TSA'S RECENT SCANNER SHUFFLE: REAL STRATEGY OR WASTEFUL SMOKESCREEN?

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

NOVEMBER 15, 2012

Serial No. 112–121

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

81–130 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY

MIKE ROGERS, Alabama, *Chairman*

DANIEL E. LUNGREN, California
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois, *Vice Chair*
ROBERT L. TURNER, New York
PETER T. KING, New York *(Ex Officio)*

SHEILA JACKSON LEE, Texas
DANNY K. DAVIS, Illinois
CEDRIC L. RICHMOND, Louisiana
RON BARBER, Arizona
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

AMANDA PARIKH, *Staff Director*
NATALIE NIXON, *Deputy Chief Clerk*
VACANT, *Minority Subcommittee Director*

CONTENTS

Page

STATEMENTS

The Honorable Mike Rogers, a Representative in Congress From the State of Alabama, and Chairman, Subcommittee on Transportation Security 1
The Honorable Danny K. Davis, a Representative in Congress From the State of Illinois 3

WITNESSES

Mr. Jonathan R. Cantor, Acting Chief Privacy Officer, U.S. Department of Homeland Security:
Oral Statement 3
Joint Prepared Statement 5
Mr. John Sanders, Assistant Administrator, Office of Security Capabilities, Transportation Security Administration:
Oral Statement 7
Joint Prepared Statement 5

FOR THE RECORD

The Honorable Mike Rogers, a Representative in Congress From the State of Alabama, and Chairman, Subcommittee on Transportation Security:
Letter From Chairman Mike Rogers to Hon. John S. Pistole 2
The Honorable Danny K. Davis, a Representative in Congress From the State of Illinois:
Joint Statement of Marc Rotenberg, President, EPIC; Ginger P. McCall, Director, EPIC Open Government Project; and Jeramie Scott, EPIC National Security Fellow 10

TSA'S RECENT SCANNER SHUFFLE: REAL STRATEGY OR WASTEFUL SMOKESCREEN?

Thursday, November 15, 2012

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TRANSPORTATION SECURITY,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 10 a.m., in Room 311, Cannon House Office Building, Hon. Mike Rogers [Chairman of the subcommittee] presiding.

Present: Representatives Rogers and Davis.

Also present: Representatives Walberg and Richmond.

Mr. ROGERS. The Committee on Homeland Security, Subcommittee on Transportation Security will come to order. This committee meeting today is to discuss TSA's use of backscatter AIT machines, and I would like to take this opportunity to welcome our witnesses, thank them for taking the time to prepare for this hearing and being here with us today. I really appreciate it.

Are you all getting feedback? It sounds like this microphone is being strange.

All right, thank you.

Three weeks ago TSA notified the public it was removing backscatter AIT machines from several large airports and replacing them with millimeter wave AIT machines. TSA initially said it would deploy these backscatter machines to smaller airports; however, TSA could not produce a list of small airports when prompted by the subcommittee. That is because the machines won't be going to smaller airports any time soon. Instead, TSA is moving those 91 backscatter machines worth $14 million of taxpayer money to its storage warehouse in Texas. According to TSA, this is because the testing of backscatter privacy software suddenly failed, and smaller airports don't have enough space to support the backscatter machines without privacy software.

At this time I would like to insert a letter for the hearing record that I sent to Administrator Pistole yesterday expressing concerns about the recent allegations of contractor malfeasance that may have led to the failed test that put us in this situation. Without objection, it is so ordered.

[The information follows:]

LETTER FROM CHAIRMAN MIKE ROGERS TO HON. JOHN S. PISTOLE

NOVEMBER 13, 2012.

Honorable JOHN S. PISTOLE,
Administrator, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598.

DEAR ADMINISTRATOR PISTOLE: I am deeply troubled by recent allegations of contractor malfeasance as it relates to the Transportation Security Administration's (TSA) use of backscatter Advanced Imaging Technology (AIT). According to information received by the subcommittee, it appears the manufacturer of backscatter AIT machines may have attempted to defraud the Government by knowingly manipulating an operational test of Automated Target Recognition (ATR) software in the field in order to have a successful outcome. In addition to these concerning allegations, I am extremely disturbed by TSA's apparent lack of oversight throughout the testing and evaluation of this technology.

I fully expect to discuss this situation at our previously scheduled subcommittee hearing on November 15, 2012, entitled: "TSA's Recent Scanner Shuffle: Real Strategy or Wasteful Smokescreen?" As such, please ensure that John Sanders, who will testify on behalf of your agency, is prepared to answer the following questions:

1. When did TSA first discover that the contractor might have manipulated an operational test?
2. What impact, if any, could the contractor's actions have on aviation security?
3. What actions has TSA taken to deal with the potential manipulation of an operational test?
4. What level of oversight does TSA provide during the testing process?
5. Who was responsible for conducting the operational test and certifying its success?
6. At the time TSA decided to move 91 backscatter AIT machines from large airports to small airports, when did the agency believe ATR software would be ready to install on those machines?
7. How long will those 91 backscatter AIT machines sit in storage?
8. Do you plan to remove the remaining backscatter AIT machines from the field? If so, when?

Thank you for your prompt and personal attention to this matter. I appreciate your continuing efforts to secure the Nation's transportation systems.

Sincerely,

MIKE ROGERS,
Chairman, Subcommittee on Transportation Security.

Mr. ROGERS. I hope we can get some answers today on this extremely disturbing situation.

Now, the reality is that TSA is squeezing backscatter machines into its warehouse next to useless puffer machines that we are all too familiar with. Perhaps the backscatter machines will be put to good use eventually, but that is the point: We just don't know.

In the mean time the subcommittee has some serious questions: How did the testing of privacy software for backscatter go so wrong? What level of oversight did TSA provide during the testing process? Why did TSA move backscatter machines out of the big airports before knowing which smaller airports to put them in? When will ATR be ready to install on backscatter?

Congress mandated that this software be installed by June. In addition, TSA still has not complied with the D.C. circuit court ruling to allow for public comment on the AIT, nor has the agency agreed to sponsor an independent third-party evaluation of the AIT's health effects, despite bipartisan consensus that an independent study would be beneficial. To me, it appears we not only are having a technology problem, but a significant transparency problem on our hands.

