Privacy Impact Assessment
for the

Secret Service Use of Advanced Imaging Technology

DHS/USSS/PIA-008

December 23, 2011

Contact Point
Cornelius Tate
Deputy Assistant Director
Office of Technical development and Mission Support
c.tate@usss.dhs.gov

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov
(703) 235-0780

Abstract

The United States Secret Service is deploying Advanced Imaging Technology (AIT), at Secret Service protective sites. This technology creates an image of the full body that highlights anomalies that are on the body. It is used as a secondary means of personnel screening at protected sites, and used after the primary screening measures indicate that an individual requires an additional level of screening.

To address privacy concerns associated with creating an image of an individual's body, the Secret Service employee who examines the image is at a remote location and cannot see the person who is being screened, only the image produced by the AIT. The Secret Service employee that is in the room with the person being imaged can communicate with the Secret Service employee who examines the image, but cannot view the image.

The image of the individual is not linked in any way to the individual nor do they provide sufficient detail to be used for personal identification. The AIT does not have the capability to store, transmit, or print these images. In addition, an electronic privacy filter is applied to the remotely viewed image which renders the facial features unrecognizable.

Introduction

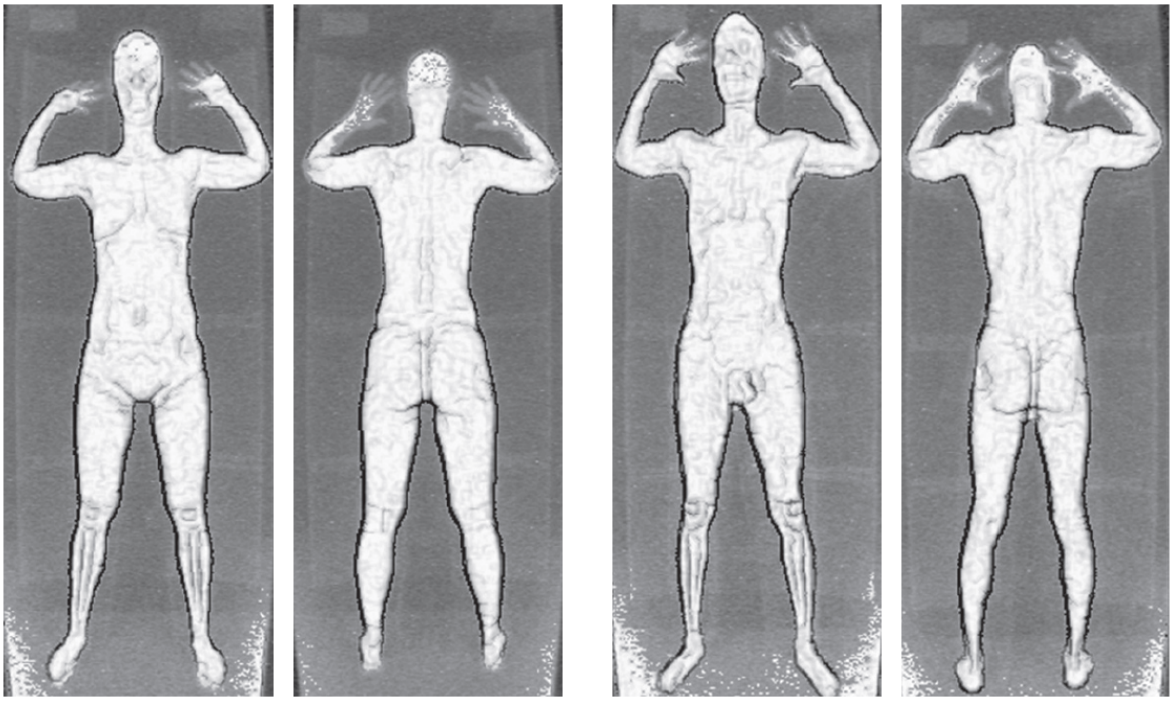
One of the major responsibilities of the Secret Service, as defined in 18 U.S.C. § 3056, is protection of the President, Vice President, their families, visiting heads of state, and other designated individuals. The Secret Service employs AIT devices, which use backscatter x-ray, as a secondary means of personnel screening if primary screening measures indicate that an individual requires an additional level of screening.

The technology relies on x-ray beams scanned over the body's surface at high speed. The beams are reflected back from the body and other objects placed or carried on the body, where it is converted into a computer image of the subject and displayed on a monitor. The Secret Service employee who examines the image is located at a remote location and cannot see the person who is being screened, only the image produced by the AIT.

The system delivers an extremely low dose of ionizing radiation to the individual and is well within American National Standards Institute (ANSI) standards.[1] For comparison purposes, the x-ray dose received from the backscatter system in use is less than the radiation received in five minutes of airplane flight at altitude. A person would have to be screened more than a thousand times in one year in order to exceed the annual radiation dose limit for people screening that has been set by expert radiation safety organizations.[2]

The images created by the AIT are not equivalent to photography and do not present sufficient details that would allow the image to be used for personal identification. In addition, an electronic privacy filter is applied to the remotely viewed image which renders the facial features unrecognizable. Examples of the current level of image detail created by the AIT device appear on the next page.

