MEMORANDUM

Date: January 11, 2010
To: Interested Persons
From: EPIC – Marc Rotenberg, John Verdi, Ginger McCall
RE: Preliminary Analysis: Documents obtained from Department of Homeland Security concerning Body Scanners (EPIC v. DHS, #1:09-cv-02084 – FOIA)

I. Summary

EPIC has obtained the technical specifications and the vendor contracts for Whole Body Imaging ("WBI") devices or "body scanners" commissioned by the Department of Homeland Security ("DHS") for use in American airports. This came about as a result of a Freedom of Information Act ("FOIA") lawsuit that EPIC has pursued against the DHS. The documents described in this memo represent a partial disclosure. EPIC is anticipating the receipt of other documents from the DHS as well as other federal agencies.

Among the key findings, based on the documents obtained by EPIC:

- The device specifications, set out by the Transportation Security Administration ("TSA"), include the ability to store, record, and transfer images, contrary to the representations made by the TSA
- The device specifications, set out by the TSA, include hard disk storage, USB integration, and Ethernet connectivity that raise significant privacy and security concerns
- The DHS Privacy office failed to adequately assess the privacy impact of these devices
- There are additional documents that the DHS should disclose to the public; the Congressional committees that are considering the further deployment of these devices must look much more closely at their actual operation

Based on the materials received to date, EPIC concludes that further deployment and contracting for body scanners should be suspended until the privacy and security problems identified are adequately resolved.

About EPIC

EPIC is a public interest research organization in Washington, DC established to focus public attention on emerging privacy and civil liberties issues. EPIC routinely testifies before Congress, submits comments for agency rulemakings, and provides friend of the court briefs for federal and state courts. The EPIC Open Government Project provides information to the public about important government programs that impact privacy and civil liberties.

II. Background on EPIC FOIA

This memo refers to five documents that EPIC received on December 2, 2009 from the United States Department of Homeland Security and its component, the Transportation Security Administration in response to EPIC's April 14, 2009 Freedom of Information Act request for:

1. "All documents concerning the capability of passenger imaging technology to obscure, degrade, store, transmit, reproduce, retain, or delete images of individuals;
2. "All contracts that include provision concerning the capability of passenger imaging technology to obscure, degrade, store, transmit, reproduce, retain, or delete images of individuals;
3. "All instructions, policies, and/or procedures concerning the capability of passenger imaging technology to obscure, degrade, store, transmit, reproduce, retain, or delete images of individuals."

The EPIC FOIA request was assigned FOIA Case Number TSA09-0510.

Among the five documents, disclosed to EPIC by DHS, are two documents prepared by the TSA and three contracts between the TSA and Whole Body Imaging manufacturers. Two of these contracts are with Rapiscan and one is with L-3. One of the Rapiscan contracts is virtually identical to the L3 contract. The other Rapiscan contract contains an additional 50 pages regarding machine maintenance.

Three of these documents contain materials of particular significance for the privacy and security evaluation of Whole Body Imaging devices.

- The <u>TSA Procurement Specifications Document</u> sets out "the performance, design, verification requirements for WBI" mandated by the agency. (TSA Specifications Document, p. 1).
- The <u>TSA Operational Requirements Document</u> sets out the "minimum requirements for Whole Body Imaging (WBI) systems that provide the capability to locate potential threats on a person including beneath clothes or otherwise obscured." (TSA Requirements Document, p. 4)
- The <u>L3 Millimeter Wave Contract</u>. According to the vendor, L3 is a "is a prime contractor in Command, Control and Communications, Intelligence, Surveillance and Reconnaissance" and is "also a major provider of homeland defense products and services for a variety of emerging markets."[1]

The most significant findings contained in the documents disclosed to EPIC are listed below, with screenshots from the relevant documents. The documents total 286

[1] "L-3 Communications," http://www.l-3com.com/.

pages, of which 279 were released on full and 7 were released with redactions. The TSA has withheld other documents sought by EPIC in this case.

Note: The findings discussed below reflect the documents disclosed to date. Additional materials sought by EPIC likely contain other relevant information.

Status of EPIC v. DHS

The documents are a response to only Part 2 of EPIC's April 14, 2009 request. Due to DHS' failure to fully comply with the Freedom of Information Act, EPIC filed suit on November 5, 2009 to compel the disclosure of all documents responsive to EPIC's FOIA request. The case has been assigned Docket # 1:09-cv-02084(RMU). Because of DHS' failure to answer the lawsuit, EPIC filed a Motion for Default Judgment in federal district court in Washington, DC on January 8, 2010.