Today I hope we can get a logical answer to some basic questions about AIT and its future. I also look forward to getting a better understanding of the coordination that exists between DHS and TSA

when it comes to assessing passenger privacy issues up front to avoid these types of costly, convoluted situations where we shuffle machines around and then stick them in a warehouse.

With that, I now recognize the Ranking Member of the subcommittee, the gentleman from Illinois Mr. Davis, for his opening statement he may have.

Mr. DAVIS. Thank you very much, Mr. Chairman, and I want to thank our witnesses for being with us this morning.

The subcommittee has closely followed advanced imaging technology for several Congresses under both Democratic and Republican leadership. On this side of the aisle, my colleagues have questioned both the effectiveness of the technology and the cost of the machines. I have a few issues that cause us as much concern as to whether these machines undermine the fundamental right of privacy. It is gratifying to see that the Chairman shares both our concerns and our commitment to privacy.

On March 17, 2009, under the leadership of Congresswoman Jackson Lee, this subcommittee held a hearing evaluating the detection and screening technologies being used by the Department of Homeland Security. That hearing offered Members a chance to understand the enhanced screening technologies, protocols, and procedures. In the aftermath of the Christmas day bomber, also known as the underwear bomber, we expressed our support for the deployment of these advanced imaging technologies and were assured that these new machines would effectively diminish the threats that continue to put aviation security at risk.

Since 2009, DHS and TSA have taken steps to implement the AIT devices in most of the major airports in the United States. However, we know that no technology is perfect. Based on a conservative estimate, it appears that the Department has invested at least $80 million on this technology so far. Given the challenges that TSA faced in assuring privacy protections in these machines, and the forward movement of technology, we must consider where we go from here.

So again, I want to thank our witnesses for being here, and I want to thank you, Mr. Chairman, and look forward to the hearing.

Mr. ROGERS. I thank the gentleman.

We are pleased to have several distinguished witnesses with us today on this important topic. Let me remind the witnesses that their entire written statements will appear in the record. Our first witness, Mr. Jonathan Cantor, currently serves as acting chief privacy officer to the Department of Homeland Security, a position he assumed in August 2012. Mr. Cantor previously served as a senior policy official at both the Department of Commerce, and the Social Security Administration.

The Chairman now recognizes Mr. Cantor for his opening statement.

STATEMENT OF JONATHAN R. CANTOR, ACTING CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. CANTOR. Good morning, Chairman Rogers, and thank you. Thank you, Ranking Member Davis and distinguished Members of the subcommittee. Thank you for the opportunity today to testify about advanced imaging technology, or AIT.

As you know, the Department of Homeland Security is the first department in the Federal Government to have a statutorily mandated privacy officer. I joined the Department in July of this year as deputy chief privacy officer, and I previously served as the chief privacy officer for the Department of Commerce and in an equivalent position at the Social Security Administration. I have had the pleasure of serving as acting chief privacy officer since the departure of my predecessor Mary Ellen Callahan in early August.

The mission of the DHS Privacy Office is to protect the privacy of individuals and their personal information by embedding and enforcing privacy protections and transparency throughout the Department. The Privacy Office works to achieve this mission by fostering a culture of privacy and transparency; demonstrating leadership through policy and partnerships; providing outreach, education, training, and reports; conducting robust oversight and compliance reviews; and ensuring that DHS complies with Federal privacy, confidentiality, and disclosure laws, policies, and principles.

The Privacy Office works with the Department's robust network of component privacy officers to ensure that Department activities incorporate privacy from the earliest stages of system and program development. Component privacy officers provide operational insight, support, and privacy expertise for component activities that require privacy compliance documentation.

The privacy impact assessment, or PIA, is a public document in the privacy compliance process that serves as a decision-making tool to identify and mitigate privacy risks. The PIA uses the Fair Information Practice Principles to assess and mitigate impacts on an individual's privacy. It also 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.

The DHS Privacy Office works collaboratively with TSA to develop the Department's PIA on AIT screening. DHS 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 technology.

Prior to initial deployment, DHS instituted several safeguards to protect the privacy of individuals who are screened using AIT. These measures included 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 a physical screening.

DHS also instituted robust privacy protections for handling AIT images. Privacy protections in places where automated target recognition, or 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. These steps ensure that 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 not stored in the system and is no longer viewable.

ATR software upgrades enhance passenger privacy by eliminating passenger-specific images. Machines upgraded with ATR software generate a generic outline that is displayed on the screen located on the AIT machine and viewable by the public. ATR-en-

abled units are not capable of storing or printing the generic image produced during screening.

It is important to note that both with backscatter and millimeter wave machines, a passenger may always decline the AIT scan and receive a pat-down as an alternative.

To provide additional awareness of the privacy protection DHS implements for AIT, the DHS Privacy Office, in collaboration with TSA, has engaged with the public through multiple methods. We briefed the Department's Data Privacy and Integrity Advisory Committee on AIT and provided a site visit that included demonstration of AIT technology. We provided a similar demonstration of AIT at a TSA test facility for members of the privacy advocacy community. In addition, my predecessor hosted quarterly roundtable meetings with privacy advocates to discuss AIT and other timely topics.

For the 3 months that I have served as acting chief privacy officer, my office has continued to embed privacy protections throughout the Department. I am happy to answer any questions you may have.

[The joint prepared statement of Mr. Cantor and Mr. Sanders follows:]

JOINT PREPARED STATEMENT OF JONATHAN R. CANTOR AND JOHN SANDERS

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 Radi-

ation 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 6 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 2 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.

Mr. ROGERS. Thank you, Mr. Cantor, for your testimony. We appreciation you being here, and know your time is valuable.

Our second witness Mr. John Sanders currently serves as the assistant administrator for the Office of Security Capabilities at TSA. Mr. Sanders joined TSA in 2010 and served as the deputy assistant administrator for the Office of Security Technologies, where he focused on day-to-day operations and assisted TSA senior leadership in the development and execution of risk-based security. Prior to joining TSA, Mr. Sanders worked in the private sector. He has more than 20 years of experience in the aviation industry.

Mr. Sanders you are recognized for 5 minutes.

STATEMENT OF JOHN SANDERS, ASSISTANT ADMINISTRATOR, OFFICE OF SECURITY CAPABILITIES, TRANSPORTATION SECURITY ADMINISTRATION

Mr. SANDERS. Good morning, Chairman Rogers, Mr. Davis—or, sorry, Congressman Davis, and Congressman Richmond. Thank you for the opportunity to testify today.

