ASSESSMENT OF CHECKPOINT SECURITY: ARE OUR AIRPORTS KEEPING PASSENGERS SAFE?

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MARCH 17, 2010

Serial No. 111–57

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

56–783 PDF WASHINGTON : 2010

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

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
WILLIAM L. OWENS, New York
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
DINA TITUS, Nevada
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
EMANUEL CLEAVER, Missouri
JAMES A. HIMES, Connecticut
DINA TITUS, Nevada
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CHARLES W. DENT, Pennsylvania
DANIEL E. LUNGREN, California
PETE OLSON, Texas
CANDICE S. MILLER, Michigan
STEVE AUSTRIA, Ohio
PETER T. KING, NEW YORK *(Ex Officio)*

MICHAEL BELAND, *Staff Director*
NATALIE NIXON, *Deputy Chief Clerk*
JOSEPH VEALENCIS, *Minority Subcommittee Lead*

CONTENTS

Page

FOR THE RECORD

ASSESSMENT OF CHECKPOINT SECURITY: ARE OUR AIRPORTS KEEPING PASSENGERS SAFE?

Wednesday, March 17, 2010

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

The subcommittee met, pursuant to call, at 2:00 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [Chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, Thompson, Luján, Himes, Titus, Dent, Lungren, and Austria.

Ms. JACKSON LEE [presiding]. The subcommittee will come to order. This subcommittee is meeting today to receive testimony on checkpoint security. Our witnesses will help us assess how effectively we are deploying processes, procedures, and technologies to enhance security at airports both at home and abroad.

These meetings that you have consented to participate in are so much a part of securing America.

Let me thank the witnesses ahead of time for their commitment to this Nation. When we give testimony and hold hearings, many times it is thought that it is perfunctory, that information goes into large records, and that actions are not generated.

This is a serious issue both in terms of the incident that occurred at Newark Airport that showed an individual going in the wrong direction, but creating sufficient havoc to shut down the airport, then, of course, a very renowned incident that occurred on Christmas day. That, too, is in the eye of not only America, but around the world, and those who intend to do us harm.

Your testimony is crucial today, and we appreciate that.

I am interested in making everyone aware that as we proceed through this process, we will be holding a series of hearings to constantly be engaged in how we can secure America. I yield myself now time to give my opening statement.

We are here today to discuss how we are increasing the security of airport checkpoints in the wake of the Christmas day terrorist attack in the skies over Detroit. Given the risks to our aviation sector, it is imperative that we take a critical look at how DHS is integrating an effective layered security approach into our aviation security program.

Today we will examine DHS processes to acquire and deploy effective passenger screening technologies and procedures. This includes the testing, evaluation, and approval of machines and equipment designed for use at airport security checkpoints. Coordination between DHS' Science and Technology Directorate and the Transportation Security Administration is essential to ensuring that the best technology is deployed in a systematic way to address current and emerging threats to the aviation system.

The need for effective coordination was once again made plain by the incident on Christmas day. It is clear that our adversaries still believe that our aviation sector is the point of attack and that they would develop novel approaches to carry out their objective. Accordingly, we must stay at least one step ahead, and this coordination is an essential prerequisite for doing so.

However, the strength of coordination between TSA and S&T has been called into question by the Government Accountability Office and developers of innovative technologies. The breach cannot exist. It can no longer exist. The hand in glove relationship between S&T and TSA and the inventiveness of the American people and many others is crucial to securing the millions of people that use the modes of transportation which we are responsible for securing.

Not on my watch will we allow the slowness of the process or even the potential unworkableness of the process stop the ability of this committee to secure America. That is the responsibility of the Homeland Security Committee under the leadership of Chairman Bennie Thompson.

We have heard that navigating the DHS labyrinth of testing, evaluating, and certifying technology has dissuaded the acquisition and production of cutting-edge technology. Earlier this year I directed staff to take a close look at the relationship between TSA and S&T. This examination raised concerns about the cohesion between both components.

Specifically, there appeared to be an almost incoherent process for testing and deploying technologies and security protocols. It is just plain slow. Roles and responsibilities were not clearly defined, and it was clear from briefings that increased oversight of this area is imperative. Components of DHS must work in tandem in order to keep the American people safe, and that is why I am happy that TSA, S&T, and GAO are here today.

Again, as I begin this hearing, I thank all of you for the public service that you render and your commitment to securing America. How can we do it better together?

Last summer the House overwhelmingly supported H.R. 2200, an authorization bill for TSA, which included a provision that TSA and S&T develop a plan to more effectively deploy processes and technologies to improve airport security.

We have passed that legislation in the House. We are waiting patiently for this bill to move so it can be passed in the other body and so the President can sign this innovative and important legislation. We cannot wait much longer. The question is how long will we wait? The answer is not long. This provision will ensure that both organizations are operating under the same parameters when developing measures to bolster checkpoint security.

It must be noted that the Flight 253 incident also highlighted vulnerabilities at foreign airports with direct flights to the United States. The security at the last point of departure airports is as critical to our aviation security as the security of our domestic airports.

We know that work has been done. We know that there have been international visits to assess those ports that many Americans are leaving from overseas. There has been work, but there needs to be partnership in the work that includes technology, inventiveness and, yes, the bottom line of: How do we secure America?

I would like to take this opportunity to congratulate the Secretary for her dedication to strengthening our relationship with foreign partners. This diplomacy is important to ensuring that all airports meet an acceptable standard for checkpoint security. TSA has been working with foreign airport operations and air carriers in implementing stronger security screening protocols, but challenges remain. Today we will hear about these international challenges and the ways to best address them.

This hearing will also afford us with an opportunity to talk about the much-discussed advance imaging technology or whole body imaging machines. Nearly all relevant stakeholders are present today, so we will glean several important perspectives about the efficacy of the AIT and the deployment plan.

The administration has announced its intent to ultimately deploy 1,000 of these machines by the end of fiscal year 2011. While I applaud this development, we will look forward to fleshing out the particulars that will make this decision an even better decision.

We want to work with the administration. We are partners in being able to secure this Nation. For example, the cost of this deployment is significant, and it brings with it the need for increased TSA personnel and potentially significant costs to modify airport terminals and checkpoints. Let me clarify when I say increased TSA personnel. Increased, proficiently trained personnel is the key to helping us secure America.

Today we will discuss AIT and how it fits into DHS' plan for deploying technology and how to address the operational challenges associated with this deployment. We will also learn about the Secretary's attempt to have similar technology located abroad.

Today's hearing offers more than just an opportunity to discuss the status quo in aviation security. It is an opportunity to envision where we want to be. Technologies have their limitations, but empowering our TSA workforce with adequate training, information, and innovative technologies will undoubtedly lead to the next generation of checkpoint security.

I know that this is the first of many examinations of this important topic. We need the commitment and resources of Government and industry to promote more efficient airport security. Accordingly, I was pleased to learn about the recent establishment of a blue ribbon panel by the travel industry aimed at providing recommendations on how to secure the aviation sector in the 21st century.

Today's hearing affords us with an opportunity to see how we can efficiently deploy security technologies and procedures. These

require the relevant components of the Department to work together, and it also requires the Department to work with relevant stakeholders, many of which are represented today.

The Chairwoman now recognizes the Chairman of the full committee, the gentleman from Mississippi, who has been a major leader on both the fixing of the system, but also the pushing of the system to be able to expeditiously and absolutely secure America, Mr. Thompson of Mississippi, for his opening statement.

