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

October 2016

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

Airport Operators are required to operate security scanners pursuant to directions made by the Secretary of State for Transport under the Aviation Security Act 1982. These directions are available on the gov.uk website.

Privacy

An effective privacy policy must be put in place by the airport operator to protect individuals when being screened by security scanners. This must include the installation and use of Automatic Threat Recognition (ATR) software. ATR software interprets the scan data, instead of creating an image, and identifies areas where items may be concealed on the body. These areas are flagged on a standardised stick-figure on a screen, to indicate to the security officer areas of the individual's body which should receive a targeted hand-search (see separate guidance). Security staff must not be able to view images produced by the scanner which have not been interpreted by ATR.

Data Protection

Analysis shall be conducted by approved ATR algorithms. Immediately after the scanning analysis is completed and the individual moves away from the security scanner, all data relating to the individual must be destroyed, irretrievable and incapable of being copied or sent.

A communication to passengers must be available at the security screening area to inform them that "For the benefit of all passengers' security, passengers may be required to be screened using security scanner equipment. Assessment of the scan data will be conducted by a computer algorithm. No images of individuals are created, and no scan data will be saved."

Health and Safety

All security scanners must use millimetre wave technology, as it poses no known health and safety risks. Millimetre wave scanners utilise a very low power, non-ionising form of electromagnetic technology. Non-ionising radiation refers to electromagnetic waves which do not alter atoms in molecules by removing electrons. The amount of electromagnetic radiation emitted by millimetre wave security scanners is many times lower than that emitted by a mobile phone.

Alternatives

An individual may opt out of being scanned. In this instance, the individual must either be screened by an alternative method which includes at least an enhanced hand search in private or that individual must not be permitted to enter the security restricted area, or, if applicable, he or she must be removed from it. An enhanced hand search in private must take place in a private room or an area away from the main search comb. This may involve the loosening and/or removal of clothing.

Equipment Approval

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

Training

Security officers must obtain appropriate security clearances before receiving training in accordance with an appropriate package that takes account of all relevant guidance. Training packages should be developed in partnership with manufacturers and shared on request with the DfT or anyone authorised to act on behalf of the Secretary of State. Before being deployed to operate a security scanner, the security officer 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 or anyone authorised to act on behalf of the Secretary of State.

Communications

An effective communication strategy must be developed to inform people of the security requirements where security scanners are deployed. It must be made clear at the earliest possible stage that all individuals selected for screening by a security scanner will be expected to be scanned. Individuals who refuse to be scanned must be offered an alternative screening method, involving at least an enhanced hand search in private. Information should be adequate, clear and provided ideally before any 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

Individuals 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). Airport Operators must also follow all the requirements relating to selection that are contained in the public and Official-Sensitive parts of the Security Scanner Direction.

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 must comply with the requirements contained in this Code of Practice.

Review

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