The Transportation Security Administration screens approximately 1.8 million people at 450 airports every day, employing risk-based, intelligence-driven operations to prevent terrorist attacks and reduce our vulnerability to terrorism. We continue to evolve our approach by examining the policies, procedures, and technologies we use to conduct screening.

TSA works with the private industry to develop and deploy the best technology available to detect metallic and nonmetallic threats, such as the explosive devices used by the underwear bomb-

er on Christmas day 2009 and the improved device discovered in the disrupted plot this past May. These are threats that walk-through metal detectors cannot detect.

TSA currently operates a mix of millimeter wave and general-use backscatter AIT units at 200 airports. All of the millimeter wave AIT units have been upgraded with automatic target recognition functionality, and testing is under way for ATR in general-use backscatter machines.

Since the beginning of the AIT program, TSA worked closely with the DHS Privacy Office to ensure that this program was a model for passenger privacy protections. ATR software further enhances passenger privacy by eliminating passenger-specific images and improves throughput at the checkpoint. The software autodetects anomalies concealed on the body. They are then resolved through additional screening.

TSA places a premium on passenger safety with respect to AIT. Both types of AIT have been repeatedly evaluated and determined to meet all applicable National health and safety standards. These tests have demonstrated that the radiation from a TSA general-use backscatter AIT screening is well below established safety limits for individuals being screened, operators, and bystanders, including children, pregnant women, frequent flyers, and individuals with medical implants. 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 X-ray exposure from 2 minutes of flight at altitude on the aircraft they are boarding. General-use backscatter X-ray AIT systems undergo a radiation survey upon initial installation and every 6 months thereafter to ensure it stays in top working condition. The surveys and periodic maintenance activities ensure the equipment operates properly and meets all emission limits.

I would like to close by emphasizing the AIT is the best available technology to protect the traveling public from nonmetallic explosive devices, has a robust 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.

I look forward to answering your questions.

Mr. ROGERS. Did I just hear you say that it has been efficiently deployed?

Mr. SANDERS. Yes, sir.

Mr. ROGERS. We are taking 91 of these things worth $14 million and going to put them in a warehouse. That is efficient?

Mr. SANDERS. When we look at the number of passengers that we are screening, if you look at the redeployment, right now we are scanning with those machines about 26 percent of the passengers that are walking through the checkpoints. With the redeployment it allows us to increase that AIT utilization from 26 percent to 76 percent, which equates at those 7 airports to about 180,000 more passengers per day through our most effective technology.

Mr. ROGERS. So what is going to happen with these 91 machines?

Mr. SANDERS. It is my hope that the contractor that we are working with will be able to develop the ATR software. We will be able to put them on those machines and then redeploy them at a later date.

Mr. ROGERS. Now, you know, it was announced 2 or 3 weeks ago, thereabouts, that TSA was going to move these to smaller airports, and that has changed. They are going to go to the warehouse. What happened? What happened with the software upgrade that was supposed to be done? Were you all expecting to do a software upgrade before you put them in the smaller airports?

Mr. SANDERS. We made a decision in May of this year to do a redeployment, as I said, to provide the most effective and efficient solution. In the May-through-July time frame, the systems were undergoing operational test and evaluation, which completed at the end of July. Then there is a period where a systems evaluation report as well as a letter of assessment is written by DHS Test and Evaluation Group, and we were expecting to start the redeployment of those eight AIT systems, the general-use millimeter waves or the general-use backscatter systems, to smaller airports starting in October through the end of the year.

Mr. ROGERS. When did TSA first discover that the backscatter AIT vendor might have manipulated the operational test?

Mr. SANDERS. I wouldn't say, sir, that we believe—that we have any evidence that—documents that they absolutely did.

Mr. ROGERS. But my understanding is that you suspect it.

Mr. SANDERS. We have information that we have contacted the manufacturer to ask for additional information so that we can look into the matter further.

Mr. ROGERS. You said in your opening statement that these machines had been independently evaluated. Was that just as to the health risks, or was it to the efficacy of the machine?

Mr. SANDERS. Both, sir. With regards to the health effects, we have had numerous independent tests performed. They include the Food and Drug Administration, the Johns Hopkins University Applied Physics Laboratory, the U.S. Army Public Health Command, and the National Institute of Standards and Technology have all looked at them with regards to the safety, and all of those have independently verified——

Mr. ROGERS. What about the efficacy?

Mr. SANDERS. The efficacy has done—is being performed by both GAO, the DHS inspector general, as well as TSA's own covert testing.

Mr. ROGERS. Well, that is my concern, is how could the vendor manipulate the outcome if, in fact, a third party is doing the evaluation?

Mr. SANDERS. Again, sir, I don't have any concrete information at this point that the vendor absolutely did anything that would lead to malfeasance. I think right now it is predecisional. We are in possession of the information, and we have contacted the vendor to provide us additional information with regards to that so that we can actually determine if that did occur.

Mr. ROGERS. I understand that, but my question is this: If the vendor is not doing the evaluation, a third party is, how could the vendor manipulate the results, even assuming that that happened? How could they if there is a third party? The vendor wouldn't have any ability to manipulate them, would they?

Mr. SANDERS. No, sir, they would not have. Once the operational test and evaluation begins, the system is under configuration con-

trol, and there is no opportunity for the vendor to make any changes to the system. Again, at the beginning of the program, before something gets under way, we might believe that the system is in one configuration when it is not in that particular configuration.

At this point we don't know what has occurred, and as I have said, we are—we have contacted the vendor, and we are working with them to get to the bottom of it to see if there is any——

Mr. ROGERS. When you all made the announcement that you all were going to move these to smaller airports, was it your expectation to move them to the smaller airports with the current software configuration?

Mr. SANDERS. No, sir, it was——

Mr. ROGERS. It was only if you could upgrade the software to the stickman image.

Mr. SANDERS. Yes, sir, that is correct.

Mr. ROGERS. You really thought that it was going to be able—you were going to be able to do that?

Mr. SANDERS. Yes, sir, we did.

Mr. ROGERS. You didn't know at that time that you made the announcement that it was not possible?

Mr. SANDERS. No, sir, we had every belief that the contractor would be able to meet their commitments and provide the ATR, and we would have it in the field.