Mr. THOMPSON. Thank you very much, Madam Chairwoman, and let me thank you for holding this important hearing.

The work we do today will help to inform us of DHS' effort to keep the flying public safe and secure. In addition, the preparation for such a hearing may also help the relevant components of DHS—in today's case, S&T and TSA—to move more effectively to cooperate.

With that said, I would like to thank the witnesses for appearing before us today.

In January the full committee held a hearing that took a close look at the events surrounding the attack on December 25. The attack on December 25 was a reminder that terrorists continue to plot against our aviation system, so we must remain vigilant and aggressive. That hearing shed light on the counterterrorism efforts and the information-sharing processes that must be improved across the Government as we address the very real terrorist threat. Likewise, the hearing highlighted some of the steps taken by the Department soon after the December 25 incident, particularly in the aviation sector.

The Department has made great efforts to enhance airport security in the aftermath of that attack by strengthening relationships with international partners and enhancing checkpoint security here at home. I look forward to an update from the Department on its development in partnering with foreign countries and how those efforts will bolster security.

In addition, we are taking another step today to evaluate the processes in the Department that are in place to develop, procure, and deploy innovative technologies and procedures at our airports. Without robust and clear processes, we will never be one step ahead of those wishing to do us harm. GAO has called into question whether the process DHS has in place is effective, and we will hear more about that from all the stakeholders today.

Obviously, there is no single technology or procedure that we can rely on to mitigate all the risks. However, through a strategic and transparent framework, we can ensure that our checkpoints are able to incorporate a layered security program that successfully identifies people wishing to cause us harm. I hear a lot about our layered security approach, and I believe it has the potential to make us more secure.

I look forward to hearing from our witnesses and am committed to improving our checkpoint security in order to meet the changing challenges we face. There is clearly a lot of work to do to improve how the Department deploys small technology and procedures so I am pleased this hearing will help to begin this process. I now yield back.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman.

I want to acknowledge the presence at the time of the gavel of Mr. DeFazio and to acknowledge Members, Mr. Luján, Mr. Himes, and Ms. Titus, for their presence here today as we begin this hearing. Thank you so very much.

Other Members of the subcommittee are reminded that under committee rules opening statements may be submitted for the record.

I welcome our first panel of witnesses. Our first witness is Mr. Robin Kane, the assistant administrator in the Office of Science Technology at TSA. Mr. Kane oversees the development and implementation of security technologies across multiple modes of transportation.

Our second witness, Mr. Bradley Buswell, is a deputy under secretary at the S&T Directorate at DHS. He is accompanied by Dr. Susan Hallowell, who is the director of Transportation Security Laboratory, which is a part of S&T. Dr. Hallowell will assist with any technical elements of our discussion.

Our third witness, Stephen Lord, is the director of GAO's Homeland Security and Justice Issues Division and is responsible for directing numerous GAO engagements on aviation and surface transportation issues. We welcome him back.

Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Kane.

I have indicated in my statement, as the Chairman has, we do this hearing in the backdrop of what took the attention and the breath of the world and the United States of a Christmas day bomber on one of our most special and sacred days to penetrate, if you will, the sanctity of our security and to send signals that we want to correct. We are not beginning today, but this is a continuing, to ensure that these kinds of incidences are stopped.

Mr. Kane, we are prepared to hear you at this time for 5 minutes.

STATEMENT OF ROBIN KANE, ASSISTANT ADMINISTRATOR, SECURITY TECHNOLOGY, TRANSPORTATION SECURITY ADMINISTRATION

Mr. KANE. Good afternoon, Chairwoman Jackson Lee, Chairman Thompson, distinguished Members of the subcommittee. Thank you for the opportunity to appear today to discuss aviation security technology at passenger screening checkpoints in the United States.

TSA procures and deploys all of the screening technologies for people and their bags in U.S. airports. Approximately 1.8 million people and their belongings are screened by these technologies every day. TSA operates and maintains over 10,000 pieces of equipment used by our transportation security officers to conduct this screening.

The attempted attack on Northwest Flight 253 on December 25 was a powerful reminder that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. The Department of Homeland Security's review of the Flight 253 incident produced five recommendations that Secretary Napolitano presented to the President.

Technology plays a critical role in three of those recommendations. We are accelerating the deployment of advanced imaging technology in U.S. airports and seeing an international move in the same direction. We have built on our partnership with the Department of Energy to establish a new initiative to engage the National laboratories in developing emerging aviation security technologies. And we are working with our international partners to strengthen international security measures, particularly technology requirements.

Advanced imaging technology, or body scanners, as they have become more commonly described, is the most promising current technology for detecting small quantities of explosives concealed on passengers. We expect to deploy almost 500 units that will be operating in the airports by the end of this calendar year. The President's fiscal year 2007 budget request includes funding for an additional 500 AIT units, which would bring the total to nearly 1,000 Nation-wide. This will provide screening of nearly 65 percent of passengers for metallic and nonmetallic threats.

The other primary screening device at the checkpoint is the X-ray machine. Advanced technology X-ray machines are the latest technology to screen carry-on bags. An upgraded version, which is ready for field testing, includes automated detection algorithms for explosives, a capability that we retrofitted to the over 900 AT X-rays that are currently deployed to 81 airports Nation-wide. TSA will procure approximately 1,300 additional machines, and we will deploy them to nearly every checkpoint by the end of 2011.

Explosive trace detection equipment, or ETDs, have been the workhorse of the TSA technology fleet since the agency's inception. ETDs detect a wide range of explosives. TSA has been expanding the use of ETDs at checkpoints and gates in airports to enhance the unpredictability of screening and increase overall effectiveness.

The President's fiscal year 2011 budget includes a request for 800 portable ETD units to complement the approximately 2,000 tabletop units we have at these checkpoints today.

We are fielding these technologies that are effective against known and emerging threats. However, terrorists are agile and determined. TSA works closely with DHS Science and Technology to ensure we have a solid process to identify and develop additional promising technologies. TSA uses intelligence and operational feedback to identify requirements that assist S&T in prioritizing research and development efforts.

TSA works with the technology industry to drive improved detection capabilities. We issue formal requests for information and requests for proposals to provide direction on TSA's intents for future purposes. TSA also hosts industry days and meets regularly with vendors to refine requirements and identify potential new solutions.

Part of the procurement process is a rigorous testing regime to ensure those technologies meet the requirements and are ready to perform in an operational environment. We test equipment in three settings: A lab environment such as the Transportation Security Lab, at TSA's systems integration facility, and in the field or operational test and evaluation.

Technologies that pass this rigorous three-part testing are included on our qualified products list. TSA leaves this process open so vendors may enter the testing and qualification process when they are ready, resulting in what we call a rolling QPL. TSA competitively purchases equipment off these QPLs, resulting in better value to the taxpayer.

TSA and S&T also work closely with our international partners and numerous working groups to improve aviation security technology. These groups focus on coordinating R&D efforts and harmonizing technology standards and processes.

TSA's qualified products lists are considered the gold standard by many countries. Sharing this type of information with those countries offers greater options for determining the mix of technology, processes, and people to meet international security standards.

Technology is critical to aviation security; however, it is just one element in the multi-layered strategy that includes the behavior detection officers, bomb appraisal officers, Federal air marshals, canine teams, well-trained personnel, and a ready and engaged traveling public. While new technologies offer great promise in DHS' on-going efforts to secure our homeland, no technology provides a guarantee against the threat of a terrorist attack. We need the layered security regime.

