

JOINT WRITTEN TESTIMONY

of

JOHN SANDERS

ASSISTANT ADMINISTRATOR

OFFICE OF SECURITY CAPABILITIES

TRANSPORTATION SECURITY ADMINISTRATION

and

JONATHAN R. CANTOR

ACTING CHIEF PRIVACY OFFICER

U.S. DEPARTMENT OF HOMELAND SECURITY

before the

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON TRANSPORTATION SECURITY

NOVEMBER 15, 2012

Good morning Chairman Rogers, Ranking Member Jackson Lee, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today about Advanced Imaging Technology (AIT).

As we have often stated, the Transportation Security Administration (TSA) screens approximately 1.8 million people who travel each day through 450 U.S. airports. We employ risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. The TSA workforce is vigilant in ensuring the security of passengers that travel through our Nation's vast transportation networks. We continue to evolve our security approach by examining the procedures and technologies we use, how we carry out specific security procedures, and how we conduct screening.

Using the Best Technology at our Nation's Airports

History shows that the threat to our transportation networks continues to evolve, as demonstrated by devices used by the underwear bomber on Christmas Day 2009 and the improved underwear bomb device discovered in the disrupted plot this past May. TSA works in partnership with private industry to develop and deploy innovative and effective screening technologies across the Nation's transportation system. For example, TSA and private industry's collaboration to deploy AIT units has resulted in Transportation Security Officers having the best technology available to detect both metallic and non-metallic threats.

TSA deploys two types of AIT: millimeter wave and general-use backscatter x-ray. Currently, there are AIT units in use at 200 U.S. airports. TSA has installed automated target recognition (ATR) software on all currently deployed millimeter wave imaging technology units and has

tested similar software for use on its general-use backscatter units. ATR software upgrades enhance passenger privacy by eliminating passenger-specific images. ATR also improves throughput capabilities by increasing the efficiency of the checkpoint screening technology. Machines upgraded with ATR software generate a generic outline that is displayed on a screen located on the AIT machine and viewable by the public. The software auto-detects anomalies concealed on the body that are then resolved through additional screening.

ATR-enabled units deployed at airports are not capable of storing or printing the generic image produced during screening and don't produce a unique image for each individual. It is important to note that a passenger may always decline to be scanned by AIT and will receive a pat-down as an alternative.

While significant progress has been made, our AIT general-use backscatter technology vendor has faced challenges in developing and refining its ATR software, thus leading to additional lab testing and extensions in certifying and deploying its ATR software. In September 2012, contract awards were made to three vendors for the purchase and testing of next generation AIT units. TSA anticipates that next generation AIT units will have enhanced detection capabilities and a smaller footprint, enabling faster passenger throughput; all next generation AIT units will have ATR software. Based on analysis of processing time, size of the units, passenger throughput, staffing requirements, and AIT allocations, TSA has begun to install ATR-equipped millimeter wave AIT units at several airports that had previously been equipped with general-use backscatter AIT units.

Protecting Passenger Privacy

The Department of Homeland Security (DHS) is committed to protecting the privacy of all individuals by embedding and enforcing privacy safeguards and transparency in all DHS activities. The Department's network of Component Privacy Officers work with the DHS Privacy Office to ensure Department activities and incorporate privacy from the earliest stages of system and program development. DHS systems, initiatives, and programs are subject to a rigorous privacy compliance process, and undergo periodic reviews to ensure continued compliance. The DHS Privacy Office works closely with Component Privacy Officers, who provide operational insight, support, and privacy expertise for Component activities that require privacy compliance documentation.

The Privacy Impact Assessment (PIA) is a key document in the privacy compliance process and serves as a decision-making tool to identify and mitigate privacy risks throughout the development life cycle of a program or system. Using the Fair Information Practice Principles to assess and mitigate impacts on an individual's privacy, the PIA helps the public understand what information the Department is collecting; the purpose for collection; and how DHS will use, share, access, and store the information.

TSA worked collaboratively with the DHS Privacy Office in developing its PIA on AIT screening. TSA published its original PIA in January 2008 to cover AIT screening of passengers at the checkpoint, and has subsequently updated it three times to address improvements in the technology. The PIA provides transparency into the Department's operations and privacy protections related to AIT.

As described in its 2008 PIA (<http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-wbi-jan2008.pdf>), TSA instituted several safeguards prior to initial deployment to protect the privacy of individuals who are screened using AIT. TSA implemented a variety of measures, both technical and operational, to integrate and incorporate privacy considerations from the start, including providing signage at all AIT locations to inform the passenger of what the scanned image looked like and of their option to decline AIT screening in favor of physical screening.

TSA also instituted robust privacy protections for handling AIT images. Privacy protections in place where ATR is not yet available include filters to make AIT images not personally identifiable and officer review of the image in a remote location to preserve passenger anonymity. Images are transmitted securely between the unit and the viewing room to prevent them from being lost, modified, or disclosed. In short, the passenger and other travelers cannot see the image, and the officer viewing the image cannot see the passenger. Once an officer clears an individual, the image is no longer viewable or stored in the system. ATR-enabled units are not capable of storing or printing the generic image produced during screening. Both types of AITs transmit the images securely—the general-use backscatter units encrypt images during transmission, whereas the millimeter wave units transmit images in a proprietary format viewable only with proprietary equipment.

To provide additional public awareness of the privacy protections DHS implements for AIT, the DHS Chief Privacy Officer and TSA Privacy Officer have regularly communicated with privacy advocates and the Data Privacy and Integrity Advisory Committee regarding AIT. In addition, in February 2010, TSA submitted a Report to Congress on privacy protections and deployment of AIT entitled “Advanced Imaging Technologies: Passenger Privacy Protections.”

Meeting National Health and Safety Standards

TSA places a premium on the safety of the traveling public. Both types of AITs have been evaluated and found to meet all applicable national health and safety standards, including those published by the Institute of Electrical and Electronics Engineers for millimeter wave systems, and those published by the American National Standards Institute/Health Physics Society and the National Council on Radiation Protection and Measurements (NCRP) for general-use backscatter x-ray systems. In addition, the ATR software upgrade has no effect on the radiation emissions from AITs.

Each TSA general-use backscatter x-ray AIT system undergoes a radiation survey upon initial installation at an airport and every six months thereafter to ensure it stays in top working condition. TSA also performs radiation surveys after maintenance on components that affect radiation safety and at the request of employees. These surveys and periodic maintenance activities ensure the equipment operates properly and meets all emission limits, thus providing a high level of confidence in the safety of the equipment.

Testing by independent entities, including the Johns Hopkins University Applied Physics Laboratory, the Food and Drug Administration's Center for Devices and Radiological Health, the National Institute of Standards and Technology, and the U.S. Army Public Health Command have demonstrated that the radiation dose from a TSA general use backscatter AIT unit is well below established safety limits for passengers, operators, and bystanders, including children, pregnant women, frequent flyers, and individuals with medical implants. These safety limits are based on recommendations published by NCRP. In fact, the average person receives more radiation naturally each hour than they do from one screening by a general-use backscatter x-ray

AIT system and receives the same amount of radiation exposure from two minutes of flight.

These independent entities had full and direct access to TSA's currently deployed general-use backscatter AITs during their evaluation and/or testing.

Conclusion

AIT has proven to be the most effective available technology to protect the traveling public from evolving threats including non-metallic explosive devices, has a strong array of privacy protections, is being efficiently deployed, and has been documented by experts independent from TSA as safe for passengers and our own employees.

Thank you, Chairman Rogers, Ranking Member Jackson Lee, and members of the Subcommittee, for the opportunity to appear before you today. We look forward to answering your questions.