Mr. ROGERS. My time is expired. I got some more questions. We will do another round in a few minutes.

Mr. Davis is recognized.

Mr. DAVIS. Thank you, Mr. Chairman.

Before I begin with my questioning, I would like to ask unanimous consent that the prepared testimony of EPIC, the Democrat witness denied by the Majority, be inserted into the record.

Mr. ROGERS. Without objection, so ordered.

[The joint statement of Mr. Rotenberg, Ms. McCall, and Mr. Scott follows:]

JOINT STATEMENT OF MARC ROTENBERG, PRESIDENT, EPIC; GINGER P. MCCALL, DIRECTOR, EPIC OPEN GOVERNMENT PROJECT; AND JERAMIE SCOTT, EPIC NATIONAL SECURITY FELLOW

NOVEMBER 15, 2012

Mr. Chairman and Members of the subcommittee: Thank you for holding this hearing and for the invitation to EPIC to submit a statement for the record. The Electronic Privacy Information Center ("EPIC") is a non-partisan research organization, focused on emerging privacy and civil liberty issues. For the last several years, EPIC has devoted considerable attention to the problems with the Transportation Security Administration's ("TSA") airport screening procedures. In the course of this work, we have uncovered a great deal of information that we believe will be of interest to the Subcommittee on Transportation Security.

This statement summarizes several of our major findings, as well as the recent decision from the D.C. Circuit Court of Appeals in *EPIC* v. *DHS,* which held that the agency failed to undertake a public rulemaking as required by law. We believe that if the agency had pursued the public comment process at the outset, the decision to deploy backscatter X-ray devices could have been averted, taxpayer dollars saved, privacy and health risks avoided, and more effective techniques to safeguard air travel developed.

THE PUBLIC CONCERNS ABOUT AIRPORT SCREENING PROCEDURES

In the aftermath of 9/11, it was clear that steps needed to be taken to improve aviation security. However, not all measures developed were equally effective. Protecting cockpits on commercial aircraft was critical. But many of the devices developed for screening passengers, such as the "puffer" devices, proved ineffective. Among the most controversial was the deployment of Whole Body Imaging ("WBI") devices, designed to reveal the air traveler stripped naked.

In 2005, EPIC published the first report that examined the privacy and health impacts of the TSA's proposed body scanner technology.[1] Since that time we have organized public conferences, received complaints from the traveling public, and worked with other organizations that share our concern about this program.[2]

EPIC has also pursued Freedom of Information Act ("FOIA") cases to learn more about the body scanner devices. We believe it is essential to assess the actual operation of the devices. When we say that there are on-going privacy risks to American travelers and that the TSA has not done enough to safeguard privacy, we are not speculating. We are pointing to facts about the devices that are known to the TSA, which the agency has been reluctant to discuss with Congress or the American public.

Following two FOIA lawsuits against the agency, EPIC received the TSA's Procurement Specifications for body scanners.[3] The Procurement Specifications provided specific stipulations made by the agency for the vendors L3 and Rapiscan, which showed: (1) TSA required the body scanners to have the capability to store, record, transmit images of the naked human body, (2) that the machines were not designed to detect powdered explosives, and (3) that the privacy filters could be turned off.[4]

In the spring of 2009, when we became aware that the TSA was planning to deploy the body scanner for primary screening in U.S. airports, we worked with a broad range of organizations and respectfully petitioned Secretary Napolitano to postpone the planned deployment until the public was given the opportunity to express its views on this dramatic change in agency procedure.[5] We asked the Department of Homeland Security ("DHS") to suspend the body scanner program while conducting "a rulemaking process to receive public input on the agency's use of 'Whole Body Imaging' technologies."[6] While DHS began to aggressively deploy full-body scanners, EPIC received no response to our initial petition. In spring of 2010, EPIC submitted a second petition to Secretary Napolitano and DHS Chief Privacy Officer Mary Ellen Callahan and urged DHS to suspend the body scanner program in light of questions about the effectiveness of body scanners, traveler complaints, privacy risks, and religious objections.[7]

---

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

[2] See, e.g., EPIC, "Whole Body Imaging Technology and Body Scanners ('Backscatter' X-Ray and Millimeter Wave Screening)," *http://epic.org/privacy/airtravel/backscatter/;* EPIC, "EPIC v. DHS (Suspension of Body Scanner Program)" *http://epic.org/privacy/body_scanners/epic_v_dhs_suspension_of_body.html;* EPIC, "EPIC v. Department of Homeland Security—Body Scanners" *http://epic.org/privacy/airtravel/backscatter/epic_v_dhs.html;* and EPIC, "The Stripping of Freedom: A Careful Scan of TSA Security Procedures" (Public Conference) (Jan. 6, 2011), *http://epic.org/events/tsa/*. EPIC also maintains a webpage where travelers can fill out a Body Scanner Incident Report *(http://epic.org/bodyscanner/incident_report/)*.

[3] TSA Office of Security Technology System Planning and Evaluation, *Procurement Specification for Whole Body Imager Devices for Checkpoint Operations,* Sept. 23, 2008 ("TSA Procurement Specifications Document"), available at *http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf*.

[4] TSA Procurement Specifications Document at 5 (stating "[w]hen in Test Mode, the WBI: shall allow exporting of image data in real time; . . . shall provide a secure means for high-speed transfer of image data; [and] shall allow exporting of image data (raw and reconstructed)"); Several reports and articles reach a similar conclusion. See, e.g., Leon Kaufman and Joseph Carlson, An Evaluation of Airport X-ray Backscatter Units Based on Image Characteristics, Journal of Transportation Security, *http://springerlink.com/content/g6620thk08679160/fulltext.pdf;* GAO, "Aviation Security: TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain" (Mar. 17, 2010), *http://www.gao.gov/assets/130/124207.pdf*.

[5] Letter from EPIC and 33 organizations to Secretary Janet Napolitano, U.S. Dep't of Homeland Security (May 31, 2009), *http://epic.org/privacy/airtravel/backscatter/Napolitano_ltrwbi-6-09.pdf*.

[6] Id.

[7] Letter from EPIC, et. al. to Secretary Napolitano and Chief Privacy Officer Callahan, U.S. Dept. of Homeland Security (Apr. 21, 2010), *http://epic.org/privacy/airtravel/backscatter/petition_042110.pdf*.

