Code of Practice for the Acceptable Use of Security Scanners in an Aviation Security Environment

November 2011

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text will be made available in full on the Department's website in accordance with the W3C's Web Content Accessibility Guidelines. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
76 Marsham Street
London SW1P 4DR
Telephone 020 7944 8300
Website www.dft.gov.uk

To order further copies contact:
DfT Publications
Tel: 0300 123 1102
www.dft.gov.uk/orderingpublications

Printed in Great Britain on paper containing at least 75% recycled fibre

This Code of Practice sets out requirements for the use of security scanners at UK airports. Where security scanners are deployed, airport operators must ensure that the following measures are adopted.

Legal Authority

Airports will operate security scanners as set out in Directions made on behalf of the Secretary of State for Transport under the Aviation Security Act 1982. These Directions are available on the Department for Transport web site.

Privacy

An effective privacy policy must be put in place by the airport operator to protect passengers when being screened by security scanners. As approved automatic threat recognition (ATR) software becomes available, it should be fitted to all new purchases of equipment. Where ATR software is not being used the privacy policy must include a requirement that the equipment is sited in such a way to ensure that the security screener(s) conducting analysis of the image (the screener) must not be able to see the person whose image they are viewing and the security screener(s) resolving any issues identified by the security scanner should not be able to see the image of the person being searched. The policy must also include procedures to ensure that image-capturing equipment (such as cameras and mobile phones) is not taken into the viewing room and that images are not left on unattended screens.

A person selected for scanning may request that the screen reader is of the same sex and the airport must meet this request as quickly as possible. If further resolution is required (i.e. a targeted hand search), an appropriate method of communication must be employed between the screen reader and the security searcher that does not include the use of the image to ensure that this privacy is protected.

Data Protection

In order to classify a passenger's security status when using a security scanner, it is necessary to capture data for analysis. Airport operators shall ensure that checks are undertaken at least twice yearly to ensure that data cannot be saved, copied or sent. Any facilities on the scanner which could be used to retain, copy or transmit data must be disabled. The scanning process shall comply with the general law on data protection.

Analysis can be conducted by a security screener and/or by approved automatic threat recognition software.

Immediately after the scanning analysis is completed and the passenger moves away from the security scanner, all data relating to the passenger must be destroyed and irretrievable. Whilst an image is being analysed, it must only be possible for the screener to view that image. In exceptional circumstances where a screener believes there is a viable threat to the safety of passengers or staff, an additional appropriate security screener may be required to view the image. There must be no method of copying or transferring images.

Communications will be available at the security screening area to inform passengers that “For the benefit of all passengers' security, passengers may be required to be screened using security scanning equipment. Screening will be conducted by security screeners acting on behalf of the airport operator. Images of passengers will not be saved.” Airport operators must provide to persons selected for screening the opportunity to provide details of their age, gender, race, ethnic origin and religion or beliefs.

Health and Safety

The Department for Transport (“DfT”) has the results of an independent assessment of the risks to health from the effects of security scanners that utilise ionising radiation technology. This assessment provides evidence that the use of such security scanners represents a negligible risk to health from exposure to ionising radiation. The assessment compares the risk from security scanners to other everyday risks and is available via the DfT website (http://www.dft.gov.uk/pgr/security/aviation/airport/). Assessments completed by authorities outside of the UK have concluded that the risks to health from security scanners using very low dose ionising radiation is so low as to be negligible.

The airport authority deploying a security scanner must ensure that all appropriate local risk assessments have been conducted for the type of security scanner being deployed and that the equipment conforms to all relevant health and safety requirements. Before deployment of security scanners that produce ionising radiation, a measure of the ambient radiation dosage and the effective dose that a passenger receives when being scanned, must be conducted by qualified persons. Local rules must be agreed and applied to mitigate the risks that a security scanner is used outside of normal operating conditions (whether through incorrect use or malfunction).

Equipment Approval

Airport operators must discuss all prospective use of security scanners with the DfT before deployment to ensure that security standards are maintained.

Training

Security screeners must obtain appropriate security clearances before receiving training and receive training in accordance with an approved package. Training packages should be developed in partnership with manufacturers and must be approved by the DfT. Before being deployed to operate a security scanner, a security screener must have completed the appropriate training including how to deal with issues sensitively and to protect privacy. Records of training undertaken must be maintained and made available upon request by the DfT.

Communications

An effective communication strategy should be developed to inform people of the security requirements where security scanners are deployed. It should be made clear at the earliest possible stage that all passengers selected for screening by a security scanner must be scanned. If a passenger declines to be scanned that passenger must be refused access to the restricted area of the airport (the Critical Part), with the result that the passenger will not be able to fly on that occasion. Information should be adequate, clear and provided ideally before ticket purchase. In any event it must be provided prior to entering the passenger screening area. Information should also be readily available in a number of languages appropriate for the profile of passengers using the airport.

Selection Criteria

Passengers must not be selected on the basis of personal characteristics (i.e. on a basis that may constitute discrimination such as disability, sex, gender reassignment, age, race, religion or belief, pregnancy and maternity and sexual orientation). Airports must also follow all the requirements relating to selection that are contained in the public and restricted parts of the security scanner Direction.

The passenger shall be informed that they have been selected for scanning in order to resolve security concerns or have been selected at random, except where selection is done by automated means.

Protocols

Security scanners must be operated in accordance with detailed protocols which contain the further information on the operation of the security scanner including selection criteria for those to be scanned. The security sensitive information is not published, but will comply with the requirements contained in this Code of Practice.

Review

DfT will continue to review this Code of Practice in light of operational experience and relevant changes in law.