Thank you for your continued assistance and support of TSA and for the opportunity to speak with you today. I welcome any questions when it is appropriate.

[The statement of Mr. Kane follows:]

PREPARED STATEMENT OF ROBIN KANE

MARCH 17, 2010

Good afternoon Chairman Jackson Lee, Ranking Member Dent, and distinguished Members of the subcommittee. Thank you for the opportunity to appear today to discuss the technology utilized at passenger screening checkpoints at United States airports. The attempted attack on Northwest Flight 253 on December 25 was a powerful reminder that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. As Secretary of Homeland Security Janet Napolitano has testified at recent hearings regarding the attempted attack, this administration is determined to thwart terrorist plots and disrupt, dismantle, and defeat terrorist networks.

Today I will give an overview of passenger screening technologies currently in place and discuss the Transportation Security Administration's (TSA) on-going development and deployment of new technologies, in coordination with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), the Transportation Security Laboratory (TSL), and other key Federal agencies and academic and private sector centers of research. I will discuss some of the promising technologies we are currently developing, and how we are working to ensure that the technological advances we are making in the United States become available to enhance screening by our partners abroad.

RESPONSE TO NORTHWEST FLIGHT 253

Following the attempted attack on Northwest Flight 253, President Obama made clear that we need to take additional actions to address the systemic vulnerabilities highlighted by that failed attack. At the President's and Secretary Napolitano's direction, to enhance the safety of the traveling public, DHS will pursue several key steps in which technology plays a critical role:

- Accelerate deployment of advanced imaging technology to provide greater explosives detection capabilities and encourage foreign aviation security authorities to do the same.
- Establish a partnership on aviation security between DHS and the Department of Energy and its National laboratories in order to develop new and more effec-

tive technologies to deter and disrupt known threats and proactively anticipate and protect against new ways by which terrorists could seek to board an aircraft.
- Work with international partners to strengthen international security measures and standards for aviation security.

ACCELERATE TECHNOLOGY DEPLOYMENT

TSA has already made great strides in accelerating the deployment of technology to enhance both checkpoint screening (for passengers and carry-on baggage) and checked baggage screening. The $1 billion in American Recovery and Reinvestment Act (ARRA) funds provided to TSA in 2009 has played a major role in this effort. Of the $1 billion allocated to TSA for aviation security projects, approximately $700 million was dedicated to checked baggage screening technology, including in-line Explosives Detection Systems (EDS), and approximately $300 million was allocated for checkpoint explosives detection technology.

TSA uses a comprehensive research, testing, and deployment process to ensure that technology deployed to U.S. airports is effective in detecting threats and can withstand the operational and environmental rigors of a system that screens nearly 2 million passengers each day. The technology development lifecycle takes time—several years in some cases. While TSA and its vendors are working to deploy the latest aviation security technology to U.S. airports as quickly as possible, there are development logistical limits to how quickly new technologies become available.

As is the case with TSA's approach to overall security, the objective in technology development and deployment is to find the most effective means to detect threats while facilitating travel and commerce and respecting personal privacy. The following are some of the technologies that we are deploying in pursuit of that goal.

Advanced Imaging Technology (AIT)

One of the most promising current technologies for detecting small quantities of explosives concealed on passengers is AIT. AIT safely and effectively screens passengers for metallic and nonmetallic threats, including weapons and explosives, without physical contact. TSA has assessed multiple types of AIT systems, including backscatter X-ray and millimeter wave.

Currently, 40 AIT units are deployed at 19 U.S. airports for both primary and secondary screening. Through ARRA funding, we procured 150 additional units, which will be deployed principally for primary screening purposes starting in early 2010, and we are in the process of procuring an additional 300 AIT units in fiscal year 2010. TSA has also budgeted for an additional 500 AIT units in fiscal year 2011, which will bring the total to approximately 1,000 Nation-wide.

In its deployment of AIT across the country, TSA has implemented strong safeguards—reviewed by the DHS Privacy Officer—to ensure the protection of passenger privacy and anonymity. TSA requires manufacturers to include software algorithms in AIT systems that blur the face on the image of the body during screening. Additionally, TSA requires that AIT machines in operation at airports cannot store images of screened passengers; storage capability is activated only for testing purposes. Furthermore, the Transportation Security Officer (TSO) who views the AIT image is located separately from the TSO at the screening location who assists the passenger through screening, to avoid a specific individual from being associated with the image. Finally, the passenger may choose whether to undergo screening by this technology or proceed through a walk-through metal detector (WTMD) followed by a pat-down. Current data shows that over 98 percent of passengers opt for AIT screening.

TSA continues to explore additional privacy protections through automated threat detection, which would transmit images only when an alarm is triggered. In collaboration with DHS S&T, the security technology industry, and our international partners, software development is currently underway and will be followed by testing to ensure effective detection with minimal false alarms.

Explosives Trace Detectors (ETD)

ETD equipment can detect a wide range of explosives, including Pentaerythritol tetranitrate (PETN), a key explosive used in the attempted attack on Northwest Flight 253. ETDs have previously been used to examine carry-on baggage for the presence of explosives residue and are currently being piloted at five airports for use on passengers' hands. Approximately 2,000 units are currently deployed in airports Nation-wide for passenger screening and the President's fiscal year 2011 budget includes a request for $60 million for approximately 800 portable ETD machines ($39 million) and associated checkpoint consumables ($21 million). Expanding the use of

ETD beyond checkpoints and throughout airports will enhance the unpredictability of screening and increase overall screening effectiveness.

Advanced Technology (AT) X-Ray

Advanced technology (AT) X-ray machines are the latest technology to screen carry-on baggage. AT X-ray provides multiple views and a greatly enhanced display that is much clearer and more detailed than that provided by current X-ray technology. The latest version, which is ready for testing in the field, includes automated detection algorithms for bulk explosives and liquid explosives—capabilities that will be retrofitted to the 922 AT X-ray machines currently deployed to 81 airports Nation-wide. TSA anticipates having contracts in place by the end of fiscal year 2010 to purchase approximately 1,300 machines, enough to cover remaining U.S. airports, with deployment to be completed in early 2011. In fiscal year 2011, we plan to buy 25 additional units and will upgrade the existing fleet with new software algorithms that bring that equipment in line with the new equipment.

Next Generation Bottled Liquid Scanner (BLS–2) Technology

Bottled liquid scanners provide TSA with enhanced liquid detection capability by screening carry-on luggage to detect potential explosive liquid or gel threats. BLS–2 systems can work either in conjunction with AT X-ray screening or as stand-alone devices to conduct primary screening of liquids. TSA has already purchased 500 units and has started deployment to airports, with plans to procure and deploy an additional 800 BLS–2 systems to all U.S. airports by the end of 2010.

DHS AVIATION SECURITY PARTNERSHIP WITH THE DEPARTMENT OF ENERGY AND ITS NATIONAL LABORATORIES

As a result of the President's directive on aviation security following the attempted attack on Christmas day, DHS has built on its partnership with the Department of Energy (DOE) and its National Laboratories in order to develop new and more effective technologies to deter and disrupt known threats and proactively anticipate and protect against new ways by which terrorists could seek to board an aircraft. We have established joint working groups to bring the laboratories' technical expertise to bear on three critical areas: Aircraft vulnerabilities, systems analysis of our approach to detection and screening, and new technology with potential application to aviation security.