Following the Secretary's failure to respond to either of our petitions calling for public rulemaking, EPIC filed a lawsuit against DHS in the D.C. Circuit Court of Appeals. In the suit, we argued that the airport body scanner program violated several privacy laws, the Administrative Procedure Act, and the Fourth Amendment. We said that the Department of Homeland Security "has initiated the most sweeping, the most invasive, and the most unaccountable suspicionless search of American travelers in history."[8]

The D.C. Circuit Court of Appeals ruled that the TSA failed to undertake the required notice-and-comment rulemaking when the agency chose to make body scanners the primary screening method at U.S. airports.[9] The Court ordered TSA to "act promptly" in conducting a notice-and-comment rulemaking.[10] Since that decision in July of 2011 we have sought to have the agency comply with the Order of the court.

With respect to the other claims, the D.C. Circuit Court of Appeals determined that there was no substantive violation of privacy rights because "[n]o passenger is ever required to submit to an AIT [Advanced Imaging Technology] scan." The Court expressed further concern about the agency's conduct:

"Signs at the security checkpoint notify passengers they may opt instead for a patdown, which the TSA claims is the only effective alternative method of screening passengers. A passenger who does not want to pass through an AIT scanner may ask that the patdown be performed by an officer of the same sex and in private. Many passengers nonetheless remain unaware of this right, and some who have exercised the right have complained that the resulting patdown was unnecessarily aggressive."

EPIC, 653 F.3d at 3.[11] Even with this clear determination from the court, we continue to receive complaints from passengers that they are not told they can opt out or that they receive overly aggressive pat-downs when they do.

THE RISK OF MORE WIDESPREAD DEPLOYMENT OF WHOLE BODY IMAGING DEVICES

EPIC pursued additional efforts regarding the development of mobile body scanners, the use of body scanners at courthouses, and the radiation risks presented by backscatter X-ray body scanners. Additionally, EPIC continued to push for TSA to do the court-ordered notice-and-comment rulemaking in the face of persistent delay by the agency.

Mobile Body Scanners

The use of body-scanner technology has expanded beyond air travel to include use at other venues and the use of mobile scanning technology. In March 2010, the DHS released a "Surface Transportation Security Priority Assessment," which detailed the agency's plans to conduct risk assessments and implement new body-scanner technology in America's surface transportation system.[12] In 2006 and again in 2009, body-scanner technology was tested on Port Authority Trans-Hudson New York/New Jersey train riders. Moreover, mobile body scanners traditionally used in the warzones of Afghanistan and Iraq, have now been deployed on U.S. streets.[13]

In response to a 2010 Freedom of Information Act request and subsequent lawsuit, EPIC obtained documents from the DHS indicating that the agency has spent millions of dollars developing and acquiring mobile body-scanner technology to be used in surface transit and other high-occupancy venues.[14] According to the documents obtained by EPIC, the Federal agency plans to expand the use of these systems to monitor crowds—peering under cloths and inside bags away from airports.

---

[8] Opening Br. For Petitioners EPIC Chip Pitts, Bruce Schneier, and Nadhira Al-Khalili, available at *http://epic.org/EPIC_Body_Scanner_OB.pdf.*

[9] *EPIC* v. *U.S. Dep't of Homeland Sec.,* 653 F.3d 1, 8 (D.C. Cir. 2011).

[10] Id.

[11] The Court further stated "any passenger may opt out of AIT screening in favor of a patdown, which allows him to decide which of two options for detecting a concealed, nonmetallic weapon or explosive is least invasive." EPIC, 653 F.3d at 10.

[12] TSA, Surface Transportation Security Priority Assessment, available at *http://www.whitehouse.gov/sites/default/files/rss_viewer/STSA.pdf.*

[13] Andy Greenberg, *Full-Body Scan Technology Deployed in Street-Roving Vans,* FORBES, Aug. 24, 2010, *http://www.forbes.com/sites/andygreenberg/2010/08/24/full-body-scan-technology-deployed-in-street-roving-vans/.*

[14] DHS, "Privacy Impact Assessment for the Rail Security Pilot Study Phase II at PATH" (July 12, 2006), available at *http://epic.org/privacy/body_scanners/EPIC_Body_Scan_FOIA_Docs_Feb_2011.pdf.*

Scanners in Courthouses

In another example of body scanners being used outside the context of airport security, EPIC filed a FOIA request with the United States Marshalls Service to obtain information about the agency's use of full-body scanners for courthouse security. EPIC pursued the case in Federal court, and has obtained acknowledgement by the U.S. Marshalls Service that a single machine has stored "approximately 35,314 images" of the full-body scans of courthouse visitors over a 6-month period.[15]

Notice-and-Comment Rulemaking

After the D.C. Circuit Court of Appeals' 2011 ruling mandating that the TSA "promptly" undertake notice and comment rulemaking,[16] a year passed without agency action. EPIC then urged the Court to require the Secretary of Homeland Security to begin a public comment process or suspend the program.[17] The agency subsequently replied that it will "finalize documents" by February 2013.[18] The D.C. Circuit Court of Appeals' then laid out a firm deadline for the TSA, stating that it expects the agency to publish the rule before the end of March 2013.[19]

REJECTION OF BODY SCANNERS OUTSIDE THE UNITED STATES

The United States remains one of the very few countries in the world that subjects air travelers to body screening technology and perhaps the only country that continues to use backscatter X-ray devices. The European Union, and the 27 member countries it represents, rejected the use of backscatter X-ray devices at airports.[20] Additionally, the European Union adopted strict operational and technical requirements for the use of body scanners generally.[21] The additional conditions include, for example, not linking the image to the screened person, informing passengers of the conditions under which the scanning takes place, and giving passengers the right to opt out.[22]

CONCLUSION

The TSA's decision to remove the backscatter X-ray devices from major airports in the United States lends considerable support to the objections that EPIC and others have raised about the airport screening program. Perhaps if the agency had undertaken the public rulemaking when many organizations and air travelers asked them to do so, money would have been saved and risks to health, privacy, and religious interests of travelers diminished.

Still, the subcommittee should press the agency to begin the public comment process. Travelers have the right to express their views about the agency program.

Mr. DAVIS. Thank you, thank you very much, Mr. Chairman.

Mr. Sanders, there was an article published earlier this week regarding sensitive information you provided to Congress regarding potential vendor misconduct. Could you explain for the committee why it is important that sensitive information regarding potential misconduct by a vendor not be leaked publicly before the vendor has the opportunity to respond?