II. Most Important Revelations in Documents Disclosed to EPIC

1. "Level Z" - The TSA Can Disable Privacy Settings Altogether

Figure 1: TSA Procedural Specifications Document, p. C-1 (EPIC v. DHS)

User Access Level	User	Capabilities
Z	Transportation Security Administration Headquarters Contractor Maintenance Technician (see Note 1) Super User	Logon and Logoff Startup and Shutdown Enable/Disable Image Filters Access Test Mode Export Raw Image Data in Test Mode Modify Access Level Capabilities Upload/Download User Database Create and Modify Accounts (All Users) Download Data (see Note 1) Set and Alter Passwords (All Users) (see Note 1) Modify Baselined or Fielded Software (see Note 1) Access Operating System Note 1: Contractor Maintenance Technicians shall not set or alter passwords and shall download data only without alteration. Contractor "superuser" passwords will be disabled by a Government representative after site acceptance. Only Government approved software changes shall be made to the baselined or fielded software.

The TSA Procurement Specifications Document contains an "Access Control Levels Table", in Appendix C, that details the level of control different users will have. There are four levels of users: Level 3, 2, 1, and Z. Level Three, which is the basic operator level, has limited capabilities, including logon and logoff, startup and shutdown, access screening mode, screening passengers, and initiate fault isolation test. Levels Two and One have more advanced capabilities, including the ability to download WBI Field Data Reporting System ("FDRS") data and to access and view FDRS databases and reports. Field Data Reporting System data is a recording of events on the device (logons, logoffs, etc.). Level Z users have many additional capabilities, including the ability to download data, access test mode (which allows for image storage, as described below), enable/disable image filters, modify access level capabilities, access the operating system, and export raw image data in Test Mode.

These combined abilities allow Level Z users to disable privacy protections, save images, and then download those images (possibly to a USB key as detailed below). The capabilities described in the TSA's own "Procedural Specifications Document" refute the TSA's claims that the devices "cannot store, print, transmit or save the image."[2]

Level Z clearances are given to an unspecified number of users – government users at TSA Headquarters, private Contractor Maintenance Technicians, and ambiguous "Super Users."

2. Ten (Adjustable) Levels of Privacy

Figure 2: TSA Operational Requirement Document, p. 8 (EPIC v. DHS)

> **2.9. Quality Control**
>
> **The WBI shall (28) possess a built-in test function, which verifies key functions automatically on power-up and displays results.**
>
> **The duration of the power-up diagnostics function shall (29) be less than 1 minute.**
>
> **The WBI shall (30) provide ten (10) selectable levels of privacy.**

The TSA Operational Requirements Document contains a statement, on page 8 of the document, that "The WBI shall (30) provide ten (10) selectable levels of privacy."

This reveals that the privacy settings are adjustable , presumably with some providing a greater level of privacy protection and some providing a lesser level. This document refutes the TSA's claim that privacy protections have been put into place that cannot be altered by TSA operators.

3. "Test Mode" Allows the TSA to Store Images

[2] TSA: Imaging Technology, http://www.tsa.gov/approach/tech/imaging_technology.shtm.

The TSA Procurement Specifications Document reveals that the WBI machines are enabled with a "Test Mode" which allows for the storage of data, exporting of image data in real-time, exporting of raw or reconstructed image data, and creates a means of high-speed image data transfer.

Figure 3: TSA Procurement Specifications Document p. 5 (EPIC v. DHS)

3.1.1.3.1.2 Test Mode

For purposes of testing, evaluation, and training development, the WBI ***shall*** (22) provide a Test Mode. The WBI Test Mode ***shall*** (23) be the sole mode of operation permitting the exporting of image data. WBI Test Mode ***shall*** (24) be accessible as provided in the User Access Levels and Capabilities appendix.

When in Test Mode, the WBI:

- ***shall*** (25) allow exporting of image data in real-time;
- ***shall*** (26) prohibit projection of an image to the IO station;
- ***shall*** (27) provide a secure means for high-speed transfer of image data;
- ***shall*** (28) allow exporting of image data (raw and reconstructed).

This test mode can be accessed by Level Z users, allowing these users to export and transfer images.

Test Mode is also mentioned on page 4 of this document, which states, "When not being used for normal screening operations, the capability to capture images of non-passengers for training and evaluation purposes is needed. To ensure that image capturing maintains passenger privacy, the WBI will provide two distinct modes of operation: Screening Mode and Test Mode."