In addition, a number of interagency initiatives are already underway including: Research and development to increase screener efficiency and effectiveness; enhanced detection of passengers who intend to do harm and personnel who may pose insider threats; next-generation fully automated checkpoints for detecting weapons and explosives on individuals for aviation, mass transit, large public venues or other potentially high-risk buildings; enhanced automatic imaging systems and trace explosives detection equipment that screen for explosives and other prohibited items; and new tools for biometric identification and credential validation.

Many of these projects are expected to show significant progress in the near-term as similar or related projects were already underway. Other projects, such as developing next-generation fully automated checkpoints for detecting weapons and explosives on people, will likely take several years to become operational.

WORKING WITH OUR INTERNATIONAL PARTNERS

DHS is also working with international partners, law enforcement, and the aviation industry to enhance international aviation security standards and practices—particularly for international flights bound for the United States. The fiscal year 2011 budget requests funding to further expand TSA's international presence and enhance support to countries that seek assistance, including $40 million and 74 positions (37 FTE) to manage international programs at 15 of our 19 existing offices around the globe. The 74 new positions, which include 34 Transportation Security Specialists, 10 International Industry Representatives, and a 10-person Rapid Response Team, will be strategically placed in high-risk areas such as the Middle East and Africa.

In January, Secretary Napolitano dispatched Deputy Secretary Lute on an international trip during which she and other senior Department officials consulted with dozens of ministers, deputy ministers, and senior officials from 13 countries across six continents to review security procedures and technology being used to screen passengers on flights bound for the United States and work with our international partners on ways to collectively bolster our international aviation security system.

As a result of this trip, the Spanish Minister of Interior Minister invited Secretary Napolitano to participate in the first organizational meeting of the Spanish EU Presidency of Justice and Home Affairs ministers, a plenary of 33 countries in To-

ledo, Spain. At this meeting, there was broad consensus and a clear sense of urgency to take immediate action to strengthen security measures. Specifically, Secretary Napolitano and her European counterparts signed a joint declaration affirming their collective commitment to strengthening information sharing and passenger vetting, deploying additional proven security technologies, and bolstering international aviation security standards. Secretary Napolitano found a similarly strong consensus in Geneva where she met with the leaders of the airlines that are part of the International Air Transport Association—which represents approximately 230 airlines and more than 90 percent of the world's air traffic. All attendees agreed that government and the private sector must work collaboratively both to develop enhanced international security standards and—most importantly—to effectively implement them.

These meetings were the first in a series to bring about international agreement on stronger aviation security standards and procedures. For example, the International Civil Aviation Organization, the United Nations agency that focuses on international civil aviation, has facilitated several regional aviation security meetings—including one in Mexico City, jointly hosted by Mexico and Brazil and one in Tokyo—to build on the progress made in Toledo and Geneva.

The discussions from these meetings and the deputy secretary's trip will culminate in an international ministerial meeting, being planned for later this year, to develop, review, and ultimately adopt key measures and proposals for increasing aviation security worldwide.

TSA and S&T also work closely with our international partners through a number of working groups, task forces, and other committees focused on improving aviation security, identifying promising technologies, and harmonizing technology standards and processes. These groups include:

- *DHS Explosives Standards Working Group (ESWG).*—The ESWG is co-chaired by TSA and the DHS Office of Infrastructure Protection, Protective Security Coordination Division (PSCD). This group provides DHS agencies a forum for collaboration and information exchange with other Federal, State, and local government agencies and non-government entities on explosives countermeasure standards and conformity assessment measures. This group also drives explosives standards requirements and policy.
- *European Civil Aviation Conference (ECAC) Technical Task Force.*—ECAC is an intergovernmental organization comprised of 44 Member States throughout Europe. TSA meets with ECAC representatives multiple times throughout the year to partner on technology standards and policy development related to aviation security.
- *Technical Support Work Group (TSWG).*—TSA participates in the TSWG, a group sponsored by the Defense Department, with an emphasis on technology research, engineering, and development for aviation security-related projects. The group has significant influence internationally and funds projects submitted from both U.S. and non-U.S. members.
- *NATO Explosives Detection Group.*—TSA meets with other NATO member countries to collaborate on next generation explosives detection technology and to share best practices.

CONCLUSION

Technology is critical to aviation security; however, it is just one element in a multi-layered strategy that includes Behavior Detection Officers, Bomb Appraisal Officers, Federal Air Marshals, canine teams, well-trained personnel, and a ready and engaged traveling public. The attempted attack on Christmas day failed due in no small part to passengers and crew members who acted quickly and courageously to subdue the attacker and gain control of the situation.

While new technologies offer great promise in DHS's on-going efforts to secure our homeland, no technology is a silver bullet against the threat of a terrorist attack. This reality makes it all the more critical that we are working together at all levels—Federal, State, and local governments, our international partners, and the American public—to counter threats.

The Department of Homeland Security and the Transportation Security Administration are using every tool at our disposal to prevent, detect, and deter terrorism and protect the traveling public.

Thank you for your continued assistance to TSA and for the opportunity to speak with you today. I would be pleased to respond to your questions.

Ms. JACKSON LEE. Thank you for your testimony.

I now recognize Mr. Buswell to summarize his statement for 5 minutes.

STATEMENT OF BRADLEY I. BUSWELL, DEPUTY UNDER SECRETARY, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. BUSWELL. Good afternoon, Chairwoman Jackson Lee, Chairman Thompson, Ranking Member Dent, distinguished Members of the committee. I am honored to appear before you today to report on the Science and Technology Directorate's research, development, test, and evaluation efforts relating to airport passenger screening technology.

First, I would like to personally thank the committee Members and the staff for their continuing support of S&T in our mission to deliver technology to protect the American people. S&T is charged with providing technical support and tools to the major DHS operating components and our Nation's first responders, all of whom are on the front lines of homeland security every day.

S&T funds basic research and technology development and supports the Department's major acquisition programs through testing, evaluation, and the development of standards. As Mr. Kane said, the Transportation Security Administration has the lead role in defining the performance requirements of equipment that are installed at our airports as part of our security measures. DHS, S&T, and TSA coordinate closely on research efforts and equipment test and evaluation to ensure that the Department is investing in technologies that meet TSA's operational needs to protect the traveling public.

The Department's research and development priorities are primarily customer-driven through the Capstone Integrated Product Team process. The customers and stakeholders in this process play a key role in informing DHS S&T's decision-making about research and development investment. DHS customers chair the Capstone IPTs and establish their desired capability priorities based on their assessment of risk in their respective mission areas. TSA leads the Transportation Security Capstone IPT. Mr. Kane does that personally.

Our research priorities in aviation security have been and continue to be to improve the capability of currently fielded screening equipment and procedures in the near term and develop and deploy new equipment and procedures that are more effective in the long term.

All three of our research portfolios, the product transition portfolio focused on the near-term deliverables, the basic research portfolio focused on long-term discovery and invention, and the innovation portfolio led by the Homeland Security Advanced Research Projects Agency, or HSARPA, participate in this IPT process.

While the IPT members drive the selection of the near-term product transition projects, the expressed needs that arise from this process also inform the selection of projects in our basic research portfolio and the higher risk, high payoff innovation portfolio undertaken by HSARPA.

The Capstone IPT process is effective at identifying high-priority technology needs, but we are constantly looking for ways to better

meet those needs. In response to the President's direction, as Mr. Kane described, we have recently established the Department of Homeland Security/Department of Energy aviation security enhancement partnership as an under secretary-level governance mechanism for managing the partnership between DHS and DOE National laboratories to advanced technical solutions to key aviation security problems.

