FEB 2 4 2010

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

**Transportation
Security
Administration**

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515-0004

Dear Chairman Thompson:

Thank you for your letter of January 21, 2010, regarding the privacy concerns that the Committee on Homeland Security has raised about the capability of Advanced Imaging Technology (AIT) to store, print, record, and export images.

The Transportation Security Administration (TSA) is committed to providing world class security while preserving privacy in our security programs. The AIT program meets this commitment through TSA's screening protocol that ensures complete anonymity for passengers undergoing AIT scans. TSA has not deviated from these operational protocols, which were first published in a Privacy Impact Assessment (PIA) in January 2008 before any devices in the AIT pilot went into operation. That PIA, and every PIA update since, states, "[w]hile the equipment has the capability of collecting and storing an image, the image storage functions will be disabled by the manufacturer before the devices are placed in an airport and will not have the capability to be activated by operators."

The procurement specifications mentioned in your letter support TSA's statements on AIT. The specifications state:

- The "systems will prohibit the storage and exporting of passenger images during normal screening operations" (para. 3.1.1.1.2); and
- "During the screening mode, the WBI [whole body imager] shall be prohibited from exporting passenger image data, including via the Security Technology Integrated Program (STIP) which is networking of technology. During the test mode, the WBI shall not be capable of conducting passenger screening. The WBI shall prohibit local storage of image data in all modes." (para. 3.1.1.1.2).

Below please find TSA's responses to your specific questions:

1. **Why does the procurement require the capability to store, print, record, and export images?**

   TSA requires AIT machines to have the capability to retain and export imagines *only* for testing, training, and evaluation purposes. Testing was done at the TSA Systems Integration Facility (TSIF) and the Transportation Security Laboratory (TSL). Images used for operator training were also recorded and used at the Threat Mitigation Laboratory (TML), the facility where Transportation Security Officer (TSO) training is developed. All AIT machines are delivered to airports without the capability to store, print, or transmit images, and cannot be modified by the operators. TSOs operating in the airport environment have neither the technical capability nor the authority to change the AIT into test mode.

2. **What is the extent of the ability AIT to store and transmit data?**

   AIT has the ability to store and transmit data; however, the only locations where the functionalities of storage and data transmission are enabled are at the testing and development sites: TSIF, TSL, and TML.

3. **Provide the titles of the employees who have the authority to place the machines in test mode and the number of employees that fall into this category.**

   Test Engineers at TSL – 8
   Test Engineers at TSIF – 3
   Training Development Contractors at TML – 4

4. **Under what circumstances, if any, can AIT machines be entered into test mode in the airport settings?**

   There are no circumstances when the system would be entered into the test mode in an airport environment.

5. **Who at TSA is authorized as a Level "Z" user? Please provide the titles of these employees and state if any government contractors or any other non-TSA officials are Level "Z" users. Also, provide the number of employees and or contractors that have this designation.**

   Test Engineers at TSL – 8
   Test Engineers at TSIF – 3
   Training Development Contractors at TML - 4
   Contracting Officer Technical Representative – 1
   Vendor Technicians – 26
   Headquarters Deployment Team – 3

   The above include both Federal employees and government contractors.

6. **What are the details of the privacy filters built into the AIT?**

   When the machines are delivered to an airport for screening operations, the privacy filters are already in place. The level of filtering is described in the PIA. The image filter setting is approved by TSA, it is configured into the imaging machine at the factory and cannot be changed by the operator of the machine in the airport environment.

   Each vendor's approved image filter is recorded in the published PIA. Any changes to these filters will be published in an updated PIA and widely communicated to the traveling public.

   Any changes to privacy settings on individual machines can only be made by the "Z" users. The only people with "Z" user access for use in the lab setting are select personnel in TSA's Office of Security Technology and technicians from the manufacturer.

7. **Has TSA asked the Chief Privacy Officer to amend or update the current Privacy Impact Assessment to reflect the storage capability of AIT and identify the individuals who have this authority?**

No. The PIA accurately states the operational storage capability of the AIT in the airport environment. Storage capability for AIT in the TSL and TSIF is not discussed because the flying public is not screened in those locations.

8. **What protections does the AIT have that will prevent people outside of TSA from obtaining image data through the device's USB and Ethernet capabilities?**

The machine *cannot* transmit or store the image onto the USB device. AITs used for screening operations at airports are not able to store, export, print, or transmit images. All images are deleted from the system after they are reviewed by the remotely-located operator. The image storage functions are disabled by the manufacturer before the devices are placed in an airport and do not have the capability to be activated by the operators. The screening statistical data that may be saved or transferred include an officer's user identification as well as log in and log out times.

The machines are not networked. The current specification does not have a STIP requirement and the referenced specification is out of date; therefore, they cannot be hacked. In addition, all produced images transmitted from the machine to the remote viewing room are encrypted.

Also, there are strict procedures applicable to AIT operation. No cameras, cellular telephones, or other devices capable of capturing an image are permitted in the image viewing room. Any official or employee who fails to follow these strict procedures is subject to serious discipline up to and including removal.

I appreciate that you took the time to share the Committee's privacy concerns about AIT and hope this information is helpful. If I may be of further assistance, please contact LaVita LeGrys, Assistant Administrator for the Office Legislative Affairs, at (571) 227-2717.

Sincerely yours,

Gale D Rossides

Gale D. Rossides
Acting Administrator