Mr. SANDERS. Yes, sir, if I could answer that question with regards to my experience from private industry. I can say as a former small business owner, it can be devastating to the business to have allegations made that have not—the proper due process has not been allowed to take place so that you can respond to those before

[15] EPIC Press Release, *Documents Reveal that Body Scanners Routinely Store and Record Images,* Aug. 3, 2010, *http://epic.org/press/EPIC_Body_Scanner_Press_Release_08-_03_10.pdf.*

[16] *EPIC.,* 653 F.3d 1 (D.C. Cir. 2011).

[17] EPIC's Petition for a Writ of Mandamus to Enforce This Court's Mandate, July 17, 2012, available at *http://epic.org/privacy/body_scanners/EPIC-Petition-for-Writ-of-Mandamus.pdf.*

[18] Resp't Resp to Opp'n to Pet. For Writ of Mandamus at 2 (Aug. 30. 2012), available at *http://epic.org/privacy/body_scanners/DHS-Response-in-Opposition.pdf.*

[19] United States Court of Appeals for the District of Columbia Circuit Court Order (Sept. 25, 2012), available at *http://epic.org/privacy/body_scanners/DC-Cir-Mandamus-Order.pdf.*

[20] European Commission Press Release, *Aviation Security: Commission Adopts New Rules on the Use of Security Scanners at European Airports,* Nov. 14, 2011, *http://europa.eu/rapid/pressrelease_IP-11-1343_en.pdf.*

[21] Id.

[22] Id.

it gets into the press, and it becomes a discussion, if you will, in a public forum that does not allow the company to defend themselves.

Mr. DAVIS. So it is very possible that the allegations not necessarily be proven, and unnecessary damage then would have been done to the vendor as well as to the users as well?

Mr. SANDERS. Yes, sir, that is a possibility.

Mr. DAVIS. While I am asking, a February 2012 DHS OIG report on TSA's use of backscatter AIT units reviewed previous TSA radiation studies, but did not include the results of any of the new tests. My question: Has TSA ever conducted testing on the day-to-day and the cumulative effect of workplace "zinging" radiation on TSOs and other TSA employees, and if not, why? If so, can we provide the results of those tests?

Mr. SANDERS. Yes, sir. We have conducted both independent and—independent tests as well as tests by TSA, and we would be happy to share those with you.

Mr. DAVIS. Then while integrating ATR software into its AIT devices, TSA has moved older backscatter X-ray machines out of the major airports with a high volume of passengers. Please explain the rationale behind this and the efforts that will be taken to ensure privacy and security requirements are met at locations receiving the backscatter X-ray machines.

Mr. SANDERS. So the redeployment was done to provide the most effective and efficient security possible to the traveling public. When we moved those machines out, we knew that we could increase, dramatically increase, the AIT utilization as well as the number of passengers that would be screened by our most effective technology to detect nonmetallic threats.

As I said earlier, the number of passengers at those 7 airports that we are now screening as a result of that redeployment has increased by 180,000 passengers per day. In response to your question with regards to the security of and the safety when it comes to the smaller airports, it was always our intention in the redeployment to ensure that ATR was on those systems before they were redeployed to the smaller airports.

Mr. DAVIS. Well, let me ask you, to date how much money has been invested in AIT machines, and how much will we need to invest before TSA gets to its target deployment numbers?

Mr. SANDERS. To date we have spent about $140 million on AIT equipment, but $100 million of that is for the millimeter wave system, and about $40 million is for the general-use backscatter systems.

With regards to your question on how do we—how much additional money will we have to spend? I can't answer that question right now. It is something that we are looking at, and the reason I can't answer that is TSA is transforming into a risk-based, intelligence-driven organization, as this committee is aware. As part of that, we are making decisions that—with regards to PreCheck and what we do with risk-based security. As part of that, we are looking at the business case around AIT equipment, understanding that it is critically important that we use AIT technology because it is the best technology that we have available to mitigate against known and evolving threats. But we don't have a final number

with regards to how many we will have to put in—how many systems we will need once we move forward with the risk-based security initiatives.

Mr. DAVIS. Thank you very much.

Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

The gentleman from New Orleans Mr. Richmond is recognized for 5 minutes.

Mr. RICHMOND. Thank you.

Mr. Sanders, I think earlier this year it was mentioned that you all wanted to purchase an additional 200 AIT machines. How many did you purchase, and how many do you think you need to have full coverage?

Mr. SANDERS. In May of this year, Mr. Richmond, we purchased an additional 200 systems, bringing the total that we have purchased to 1,000 systems. Right now our stated full operational capability is 1,800 systems to cover all of our lanes at all of the airports. As I said, though, that we are reevaluating what that full operational capability is going to be given the initiative that Mr. Pistole kicked off with regards to risk-based security.

Mr. RICHMOND. You mentioned, and the Chairman asked you a question about it also—you mentioned efficiency, and I think you can talk about the machines and make sure they are deployed, but when you are talking about efficiency, tell me what you are talking about.

Mr. SANDERS. I am talking about a couple of things. I am talking about the number of passengers that we can put through our most effective technology to look for nonmetallic threats. Also I am talking about the passenger experience. If you look at the amount of time it takes for a pat-down right now, it takes about 80 seconds to do a pat-down. If you put an individual through an AIT system with an image operator attached to it, that takes a certain amount of time as well. But when we move to ATR, we can get that processing time down to 12 seconds, which allows us to put more people through them, thereby using our most beneficial technology to detect a threat.

Mr. RICHMOND. So you are strictly limiting that to efficiency in terms of technology. I understand you are saying that a pat-down is 80 seconds compared to 12 seconds going through the machine, but that doesn't calculate the human decisions that are made going through checkpoints. Part of, I guess, my question to you is do you all coordinate from the technology side with the actual people who guide people through, and do all of those things to make sure that things are working efficiently?

Let me just give you my short frustration. You can have all of the machines in the world, but if you don't have two or three tables put together so people can put their items into those things to go through the machine so that they can walk through the AIT, then we are not becoming more efficient. The technology is more efficient, but the incompetence reduces the efficiency of the machine.

So have you all—and I guess from the technology standpoint, have you all worked with the human factors and the people who make the decisions to tell them what an optimal site should look like in terms of being efficient so people can get through in the 12

seconds? The machine is 12 seconds, but not the process to get through it. So that is my question.