Now, partnering with the National laboratories is not new for us. Since its inception DHS has worked in close collaboration with the DOE National laboratories in pursuit of technology supporting the operational needs of DHS, but this particular partnership is unique in its focus and will allow us to extend and leverage this long-standing relationship to accelerate the delivery of key advanced aviation security technologies and knowledge.

DHS S&T also plays an important role in the test and evaluation of equipment in advance of major acquisition decisions. S&T's director of test and evaluation standards approves the test and evaluation master plans that describe the necessary developmental and operational testing that must be conducted in order to determine system technical performance and operational effectiveness and suitability throughout the development process.

The director of operational test and evaluation is responsible for reviewing and approving the operational test plan for each major DHS acquisition program and providing independent assessments to the DHS acquisition review board prior to major acquisition decisions.

As Mr. Kane said, for aviation security technologies, the actual testing is led by TSL, the Transportation Security Laboratory in Atlantic City. TSL conducts independent verification and validation tests, including certification tests, qualification tests, and laboratory assessments, depending on the maturity of the type of the detection equipment.

I am delighted to have alongside me today Dr. Susan Hallowell, director of TSL, to whom I will promptly refer all of your difficult questions.

Ladies and gentlemen, aviation security is clearly an endeavor of global importance, and success will require the full involvement of the Homeland Security research enterprise, Government, academia, the private sector, and our international partners. In addition to the DHS-DOE aviation security enhancement partnership, we are also utilizing our intra-Government partnership with DOD to ensure that we are fully utilizing their research investments as we pursue capabilities to keep the traveling public safe.

Academia is a critical partner in long-term research and development of the science and technology workforce that America will need to maintain its security. Our university-based centers of excellence are leading long-term efforts to ensure we are keeping the technology pipeline full.

The December 25 event made it clear that terrorism knows no borders. Similarly, the directorate continues to look to the international community for technologies and techniques critical to bolstering aviation security, and I am personally engaged with the 10 countries with which we have formal bilateral S&T agreements to

ensure we have identified the most promising aviation security technologies and techniques around the globe.

Finally, I am acutely aware that American innovation also resides outside of the Federal Government. That is why we are fully engaged with the private sector to ensure we are hearing their technological ideas across a broad range of mission areas that we support, including aviation security.

Members, thank you for your dedicated efforts to improve the safety of air travel for all Americans, and I appreciate the opportunity to be here and look forward to your questions.

[The joint statement of Mr. Buswell and Ms. Hallowell follows:]

JOINT PREPARED STATEMENT OF BRADLEY I. BUSWELL AND SUSAN HALLOWELL

MARCH 17, 2010

INTRODUCTION

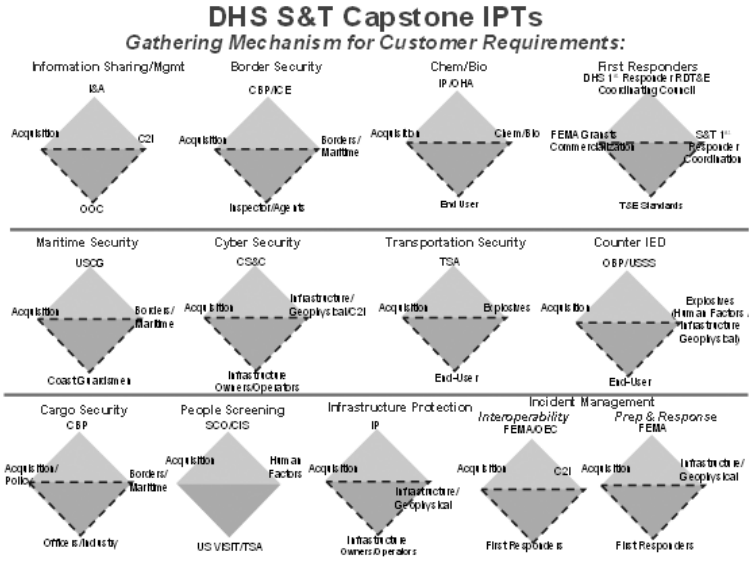
Good afternoon, Chairwoman Jackson Lee, Congressman Dent, and distinguished Members of the subcommittee. I am honored to appear before you today on behalf of the Department of Homeland Security (DHS) to report on the Science and Technology Directorate's (S&T) research, development, test, and evaluation (RDT&E) efforts relating to airport passenger screening technology.

Passenger Screening Capability Development

S&T has a variety of roles in the Department. S&T provides technical support and tools to the major DHS operating components and the Nation's first responders; funds basic research and technology development; and supports the Department's major acquisitions through testing, evaluation, and the development of standards.

The Transportation Security Administration (TSA) protects the Nation's transportation systems to ensure freedom of movement for people and commerce. While TSA has the lead role in defining the performance of airport security equipment, S&T and TSA coordinate closely on research efforts and equipment test and evaluation to advance capabilities that best protect the traveling public. These efforts have yielded numerous technical improvements that enhance the effectiveness of screening techniques and technologies while moving increasing numbers of people more quickly through security.

The Department's research and development priorities are primarily customer-driven through our Capstone Integrated Product Team (IPT) process. DHS customers—such as TSA—chair the Capstone IPTs and establish their desired capability priorities based on their assessment of risk in their respective mission areas. Three IPTs—Transportation Security, Counter Improvised Explosive Devices (C-IED), and People Screening—are dedicated to identifying and delivering technological solutions for detecting and countering threats to the safety and security of the traveling public. Our Transportation Security IPT, led by TSA with support from S&T's Explosives Division, strives to identify and deliver technologies to improve our layered approach to aviation security. TSA is also an integral member of the People Screening IPT, providing valuable input as a user of proposed screening technologies. Finally, the Counter-IED IPT works to identify and develop trace detection and standoff imaging technologies that will impact the next generation of checkpoint technologies.



All three DHS S&T portfolios—Product Transition, Innovation/Homeland Security Advanced Research Projects Agency (HSARPA), and Basic Research—participate in the IPT process. While the IPT members drive the selection of Product Transition projects, the expressed needs that arise from this process also inform the selection of projects in our Basic Research portfolio and similarly inform the higher-risk/high pay-off initiatives undertaken by our Innovation/HSARPA portfolio. The more insight we gain regarding current and future threats and the capability gaps of our stakeholders, the better positioned we are to identify promising areas of research and explore innovative solutions that are outside the development time frame for the nearer term-focused Product Transition portfolio.

In addition to the Capstone IPT process, we have recently established the DHS—Department of Energy (DOE) Aviation Security Enhancement Partnership to advance technical solutions to key aviation security problems in support of priorities announced by the President following the failed December 25 bombing attempt. While DHS has always worked in close collaboration with the DOE National Laboratories, this new partnership allows an unprecedented level of access between the research community and operators that conduct aviation security efforts in DOE, DHS, and TSA. We have now agreed to create a senior-level (at the Under Secretary level) governance mechanism to manage ways to extend and leverage this relationship with a focus on improving aviation security by:

- Delivering key advanced aviation security technologies and knowledge;
- Conducting analyses to assess possible vulnerabilities and threats and support/inform technology requirements, policy, planning, decision-making activities; and
- Reviewing the use of existing aviation security technologies and screening procedures, and the impact of new or improved technologies using a systems analysis approach to illuminate gaps, opportunities, and cost-effective investments.

