Privacy Impact Assessment Update
for

TSA Advanced Imaging Technology

DHS/TSA/PIA-032(d)

December 18, 2015

Contact Point
Jill Vaughan
Assistant Administrator
Office of Security Capabilities
OSCCommunications@dhs.gov

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

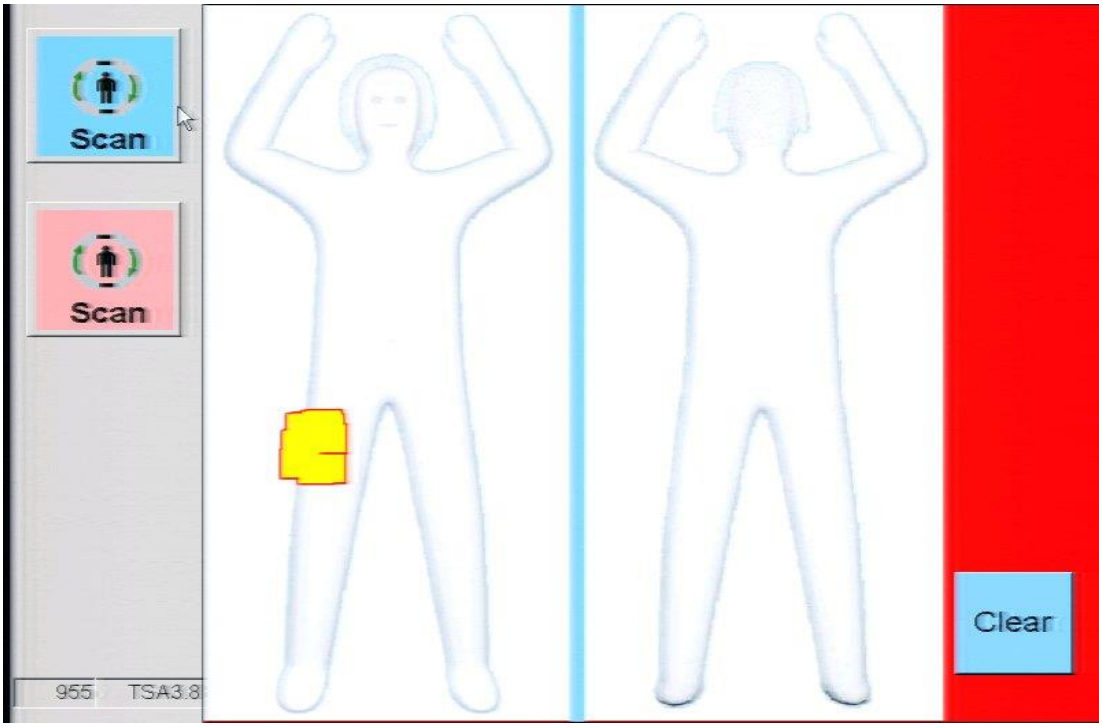
The Transportation Security Administration (TSA) has deployed Advanced Imaging Technologies (AIT) for operational use to detect threat objects carried on persons entering airport sterile areas. AIT identifies potential threat objects on the body using Automatic Target Recognition (ATR) software to display the location of the object on a generic figure as opposed to displaying the image of the individual. TSA is updating the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt opt-out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may direct mandatory AIT screening for some passengers. TSA does not store any personally identifiable information from AIT screening.

Introduction

Under the Aviation and Transportation Security Act (ATSA),[1] TSA is responsible for security in all modes of transportation, and must assess threats to transportation, enforce security-related regulations and requirements, and ensure the adequacy of security measures at airports and other transportation facilities. TSA has deployed AIT for operational use to detect threat objects carried on persons entering airport sterile areas.[2] AIT identifies potential threat objects on the body using ATR software to display the location of the object on a generic figure as opposed to displaying the image of the individual. TSA currently uses AIT equipped with ATR to quickly, and without physical contact, screen passengers for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing. ATR software identifies objects on the body and highlights the location of the object with bounding boxes on a generic figure.[3] ATR eliminates the need for a remote image since it is a generic image that can be presented on a monitor connected to the AIT and co-located with the officer assisting the screened individual. The individual will undergo physical screening if ATR alarms for the presence of an object.

