area. As appropriate, the ELBC system will automatically activate audio and/or visual alarms and, possibly deploy physical barriers when warranted to limit the individual's or object's access to the sterile area. TSA will assess the technology using cameras installed by TSA for the test. Images captured by the test cameras will either be transmitted on a stand-alone network created for the test that is monitored by a TSA officer, or will be integrated into the existing airport CCTV network, as available. TSA is assessing the ELBC system to determine the effectiveness of such a system.

The video analytics of the ELBC software identify anomalous movement (such as movement leading into the exit lane) or loitering. Accordingly, the CCTV images will not be associated with any individuals unless they are required to be used as part of an enforcement proceeding against an individual who has attempted to enter the sterile area through an exit point. CCTV images will be shared with the airport authorities where existing camera networks will be used in the assessment, as well as with law enforcement if there is an incident or as otherwise authorized.

¹ Section 1613. Pilot Project to Test Different Technologies at Airport Exit Lanes. (a) In General.—The Administrator of the Transportation Security Administration shall conduct a pilot program at not more than 2 airports to identify technologies to improve security at airport exit lanes.



Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974 and shall assure that technology sustains and does not erode privacy.

In response to this obligation, the DHS Privacy Office has developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act, which encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure. Given the particular technologies and the scope and nature of their use, TSA used the DHS Privacy Office FIPPs PIA template.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Existing signage clearly identifies the sterile and non-sterile portions of the airport and the existence of monitoring at those egress points. The use of CCTV and any notification to individuals is the responsibility of local airport authority policies. TSA is providing general notice of this assessment through this PIA.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Generally, individuals do not have an opportunity to provide consent to the collection of images by the ELBC system. Currently, exit lanes are manned by TSA or airport personnel, and there are signs indicating that entry is prohibited. Individuals who proceed to enter the exit lane are currently subject to observation and appropriate response by TSA or airport personnel. CCTV systems capture the actual event and are not subject to correction or redress. It may be possible to access the CCTV images through an appropriate request under the Freedom of Information Act or appropriate state equivalent to the airport authority.



3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII, to include images, and specifically articulate the purpose or purposes for which the PII is intended to be used.

TSA is responsible for security in all modes of transportation, including commercial aviation.² Congress directed TSA to conduct “research, development, testing and evaluation of threats carried on persons boarding aircraft or entering secure areas, including detection of weapons, explosives, and components of weapons of mass destruction.”³ Specifically, the Implementing Recommendations of the 9/11 Commission Act of 2007 require TSA to conduct a pilot program to identify ELBC technologies that minimize the risk of unauthorized access, reduce resource requirements at the exit lane, and maintain or exceed the existing level of security. In the event that an individual attempts to breach the exit lane, the CCTV images may be used by TSA to determine an appropriate operational response or civil penalty. If law enforcement is involved, video images may be used by law enforcement to determine an appropriate enforcement response.

Pursuant to these authorities, as well as its general authorities to conduct research and development to enhance transportation security, TSA is testing and evaluating the performance capabilities and technical viability of ELBC technologies. TSA will share assessment results with airport authorities that may be seeking to utilize such technology.

4. Principle of Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

CCTV images collected as part of the assessment will appear to the Transportation Security Officer or airport authority personnel responsible for maintaining the security of the exit lane either in real-time or following an alert. In accordance with TSA’s records disposition schedule, N1-560-04-3, CCTV images that do not document an incident will be destroyed after 14 days, CCTV images that document an incident not needed as evidence will be destroyed 14 days after date of recording or date of determination, whichever is later, and CCTV images that document an incident needed as evidence will be permanently retained.

In some instances, TSA may share the image with law enforcement and transportation facility operators if it is necessary to locate an individual who has moved out of the area before there has been an opportunity to resolve the incident.

² 49 USC §114.

³ 49 USC §137.



If an incident report is generated, the image may be appended to the incident report and retained. These records are covered by TSA's Privacy Act system of records, DHS/TSA 001 Transportation Security Enforcement Records System (TSERS) (May 19, 2010, 75 FR 28042). In addition, the image may be provided to local law enforcement for their law enforcement report. After the image is appended to the incident report, it will be deleted from the ELBC.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The images captured by the ELBC are the same images that are viewed by the naked eye and do not contain any associated personally identifiable information. The assessment team may review captured CCTV images to determine if the ELBC system is functioning as expected. When there is no indication of an anomaly, the video of the monitored area is deleted after 14 days. When there is an indication of an anomaly and an incident report is generated, the image may be appended to the incident report and retained. These records are covered by TSA's Privacy Act system of records, DHS/TSA 001 Transportation Security Enforcement Records System (TSERS). In addition, the image may be provided to local law enforcement for their law enforcement report.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII, including images, is accurate, relevant, timely, and complete, within the context of each use of the PII.

The images collected by the ELBC system are similar to CCTV or other camera images. Accordingly, these images are accurate, timely, and complete, and are directly relevant to detecting the presence of an anomaly in exit lane traffic.

The minimal privacy risk associated with this technology is the retention of the image of an individual that is the same as what that individual presents to the general public and which does not contain any other PII. The privacy risk is minimal because TSA only retains ELBC images under a limited set of circumstances as discussed in Sections 4 and 5.

ELBC does not collect additional personally identifiable information (such as name); thus individuals remain anonymous to TSA unless the interaction leads to an incident report.

7. Principle of Security

Principle: DHS should protect PII, including images, through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.



TSA will secure ELBC images against unauthorized use through a layered security approach involving procedural and information security safeguards. Only TSA employees with proper security credentials and passwords, and a need to know to fulfill their duties, will have access to the ELBC and ELBC images. Access to ELBC images is limited to authorized individuals with a need to know.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, including images, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TSA personnel operating ELBC systems are given training in systems operation protocols and processes for protecting the privacy of individuals undergoing ELBC monitoring. Further, TSA personnel take DHS Privacy training.

9. Additional Issues

None.

Responsible Officials

Robin Kane
Assistant Administrator
Operational Process and Technology

Approval Signature Page

(Original signed copy on file with the DHS Privacy Office)

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security