Research and Development Priorities

There is no single technological solution to aviation security. A layered security approach to passenger screening features multiple passenger and baggage screening tools and integrates human factors considerations, metal detectors, Advanced Imaging Technology (AIT) with X-rays and millimeter waves, trace explosives detection, and canines. S&T's R&D Program is focused on improving the performance of currently deployed screening equipment and procedures in the near-term, and developing and deploying new technologies and procedures in the long-term. Future improvements aim to screen passengers and carry-on baggage for an increasing range of threats and streamline travel by easing certain restrictions, such as the need to remove shoes during screening or limits on carrying liquids onto the plane.

We develop technologies and techniques that maximize DHS and other end users' operational flexibility as well as ensure the privacy, civil rights, and civil liberties of our citizens are protected. Our screening research programs are developed and executed in close cooperation with the DHS Chief Privacy Officer as well as the Office of Civil Rights and Civil Liberties to ensure that we consciously consider and address their impacts or risk to the public. S&T conducts in-depth analyses of such efforts through on-going dialogue with the DHS Privacy Office and the DHS Office of Civil Rights and Civil Liberties and related documentation such as Privacy Impact Assessments or Civil Liberties Impact Assessments.

We continuously evaluate and improve the capabilities of currently deployed technologies against new threats and seek to develop state-of-the-art threat detection technology for TSA passenger checkpoints to screen out evolving threats while improving the passenger experience with higher throughput and minimal restrictions. The highest-priority effort in this area is improving detection software algorithms, including effective automatic target recognition, in our currently deployed imaging systems, particularly AIT and Advanced Technology (AT) X-ray screening devices. AIT is one of the most promising technologies for detecting non-metallic weapons and small quantities of explosives concealed on individuals. AT X-ray provides an enhanced detection capability with multi-dimensional visual screening and improved image resolution of carry-on bags. Both of these technologies would greatly benefit from algorithm improvement and other systems research and engineering approaches that consider human factors to optimize security officer performance in threat detection and identification.

Efforts dedicated to suspicious behavior detection could also provide near-term benefit in passenger screening. The Suspicious Behavior Detection Program strives to improve screening by providing a science-based capability to identify unknown threats indicated by deceptive and suspicious behavior. This program addresses operational needs for real-time, non-invasive detection of deception or hostile intent that are applicable across the DHS mission. In the longer term, a continuing, robust RDT&E program across the three S&T portfolios is necessary.

The Explosives Research Program funds multidisciplinary basic research in imaging, particle physics, chemistry, material science and advanced algorithm development to develop enhanced explosive detection and mitigation capabilities.

The transition program, guided by the Capstone IPT process, is comprehensive and encompasses:

- Automated imaging systems to screen for weapons, conventional explosives, and home-made explosives (HME) in carry-on bags;
- Trace explosives detection capabilities for identifying explosives on people and in carry-on baggage;
- A next generation fully automated checkpoint for detecting weapons and explosives on people for aviation, mass transit, public gathering venues, or other potentially high-risk buildings;
- Human performance research and technology development for increased security officer efficiency and effectiveness;
- A science-based capability to derive, validate, and automate detection of observable indicators of suicide bombers;
- A science-based capability to identify known threats and facilitate legitimate travel through accurate, timely, and easy-to-use tools for biometric identification and credential validation;
- Technologies and methods for identifying insider threats.

The innovation program, managed by HSARPA, is looking at "leap-ahead" technologies such as:

- Future Attribute Screening Technology (FAST) to determine if it is possible to detect malintent (the mental state of individuals intending to cause harm) by utilizing non-invasive physiological and behavioral sensor technology, deception theory, and observational techniques. Though we have established an initial scientific basis for the technology, this project is still in the early stages as we work on both the science and theory to support the concept.
- MagViz is looking at the possibility of using technology similar to hospital MRI machines to look for and identify liquids. The magnetic fields in MagViz are much lower power than its medical counterparts, allowing operation without the restrictions and high costs of traditional MRI. We demonstrated this technology with a small-scale prototype at the Sunport Airport in Albuquerque, NM, in December 2008. MagViz was successful at identifying a dangerous liquid in a small bottle among many non-hazardous liquids in a standard TSA checkpoint bowl. The project is still in the research phase, and we are now trying to prove the technology using a larger-size container and a broader array of both non-hazardous and potentially hazardous liquids.

S&T Role in Test & Evaluation

Section 302 of the Homeland Security Act of 2002 charges S&T with the responsibility for "coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department." To carry out these and other test and evaluation (T&E)-related legislative mandates, the Directorate established the Test and Evaluation and Standards Division (TSD) in 2006 and created the position of Director of Operational Test & Evaluation in 2008.

TSD develops and implements robust Department-wide T&E policies and procedures. Working with the DHS under secretary for management, TSD approves Test and Evaluation Master Plans (TEMP) that describe the necessary Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) tasks that must be conducted in order to determine system technical performance and operational effectiveness based upon vetted Operational Requirements Documents.

Many of the Department's airport security technologies begin testing at the Transportation Security Laboratory (TSL). Test and evaluations activities at the TSL encompass two independent functions and complies with the robust Department-wide T&E policies and procedures. First, the Independent Test and Evaluation (IT&E) function is responsible for evaluating mature technology that may meet TSA's security requirements and is suitable for piloting or deployment. Second, the research and development function has responsibilities ranging from applied research to prototype development to technology maturation that produces prototypes suitable for evaluation by the IT&E Team. I am joined today by the TSL Director, Susan Hallowell.

The IT&E group works closely with TSA's Office of Security and Technology to determine testing requirements, priorities, and results of evaluations. At TSL, IT&E activities, which include certification, qualification, and assessment testing, are generally performed to determine if detection systems meet TSA-defined requirements. Results help define key program milestones, benchmarking, and investment strategy as well as support decisions of DHS operating components (such as TSA) for field trials, production, or deployment. RDT&E activities are designed to verify that a prototype or near-commercial off-the-shelf system has met performance metrics established within the R&D program such that it can proceed to the next R&D stage.

The *Certification Test* Program is reserved for detection testing of bulk and trace explosives detection systems (EDS) and equipment under statutory authority 49 U.S.C. § 44913 for checked baggage. Before mature EDS are deployed, it must be certified that salient performance characteristics are met.

Qualification Tests are designed to verify that a security system meets requirements as specified in a TSA-initiated Technical Requirements Document. This test, along with piloting (field trials), generally results in a determination of fitness-for-use. This process is modeled after the certification process and is defined within the Qualification Management Plan. Unlike the Certification Test, the requirements of the Qualification Management Plan typically expand beyond detection functions to include operational requirements. The result of Qualification Testing is a recommendation of whether candidate systems should be placed on a Qualified Products List.

Laboratory Assessment Testing is conducted to determine the general capability of a system. These evaluations of candidate security systems are carried out in accordance with interim performance metrics, and the results drive future development efforts or operational deployment evaluations. While the IT&E group practices best scientific principles in test design, execution, and evaluation of data, assessment criteria are determined by the DHS component's needs.

Developmental Test and Evaluation is performed by the R&D team at the TSL and involves testing in a controlled environment to ensure that all system or product components meet technical specifications. These tests are designed to ensure that developmental products have met major milestones identified within the R&D project and DT&E testing at the TSL assesses the strengths, weaknesses, and vulnerabilities of technologies as they mature and gain capability. The primary focus is to ensure that the technology is robust and ready for Certification or Qualification tests.