4. Training Images Exist

EPIC has previously made FOIA requests for images produced by WBI machines. The DHS has failed to release these documents. Now there is confirmation that these images exist. The TSA Operational Requirements Document that "The contractor shall provide a training library of 50 images that consist of a representative mix of passenger body types and gender."

Figure 4: TSA Operational Requirements Document p. 14 (EPIC v. DHS)

9.1.1. Training Simulator

The contractor shall (81) provide a simulator that emulates all operator functionality.

The contractor shall (82) provide a training library of 50 images that consist of a representative mix of passenger body types and gender.

Of the 50 images, 30 images shall (83) be of persons carrying threats.

The remaining 20 images shall (84) be of innocent persons.

This confirms that TSA possesses at least fifty images that should be disclosed to EPIC in response to EPIC's FOIA request.

5. Image Filters Can Be Disabled

As discussed in Item 1, image filters on the WBI machines can be disabled by Level Z users. These filters may provide some level of privacy protection (obscuring faces, etc.) and, if disabled, this protection is lost. An undisclosed number of users have the ability to disable filters, as described on page 5 of the TSA Procurement Specifications Document.

Figure 5: TSA Procurement Specifications Document p. 5 (EPIC v. DHS)

The WBI ***shall*** (10) provide image filters to protect the identity, modesty, and privacy of the passenger.

Enabling and disabling of image filtering ***shall*** (11) be modifiable by users as defined in the User Access Levels and Capabilities appendix.

6. The WBI Machines Run on a Standard Operating System – Windows XPe

The L3 Millimeter Wave Contract details the major system requirements on page 27 of the document. The contract specifies that the machines will run Windows XPe.

Figure 6: L3 Millimeter Wave Contract, p. 27 (EPIC v. DHS)

3.5 Major System Components

The WBI units shall consist of the following components:

- Single WBI Unit
- 17" monitor
- Keyboard and Mouse
- Windows XPe
- Side-by-side image display
- Year 1 Parts & Labor Warranty (in accordance with Section H.8)

This means that the machines would be subject to the security flaws and risks of the Windows XPe operating system.

7. The WBI Machines Use Standard USB Interfacing

The WBI machines are designed to transfer information via USB device. The TSA Procurement Specifications Document details the specific capabilities of the machines on page 10.

Figure 7: TSA Procurement Specifications Document p. 10 (EPIC v. DHS)

3.1.1.5.1 Data Storage/Transfer

The WBI system ***shall*** (98) provide capabilities for data transfers via USB devices. These devices ***shall*** (99) provide connectivity to download FDRS data as described in 3.1.1.5 and to upload/download a user database as defined in 3.1.11.2. A high capacity read/write drive ***shall*** (100) be installed to permit data uploads and downloads. All necessary software drivers and operating system services to support the data collection devices ***shall*** (101) be preinstalled and preconfigured.

USB devices are easily concealed and readily available. Allowing downloads from WBI machines to USB devices creates a very real risk that data may be removed on an unauthorized USB device and shared or stored elsewhere.

8. The WBI Machines have High Capacity Internal Drives

The TSA Procurement Specifications Document also reveals that the WBI machines are equipped with high capacity internal drives.

Figure 8: TSA Procurement Specifications Document p. 10 (EPIC v. DHS)

3.1.1.5.1 Data Storage/Transfer

The WBI system ***shall*** (98) provide capabilities for data transfers via USB devices. These devices ***shall*** (99) provide connectivity to download FDRS data as described in 3.1.1.5 and to upload/download a user database as defined in 3.1.11.2. A high capacity read/write drive ***shall*** (100) be installed to permit data uploads and downloads. All necessary software drivers and operating system services to support the data collection devices ***shall*** (101) be preinstalled and preconfigured.

These drives would not be necessary unless the machines were being used to store images.

9. The WBI Machines are Designed for Ethernet Interfacing

The TSA Procurement Specifications Document (on page 7) and the TSA Operational Requirements Document (on pages 10-11) reveal that the machines are equipped with Ethernet network interfacing capabilities. They employ a RJ-45 connector and are configurable with an IP address.

Figure 9: TSA Procurement Specifications Document p. 7 (EPIC v. DHS)

The WBI system:

(a) ***Shall*** (52) possess an Ethernet network interface equipped with an RJ-45 connector.

(b) ***Shall*** (53) support full/half duplex data rates of 10/100 mega-bits per second to support future requirements.