Mr. SANDERS. Yes, sir, we work very closely with the Office of Security Capabilities on that very point.

I misunderstood your question. So when we deployed the AIT systems originally, we never had the full staffing to allow us to handle that. So what we had to do is make some risk-based decisions, and what we decided at the time, because of the intelligence, is to move FTEs away from other layers of security and apply them to the AIT systems.

Now that we have the ATR, it allows us to process people. It also allows us to make decisions to move those FTE to other security layers so that we are getting the efficiencies that you are referring to.

Mr. RICHMOND. Well, and I would just say that in terms of technology, I don't have many complaints, and I think that you all are putting a good effort in trying. But my experience now—and I guess the new word is "evolving." I am evolving on privatizing of TSA, because I just am getting increasingly frustrated with the incompetency of the checkpoints, and not just—not the people at the checkpoint, but the management at the checkpoint.

So I would just ask you to take that back to TSA, that the staunch supporters that they have had they are losing over small decisions that any business person or person with common sense would make at checkpoints. The management is increasingly frustrating not only in my home airport, but at other airports also.

Thank you, Mr. Chairman. With that I yield back.

Mr. ROGERS. I completely concur with Mr. Richmond's observations, and I have conveyed that to Mr. Pistole that the Department has a real problem with the public level of confidence, but it is penetrating the Congress pretty badly, and you all have got to remedy that. You really do.

I am really aggravated about this $91 million being wasted. You know, we have made the mistake with the—you all made the mistake with the puffer machines, and now you are going to have to move them over in the warehouse to put these machines in. It is like you spend money on the latest technology first and then test it later, and we are broke. I mean, the country, we are really struggling with some tough budgetary decisions, and it is just really hard to understand how this happens. Now I understand that TSA has spent $5 million developing this ATR software for the backscatter machines, and it is not working. Do you know how much more money you are going to spend to get this software right?

Mr. SANDERS. Sir, we have no intention to spend additional money on the ATR software.

Mr. ROGERS. Okay, good. I am glad to hear that.

Mr. Cantor, you talked a little bit a while ago about you put the signs up letting people know they have got a choice between going through the AIT machines or a pat-down. Have you all thought about giving them another alternative, that if they don't have a problem with the software, they can go through a lane that has these? Because some people like me don't care. If I can get through that line faster, it doesn't matter to me. Rather than put these

things in a warehouse, have you thought about just allowing the public that option?

Mr. CANTOR. Matters about how the machines are actually deployed——

Mr. ROGERS. The privacy issue.

Mr. CANTOR. Okay.

Mr. ROGERS. I mean, some people just don't care. I mean, some people are very sensitive to it, and I understand and appreciate that. But I can tell you that if you had a lane that said, you know, this is the stickman lane, and the line is twice as long as this lane, and if you don't—if you are not concerned about the privacy issue, you can go through this lane, a lot of folks are going to say, let us do it. Why put the things in a warehouse when you can give us that option?

Mr. CANTOR. From a privacy perspective we designed the operational protocols for the original machines; for example, the TSO in a separate room and obscuring of the image. Those operational proposals from a Privacy Office's perspective are still valid for those machines. The ATR-enabled devices are also a valid, you know, implementation of that, so the operational usage would be a decision on that TSA would make.

Mr. ROGERS. But to your knowledge, as the privacy officer, you are not aware that that has been discussed?

Mr. CANTOR. Not with my office.

Mr. ROGERS. How about you, Mr. Sanders?

Mr. SANDERS. Sir, I would say that these—it has never been a question whether these machines are effective from a security performance perspective.

Mr. ROGERS. That is my point. So why are you going to put them in a warehouse when you can give consumers another option and still use the machines? I mean, $91 million is a lot of money. Or is it—how much? Fourteen million dollars.

Mr. SANDERS. Fourteen million dollars.

Mr. ROGERS. For 91 machines.

Mr. SANDERS. Yes, sir. We are putting them in the warehouse waiting to see how the ATR deployment—or development works out so that we can deploy them with ATR. That decision is primarily based on the mandate to have ATR in all the machines by June 1 of this year, or of 2013.

Mr. ROGERS. Okay. According—so are you going to make that deadline, the mandate?

Mr. SANDERS. Yes, sir. We will make the deadline that all of the machines in the field have ATR software on them.

Mr. ROGERS. By June 2013.

Mr. SANDERS. Yes, sir.

Mr. ROGERS. Okay. How long would it take for the 91—or how long do you expect the 91 machines to sit in storage?

Mr. SANDERS. Sir, at this point I cannot answer that. We are talking to the manufacturer on the time line to get to the ATR, and we are waiting to hear back from them.

Mr. ROGERS. What about the remaining 155 backscatter machines? What is going to happen with them?

Mr. SANDERS. That goes back to your earlier question, sir. If we are not able to make the—we are going to make the deadline of

June 1, 2013, to have ATR in all of the AIT systems in the field, so we will have to make business decisions with regards to that as we progress and learn additional information.

Mr. ROGERS. My understanding is you have the next generation of AIT, which is AIT–2, coming out soon; is that correct?

Mr. SANDERS. Yes, sir.

Mr. ROGERS. What developments, if any, can you share with us on that technology?

Mr. SANDERS. We awarded three contracts to three different companies. One of them—we have awarded three contracts to three companies. The total value of each of those contracts is about $1 million for low-rate initial production. We are going through the testing process now to ensure that they are suitable and effective, and then we will make decisions on the procurement once we have those results.

Mr. ROGERS. All right. Thank you very much. My time is expired.

Mr. Davis, if you have any additional questions, you are recognized.

Mr. DAVIS. Thank you very much, Mr. Chairman.

Mr. Sanders, let me just ask, do you know how much—what the total dollar value is of security devices and machines that we have in storage?

Mr. SANDERS. Yes, sir. It is roughly about $155 million that is in storage waiting for redeployment, or waiting to be disposed.

Mr. DAVIS. We do expect that much of that is going to be used; that it is just a matter of when we are able to effectively do so.

Mr. SANDERS. Yes, sir. It is a combination of machines or equipment that has to be disposed because it has served its purpose and it has come to the end of its useful life, as well as equipment that we are waiting to deploy. We expect that in 2013 that that number will be down closer to about $75 million.