Following completion of the IT&E, an Operational Test Readiness is conducted to determine whether the certified or qualified systems are ready for operational testing. OT&E for systems occurs in several airports, by trained TSA operators using test plans that are approved by S&T's Director of Operational T&E. Testing in an operationally accurate environment identifies issues in system operations before deployment is contemplated.

TSD currently provides oversight to major acquisition programs, including TSA programs, by: Participating in T&E working groups; approving TEMPs, and Oper-

ational Test Plans; participating in Operational Test Readiness Reviews; observing testing; and participating in Acquisition Review Boards.

Public and Private Sector Engagement

To maximize the effectiveness of our resources and leverage the scientific work being done in both the public and private sectors, we have made concerted efforts to form partnerships throughout the Government and across the academic, business, and international communities. In addition to the DHS-DOE Aviation Security Enhancement Partnership, we are also utilizing our intra-government partnership with Department of Defense (DOD) in the form of the Capability Development Working Group (CDWG). Co-chaired by the DHS Under Secretaries for S&T and Management, as well as the Under Secretary of Defense for Acquisition, Technology, and Logistics, the CDWG will ensure that investments in explosive detection made by DOD are considered as we pursue capabilities to keep the traveling public safe. Academia is a critical partner in long-term research and the development of the science and technology workforce that America will need to maintain its security. Our university-based Centers of Excellence (COE) are conducting or have finished approximately 500 research projects. Efforts relevant to transportation security are underway at our explosives research COE at Northeastern University, our BORDERS COE at the University of Arizona, and, of course the seven-institution National Transportation Security COE. These COEs are leading long-term efforts, such as developing advanced technologies for detecting a variety of explosive precursors and mixtures; conducting scientific research related to next-generation screening techniques; and research to give us fundamental understanding of other counter-explosive technologies.

The failed December 25 bombing attempt made it clear that terrorism respects no borders. Similarly, S&T continues to look to the international community for technologies and techniques critical to bolstering aviation security. I am personally engaged with the ten countries with which we have formal bilateral S&T agreements—Australia, Canada, France, Germany, Great Britain, Israel, Mexico, New Zealand, Singapore, and Sweden—to ensure that we have identified the most promising aviation security technologies and techniques around the globe.

Finally, in order to leverage the innovation that resides outside the Federal Government, we have a standing Broad Agency Announcement (BAA 09–05) that provides a means for the private sector to submit its technological ideas for consideration across the broad range of mission areas that we support, including aviation security.

CONCLUSION

Thank you for your dedicated efforts to improve the safety of air travel for all Americans. I appreciate the opportunity to meet with you today to discuss research initiatives to strengthen passenger screening. I look forward to answering your questions.

Ms. JACKSON LEE. Thank you very much for your testimony.

I now recognize Mr. Lord to summarize his statement for 5 minutes.

STATEMENT OF STEPHEN LORD, DIRECTOR, HOMELAND SECURITY AND JUSTICE TEAM, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. LORD. Thank you, Madam Chairwoman, Chairman Thompson.

I am pleased to be here again today to discuss recent steps TSA has taken to enhance aviation security, including efforts to deploy advanced imaging technology, or AIT. In response to the attempted Christmas day attack, TSA has significantly revised its strategy for deploying AIT, formerly referred to as whole body imagers.

First, TSA now plans to deploy 1,800 units by 2014, a more than two-fold increase from the initial plan buy of 878 units.

Second, TSA now plans to use this technology as the primary rather than secondary screening measure. For the purposes of this testimony, I think it is important to note that DHS' S&T and TSA

share responsibilities related to research and development of AIT and other important checkpoint screening technologies.

As highlighted in our October 2009 report, some coordination challenges existed because of poor communication between the S&T and TSA. However, several steps were taken to address this issue, and I am hoping today's hearing can help clarify the extent those issues have been resolved.

Our October 2009 report also highlighted several challenges that TSA faced in deploying advanced technology, specifically the so-called explosive trace portals, or puffers, which I believe is a cautionary tale for the AIT acquisition. We found that TSA had deployed over 100 puffers without fully testing them in an operational environment. As a result the technology did not perform as expected, and TSA had to curtail their deployment.

The good news is TSA officials concurred with our report recommendations to improve this process and stated that unlike the puffers, operational testing for the AIT was successfully completed. However, it is still unclear to GAO whether the AIT would have detected the weapon used in the attempted Christmas day attack, based on the preliminary information we have reviewed to date.

We are currently reviewing TSA testing results to first assess the AIT's detection capabilities and second to verify that TSA successfully completed operational testing of this technology. Also, while TSA has completed a life-cycle cost estimate and a so-called alternatives analysis for the AIT, it has not conducted a full cost-benefit study as called for in our October 2009 report.

While we recognize and appreciate that TSA has taken some immediate steps to address the vulnerability exposed by the Christmas day attack, we still believe a cost-benefit analysis is important, as it would help TSA identify the total cost of the deployment and how security is enhanced through this deployment relative to other checkpoint technologies. Again, this information is especially important, since TSA is proposing to more than double the number of AITs to be deployed.

We estimate that the staffing costs alone associated with the planned increase in AITs from 878 units to 1,800 units could add up to $2.4 billion in additional costs over the project life-cycle. Moreover, the total staff cost for the 1,800 units could range as high as $4.7 billion. These costs were not reflected in TSA's most recent February 2010 life-cycle cost estimate.

While a lot of recent attention has been focused on passenger checkpoint technology, and AIT in particular, I think it is important to also be mindful of the other components of aviation security. That includes policies and procedures and the staff you have implementing these procedures.

Also, the checkpoint technology represents only one layer of many layers of aviation security. Other layers involve air cargo, the screening of air cargo on passenger aircraft, airport perimeters, the so-called behavior detection officers. So when addressing aviation security issues, you have to keep this full context in mind in reaching any conclusions.

In closing, I look forward to participating in today's hearing and hope it can help answer three important oversight questions. First, how effectively will the AIT detect those seeking to replicate the

Christmas day attack? Second, do the security benefits of AIT outweigh its cost? That is when you include all relevant costs. Finally, how does the new AIT deployment plan fit into TSA's broader passenger checkpoint screening strategy and suite of technologies being deployed at the checkpoint? As Robin mentioned, TSA is in the process of fielding a number of highly sophisticated technologies.

Madam Chairwoman, that concludes my statement. Once again, I look forward to answering your questions.

[The statement of Mr. Lord follows:]

PREPARED STATEMENT OF STEPHEN LORD

MARCH 17, 2010

GAO HIGHLIGHTS

Highlights of GAO–10–484T, a testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

The attempted bombing of Northwest Flight 253 highlighted the importance of detecting improvised explosive devices on passengers. This testimony focuses on: (1) The Transportation Security Administration's (TSA) efforts to procure and deploy advanced imaging technology (AIT), and related challenges; and (2) TSA's efforts to strengthen screening procedures and technology in other areas of aviation security, and related challenges. This testimony is based on related products GAO issued from March 2009 through January 2010, selected updates conducted from December 2009 through March 2010 on the AIT procurement, and on-going work on air cargo security. For the on-going work and updates, GAO obtained information from the Department of Homeland Security (DHS) and TSA and interviewed senior TSA officials regarding air cargo security and the procurement, deployment, operational testing, and assessment of costs and benefits of the AIT.