(c) ***Shall*** (54) support Transmission Control Protocol / Internet Protocol (TCP/IP).

This creates additional security concerns: that images could be leaked or stolen over this Ethernet network if it is not properly secured.

III. <u>Summary of What EPIC Learned from the Disclosed Documents</u>

Contrary to TSA's claims about WBI machines, these documents make clear that the WBI machines are designed to allow for the production of images with no privacy filters and to allow for the storage and transfer of those images. The capability to create unfiltered images and to store and transmit those images was expressly required by TSA in its Operational Requirements and Procurement Specifications.

These documents reveal that there are numerous security threats inherent in the WBI machines' design. The WBI machines are subject to outside security threats because they employ Windows XP operating system and the Ethernet network. More disturbingly, they are subject to inside security threats due to the existence of Level Z clearance, which allows an unspecified number of TSA employees, outside contractors, and generic "superusers" to disable privacy functions while at the same time storing and/or transferring data.

III. <u>DHS Privacy Review of Body Scanners</u>

The TSA, a DHS component, undertook a privacy review of Whole Body Imaging, which was published on October 17, 2008, approximately one month after the date of the TSA Procurement Specifications Document obtained by EPIC.[3]

The TSA Privacy Impact Review makes no mention of the device capabilities described in the TSA Procurement Specifications or Requirements Document. The TSA privacy review states:

> While 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.

As the documents obtained by EPIC from the DHS indicate, **<u>the TSA itself specified that the devices have the ability to store images.</u>**

This is an extraordinary oversight that calls into question the Privacy Impact Assessment process and the ability of the office of the DHS Privacy Office to uphold its statutory obligations to protect the American public and to "ensure that technologies sustain and do not erode privacy protections."[4]

I. <u>Further Areas of Examination</u>

With Congressional hearings scheduled on Whole Body Imaging later this month, it would be appropriate for the oversight committees to pursue the following topics related to the documents obtained by EPIC

1. What is the extent of the ability WBI imaging machines to store and transmit data? What is the significance of the USB, Ethernet, and disk storage capability? Who will have the authority to enter "Test Mode"?

2. What is the ability of WBI machines to create unfiltered pictures of passengers? What is the purpose of the various privacy settings? And who at TSA is authorized as a Level Z user and what oversight will be exercised over these individuals?

---

[3] DHS, "Privacy Impact Assessment for TSA Whole Body Imaging," (October 17, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf,
[4] Section 222 of the Homeland Security Act. See Privacy Coalition letter to Rep. Bennie Thompson and Rep. Peter King concerning the Chief Privacy Officer of the DHS (October 22, 3009), available at http://epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf

3. Do the WBI machines have adequate security protections that will prevent outsiders from obtaining image data through the devices' USB and Ethernet capabilities, as well as the Windows XPe operating system's security holes?

4. What are the details of the privacy filters (or settings) built into the WBI machines?

5. What consideration has been given to deployment of these devices in less than fully controlled settings, e.g. airports operated outside of the United States? Is it possible that WBI devices could be installed without remote operators, without privacy filters, or without storage capabilities disabled?

EPIC Resources on Whole Body Imaging

EPIC, Whole Body Imaging Technology
http://epic.org/privacy/airtravel/backscatter/

EPIC, Stop Digital Strip Searches
http://stopdigitalstripsearches.com/

EPIC, Spotlight on Surveillance: Transportation Agency's
Plan to X-Ray Travelers Should Be Stripped of Funding (2005)
http://epic.org/privacy/surveillance/spotlight/0605/

EPIC letter to Congress Concerning Failures at DHS Privacy Office
http://epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf

Legal Issues

- The federal Privacy Act limits the collection and use of personal information by federal agencies, including the TSA.

- The Homeland Security Act requires that the DHS Chief Privacy Officer conduct a thorough review of all DHS programs to assess their impact on privacy.

- The Fourth Amendment limits the conduct of searches by federal agents. Although the courts have permitted suspicionless "sui generis" searches in airports for safety-related contraband, the Supreme Court recently ruled impermissible the strip search of a high school student for contraband, and courts have expressed increasing concern about the reliability of invasive searches techniques.

- The DHS has been sued for exceeding its authority by searching air travelers for items, including cash, that have no relation to safety.

Contact

Marc Rotenberg, EPIC Executive Director
202-483-1140 x 106, rotenberg@epic.org

Ginger McCall, Assistant Director, EPIC Open Government Project
202-483-1140 x102, mccall@epic.org