[1] ANSI N43.17-2009 Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation
[2] See FDA notation at: http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm#2



Front and Back of Female **Front and Back of Male**

BACKSCATTER IMAGES

Storage of images

The AIT used at Secret Service protected sites do not have the capability to store, transmit, or print images. Images are maintained on the monitor only for as long as it takes to resolve any anomalies. If the image operator sees a suspicious area or prohibited item, the image remains on the monitor until the anomaly is cleared by a physical search of the individual.

What to expect

Separate technologies and processes are used as the primary means of screening individuals entering protected sites. The AIT is used as a secondary means of personnel screening after the primary screening measures indicate that an individual requires an additional level of screening. Because the Secret Service is using AIT as part of a secondary screening process, the direct image of the individual is required. If secondary screening is required, the individual is advised that an AIT will be used. Persons undergoing secondary screening may decline an AIT screening in favor of a physical search. The Secret Service employee who examines the image is located at a remote location and cannot see the person who is being screened, only the image produced by the AIT. A privacy filter is applied to the remotely viewed image which renders the facial features unrecognizable. The Secret Service employee that is in the room with the person being imaged communicates with the Secret Service employee who examines the image, but cannot view the image.

Rules governing the use of the AIT are documented in standard operating procedures (SOP), and Secret Service employees who are part of the screening process where this equipment is used and who operate this equipment have been trained according to these SOPs. Due to the sensitivity of the technical and operational details, the SOP is not publicized.

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 PII. 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.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to 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.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of 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.

The Secret Service does not collect PII with this technology, and PII is not collected from individuals who are identified for secondary screening using this technology. The image of the individual is not linked in any way to PII. The AIT does not have the capability to store, transmit, or print these images. The individual who examines the image is located at a remote location and cannot see the person who is being screened, only the image produced by the AIT. A privacy filter is applied to the remotely viewed image which renders the facial features of the individual being screened unrecognizable. The Secret Service employee that is in the room with the person being imaged communicates with the Secret Service employee who examines the image, but cannot view the image.

Extensive information on the use of this technology is available on the manufacturer's web site(http://www.rapiscansystems.com/en/products/ps/rapiscan_secure_1000_health_and_safety_information) and from the Food and Drug Administration (http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm).

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.

Individual participation and consent is exercised by the person agreeing to allow the use of the AIT. Persons undergoing secondary screening may decline an AIT screening in favor of a physical search. Further notice is provided through the publication of this PIA that explains the technology and shows sample usage.

3. Principle of Purpose Specification

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

One of the major responsibilities of the Secret Service, as defined in 18 U.S.C. § 3056, is protection of the President, Vice President, their families, visiting heads of state, and other designated individuals. The Secret Service employs AIT devices, which use backscatter x-ray, as a secondary means of screening individuals after the primary screening measures indicate that an individual requires an additional level of screening. This technology is a needed measure for resolution after the primary screening measures indicate that an individual requires further screening.

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).

The Secret Service does not collect PII with this technology, and PII is not collected from individuals who are identified for secondary screening using this technology. The image of the individual is not linked in any way to PII. The AIT does not have the capability to store, transmit, or print these images. The individual who examines the image is located at a remote location and cannot see the person who is being screened, only the image produced by the AIT. A privacy filter is applied to the remotely viewed image which renders the facial features of the individual being screened unrecognizable. The Secret Service employee that is in the room with the person being imaged communicates with the Secret Service employee who examines the image, but can not view the image.

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 Secret Service uses this technology only for resolution after the primary screening measures indicate that an individual requires an additional level of screening; it is not used to screen everyone entering a protected site. Because there are no images to share, they cannot be used in any other context inside or outside of the Secret Service.

6. Principle of Data Quality and Integrity

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

The AIT images are generated by direct contemporaneous observation. Accordingly, it 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 a protected site. The images are not retained, thereby further mitigating any data quality or integrity issues.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Images are transmitted via a dedicated landline from the location where the images are taken to where they are examined, which is located on a protected, secure site and within a facility that is controlled by the Secret Service. There is no opportunity for this data to be lost, modified, or disclosed. The Secret Service's decision not to retain images further mitigates 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, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Rules governing the use of the AIT are documented in standard operating procedures (SOP), and Secret Service employees who are part of the screening process where this equipment is used and who will operate this equipment, have been trained according to these SOPs. On site supervisors will ensure that policies and procedures are adhered to and fully enforced.

Conclusion

AITs are needed at protected sites as a secondary means of personnel screening after the primary screening measures indicate that an individual requires an additional level of screening. This technology will improve the Secret Service's ability to detect prohibited items and concealed threats carried by individuals attempting to enter a protected site. The operational protocols of remote viewing of images, the AIT being configured with a privacy filter and not being able to store images, and the SOP and protocols in place provide strong controls to protect individuals' privacy while allowing the Secret Serive to effectively utilize this technology.

Responsible Official

Cornelius Tate
Deputy Assistant Director
Office of Technical Development and Mission Support
United States Secret Service
Department of Homeland Security

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security