[1] Pub. L. 107-71
[2] "Sterile area" is defined in 49 CFR 1540.5 and generally means an area of an airport with access limited to persons who have undergone security screening by TSA.
[3] For additional information, *see* DHS/TSA/PIA-032 TSA Advanced Imaging Technology and associated updates, *available at* www.dhs.gov/privacy.

A sample image from a system using ATR appears below:



Storage of images

The AIT devices at airports do not have the ability to store images..[4] The ATR generic image is maintained on the monitor only for as long as it takes to resolve any alarms. The AIT equipment does not generate or retain an underlying image of the individual.

What to expect

Because the ATR software replaces the individual's image with that of a generic figure, the monitor will be co-located with the individual being screened. The screening officer will view both the individual and the ATR image. If there is an alarm, the physical screening will target the location indicated by the ATR software. If there are multiple alarms, the individual may receive a full screening.

[4] Initial versions of AIT were manufactured with storage functions that TSA required manufacturers to disable prior to installation at the airport. Current versions of the software installed at airports do not include any storage function to disable, and eliminate the need to perform the disabling of the storage function.

Reason for this Update

TSA is updating the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may direct mandatory AIT screening for some passengers as warranted by security considerations in order to safeguard transportation security.

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. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices 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 underling concepts of the Privacy Act that 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.

TSA has published information on AIT technologies on its website (www.TSA.gov), and published an original PIA on AIT in January 2008 with subsequent updates reflecting operational or technology changes.[5] In 2013, TSA published a Notice of Proposed Rule Making on the use of AIT in screening operations which received more than 5500 comments from the public. TSA expects to publish its Final Rule in 2016. This PIA update reflects TSA's continued transparency on its use of AIT.

[5] For all TSA Privacy Impact Assessments, please visit http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

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.

Individuals undergoing screening using AIT generally will have the option to decline an AIT screening in favor of physical screening. Given the implementation of ATR and the mitigation of privacy issues associated with the individual image generated by previous versions of AIT not using ATR, and the need to respond to potential security threats, TSA will nonetheless mandate AIT screening for some passengers as warranted by security considerations in order to safeguard transportation security.

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.[6] 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.[7] AIT technologies are being used to identify prohibited items, particularly non-metallic threat objects and liquids secreted on the body. ATR software identifies the location of the potential prohibited item on a generic figure. Because of the greater privacy protections provided by a generic figure, the image monitor for ATR is co-located with the AIT so that the screening officer can view it.

4. Principle of Data 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).

TSA does not collect PII with this technology. AIT with ATR does not generate an individual image but rather overlays the location of objects on a generic image.

[6] 49 U.S.C. § 114(d).
[7] 49 U.S.C. § 44912 note.

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.

TSA uses AIT solely for purposes of identifying objects that may be threat items. Once an alarm is resolved, the generic image is cleared from the screen, and therefore cannot be used for any other purpose or shared with anyone. Because there are no images to share, they cannot be used in any other context inside DHS or outside of the Department.

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 ATR generated image is accurate, timely, and complete and is directly relevant to the identification of threat objects. Potential threat items are resolved through a directed physical screening before the individual is cleared to enter the sterile area.

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.

AIT data is transmitted in a proprietary format to the viewing monitor, and cannot be lost, modified, or disclosed. TSA's decision not to retain images mitigates further data storage security issues.

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.

No PII is generated by AIT using ATR.

Conclusion

AIT technology improves threat detection capabilities for both metallic and non-metallic threat objects, while improving the passenger experience for those passengers for whom a physical screening is uncomfortable. ATR software provides even greater privacy protections by eliminating the human image that appeared with previous AIT technologies.

Responsible Officials

Jill Vaughan
Assistant Administrator
Office of Security Capabilities

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security