Mr. DAVIS. Thank you very much.

Mr. Cantor, could you describe for us the role the DHS Privacy Office plays in responding and addressing privacy complaints pertaining to airport screening operations? Please speak to the procedures and policies used by the DHS Privacy Office in assessing and investigating privacy complaints made by travelers.

Mr. CANTOR. Yes. As you know, the DHS Travelers Redress Inquiry Program, more commonly known as DHS TRIP, serves as a one-stop shop for traveler redress for all of the DHS components. DHS TRIP provides a mechanism through which passengers can voice their concern about particular travel experiences, including their experience with AIT or pat-downs.

If the TRIP system tasks a complaint involving AIT or a pat-down to the Privacy Office for review, we would refer it to TSA's contact center and to the TSA Privacy Office as required by TSA's policies. The DHS Chief Privacy Officer serves as a member of the TRIP advisory board, and my office's privacy oversight team works with any relevant component as well as the DHS Office of Civil Rights and Civil Liberties to effectively address TRIP complaints tasked to the Privacy Office.

Mr. DAVIS. Does the DHS Privacy Office have a position on the deployment and continued use of AIT machines that are not equipped with the ATR privacy software?

Mr. CANTOR. Our position with the deployment of non-ATR-enabled machines is that as long as they follow the approved privacy protocols that we went through with TSA and developed in our privacy impact assessment, that is okay from our perspective.

Mr. DAVIS. Thank you very much.

Mr. Chairman, I have no further questions and yield back.

Mr. ROGERS. I thank the gentleman.

I just got a few remaining questions, and this is for Mr. Cantor. Would you agree that DHS and TSA underestimated the privacy concerns with AIT machines when that technology was moved into the marketplace?

Mr. CANTOR. No, I don't think so. We understood from the outset that many people would find this technology uncomfortable, and that is why the Department took its responsibility to protect the privacy of each and every passenger very seriously. We deployed AIT only after we were fully confident it would work in an operational environment, and with the appropriate privacy safeguards in place.

As threats changed and the technology evolved to meet those threats, we continue to update the privacy protections while fulfilling our missions, and we continue that rigorous process of considering the available technology and updating our privacy protections as appropriate.

Mr. ROGERS. Are you suggesting that you all moved to the ATR just—and it wasn't in response to the privacy concerns?

Mr. CANTOR. It would be my view that we moved to the ATR as a happy combination of both. It has operational benefits for TSA in addition to having an added privacy benefit. However, at the time that the initial procurements took place to deploy the AIT machines, there was no option of satisfactory ATR-enabled devices.

Mr. ROGERS. What kind of review or evaluation did you do before deployment of the machines to kind of gain a perspective on how people may react to them before you made the purchase?

Mr. CANTOR. Sir, the way that we traditionally work with components is we partner with the component. The components would come to us with the proposal or an idea to move something. We would work together with them, evaluate their proposal, talk to them about privacy-mitigation strategies, working through the component privacy officer.

In this case that is exactly what we did. We worked through the TSA Privacy Office with TSA and closely evaluated the technology, you know, responded to their concerns about the threat and their operational realities in terms of dealing with that threat, and helped, working with them, design operational protocols and technological protocols that we could put in place to help mitigate the risks to privacy.

Mr. ROGERS. How closely does your Department work with TSA on these issues?

Mr. CANTOR. Very closely.

Mr. ROGERS. Can you give us some assurance based on that working relationship that you are going to be able to avoid this kind of situation in the future?

Mr. CANTOR. Yes. I mean, as a matter of process, we subject every program throughout the Department with privacy implica-

tions to rigorous review. I don't sign PIAs unless I am satisfied that, you know, the component has sufficient privacy protections in place. Indeed, the initial deployment of AIT incorporate many privacy protections, some of which we have already gone through, such as the signage, the remote viewer of the TSO, and no ability, you know, to see the person going through the screening. That evolution that you have seen in AIT to AIT with ATR-enabled devices demonstrates that we are dedicated to continually improving our technologies, including the screening technologies, and how we protect privacy.

You know, we have reviewed our privacy safeguards for AIT as the technology has changed, and we will continue to do so to ensure future screening technologies——

Mr. ROGERS. Let me ask you, do you believe that smaller airports are going to have the physical capacity to take these machines once the ATR software upgrades are possible? There is a lot of—you know, when you think about some of the smaller airports, these things take up a lot of room. Do you think it is realistic to expect to move them into these smaller airports?

Mr. CANTOR. I would have to defer to my colleague on the size of the airports and their operational capabilities.

Mr. ROGERS. Mr. Sanders.

Mr. SANDERS. Yes, sir, I do.

Mr. ROGERS. We may have to have a hearing. We will get some airport people in here to talk about that. I am real concerned about that.

But I will close with this: You know, $155 million is a lot of money, and I want you all to understand you are making it really tough on the Congress to fund this kind of stuff when we find out you keep putting it in a warehouse after you find out it is not working or working the way it ought to work. These are just large sums of money, and it is just hard.

I would also point out, I have been a little surprised at the way you have pushed back on this thought about the manipulation of the operational test. It was not us that suggested that happened; it was TSA. You know, I find it difficult to understand how that could happen given that you have acknowledged that there were third parties doing the test. It seems to me the Department, you know, is trying to find a scapegoat.

But I just hope that you take back to the Department you have all got to get a handle on this kind of procurement and acquisition process, because it is really killing your ability on Capitol Hill to continue to get funded for these kinds of projects.

With that, do you have any more questions, Mr. Davis?

Mr. DAVIS. No. Mr. Walberg is here.

Mr. ROGERS. Mr. Walberg is recognized for any questions he may have. Welcome to the committee.

Mr. WALBERG. Thank you, sir. Sorry to be late. I think I will defer the questions for now, since I don't know what has been asked.

Mr. ROGERS. Okay. All right. With that, I want to thank the witnesses for their testimony, their preparation and their time. I know it take a lot of time and energy to get ready for these things, and I really do appreciate it.

I will remind the witnesses that we will leave the official record of the committee open for 10 days. There may be some Members that weren't here, or, like Mr. Walberg, that just got here, that may have some additional questions, or I may, that we will submit to you, and we ask that you reply to those in writing if you could.

And with that, this hearing is adjourned.

[Whereupon, at 10:45 a.m., the subcommittee was adjourned.]