What GAO Recommends

GAO is not making new recommendations. In past reports, GAO has recommended, among other things, that TSA operationally test screening technologies prior to deployment and assess costs and benefits of screening technology investments. DHS concurred and is working to address the recommendations. DHS provided comments to this statement, which were incorporated.

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

What GAO Found

In response to the December 25, 2009, attempted attack on Northwest Flight 253, TSA revised the AIT procurement and deployment strategy, increasing the planned deployment of AITs from 878 to 1,800 units and using AITs as a primary—instead of a secondary—screening measure where feasible; however, challenges remain. In October 2009, GAO reported on the challenges TSA faced deploying new technologies such as the explosives trace portal (ETP) without fully testing them in an operational environment, and recommended such testing prior to future deployments. TSA officials concurred and stated that, unlike the ETP, operational testing for the AIT was successfully completed late in 2009 before its deployment was fully initiated. While officials said AITs performed as well as physical pat-downs in operational tests, it remains unclear whether the AIT would have detected the weapon used in the December 2009 incident based on the preliminary information GAO has received. GAO is verifying that TSA successfully completed operational testing of the AIT. In October 2009, GAO also recommended that TSA complete cost-benefit analyses for new passenger screening technologies. While TSA conducted a life-cycle cost estimate and an alternatives analysis for the AIT, it reported that it has not conducted a cost-benefit analysis of the original deployment strategy or the revised AIT deployment strategy, which proposes a more than two-fold increase in the number of machines to be procured. GAO estimates increases in staffing costs alone due to doubling the number of AITs that TSA plans to deploy could add up to $2.4 bil-

lion over its expected service life. While GAO recognizes that TSA is attempting to address a vulnerability exposed by the December 2009 attempted attack, a cost-benefit analysis is important as it would help inform TSA's judgment about the optimal deployment strategy for the AITs, and how best to address this vulnerability considering all elements of the screening system.

TSA has also taken actions towards strengthening other areas of aviation security but continues to face challenges. For example, TSA has taken steps to meet the statutory mandate to screen 100 percent of air cargo transported on passenger aircraft by August 2010, including developing a program to share screening responsibilities across the air cargo supply chain. However, as GAO reported in March 2009, a number of challenges to this effort exist, including attracting participants to the TSA screening program, completing technology assessments, and overseeing additional entities that it expects to participate in the program. GAO is exploring these issues as part of an on-going review of TSA's air cargo security program which GAO plans to issue later this year. Further, while TSA has taken a variety of actions to strengthen the security of commercial airports, GAO reported in September 2009 that TSA continues to face challenges in several areas, such as assessing risk and evaluating worker screening methods. In September 2009, GAO also recommended that TSA develop a National strategy to guide stakeholder efforts to strengthen airport perimeter and access control security, to which DHS concurred.

Madam Chairwoman and Members of the subcommittee, I am pleased to be here today to discuss the Transportation Security Administration's (TSA) progress in securing passenger checkpoints and other areas of commercial aviation. In response to the December 25, 2009, attempted bombing of Northwest Flight 253, the Secretary of Homeland Security announced five corrective actions to improve aviation security, including accelerating deployment of the advanced imaging technology (AIT)—formerly called the Whole Body Imager—to identify materials such as those used in the attempted Christmas day bombing. The AITs produce an image of a passenger's body that TSA personnel use to look for anomalies, such as explosives. TSA is deploying AITs to airport passenger checkpoints to enhance its ability to detect explosive devices and other prohibited items on passengers. Passengers undergo either primary or secondary screening at these checkpoints. Primary screening is conducted on all airline passengers before they enter the sterile area of an airport and involves passengers walking through a metal detector and their carry-on items being subjected to X-ray screening.[1] Secondary screening is conducted on selected passengers and involves additional screening of bboth passengers and their carry-on items. While screening passengers at the checkpoint is a vital layer of security, it is also important to ensure the security of other areas of commercial aviation, such as air cargo transported on passenger aircraft, and airport worker screening and checked baggage screening.

TSA's passenger checkpoint screening system comprises three elements: (1) Personnel responsible for, among other things, screening passengers and baggage; (2) the policies and procedures that govern the different aviation security programs; and (3) the technology used to screen passengers and baggage. All three elements—people, process, and technology—collectively help determine the effectiveness and efficiency of passenger checkpoint screening, and our past work in this area has addressed all three elements of the system.[2] Similarly, securing the flying public involves trade-offs between security, privacy, and the efficient flow of commerce. Striking the right balance between these three goals is an on-going challenge facing TSA.

My testimony today focuses on: (1) TSA's plans to procure, deploy, and test AITs to enhance the security of the passenger checkpoint, and any challenges TSA faces in this effort; and (2) TSA's efforts to strengthen screening procedures and tech-

---

[1] Sterile areas are areas of airports where passengers wait after screening to board departing aircraft.

[2] See for example, GAO, *Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security,* GAO–10–401T (Washington, DC: Jan. 27, 2010); *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges,* GAO–10–128 (Washington, DC: Oct. 7, 2009); *Homeland Security: DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity,* GAO–10–106 (Washington, DC: Dec. 2, 2009); *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks,* GAO–09–292 (Washington, DC: May 13, 2009); *Aviation Security: Preliminary Observations on TSA's Progress and Challenges in Meeting the Statutory Mandate for Screening Air Cargo on Passenger Aircraft,* GAO–09–422T (Washington, DC: Mar. 18, 2009); *Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process,* GAO–08–48T (Washington, DC: Nov. 15, 2007); and *Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List,* GAO–08–110 (Washington, DC: Oct. 11, 2007).

nology in other areas of aviation security, and any related challenges the agency faces in these areas.

This statement is based on related GAO reports and testimonies we issued from March 2009 through January 2010, as well as preliminary observations based on on-going work—from October 2008 through February 2010—to be completed later this year assessing the progress that DHS and its component agencies have made in addressing challenges related to air cargo security.[3] To conduct all of this work, we reviewed relevant documents related to the programs reviewed, and interviewed cognizant Department of Homeland Security (DHS) and TSA officials. All of this work was conducted in accordance with generally accepted government auditing standards, and our previously published reports contain additional details on the scope and methodology for those reviews. In addition, this statement contains selected updates conducted from December 2009 through March 2010 on TSA's effort to procure and deploy the AIT. For the updates, we obtained information from DHS and TSA on the AIT and interviewed senior TSA officials regarding the planned procurement, deployment, operational testing and evaluation, and assessment of benefits and costs of the AITs. We conducted these updates in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

BACKGROUND

Airline Passenger Screening Using Checkpoint Technology

Passenger screening is a process by which screeners inspect individuals and their property to deter and prevent an act of violence or air piracy, such as the carrying of any unauthorized explosive, incendiary, weapon, or other prohibited item on board an aircraft or into a sterile area. Screeners inspect individuals for prohibited items at designated screening locations. TSA developed standard operating procedures for screening passengers at airport checkpoints. Primary screening is conducted on all airline passengers before they enter the sterile area of an airport and involves passengers walking through a metal detector, and carry-on items being subjected to X-ray screening. Passengers who alarm the walk-through metal detector or are designated as selectees—that is, passengers selected for additional screening—must then undergo secondary screening, as well as passengers whose carry-on items have been identified by the X-ray machine as potentially containing prohibited items. Secondary screening involves additional means for screening passengers, such as by hand wand; physical pat-down; or other screening methods such as the AIT.

Role of DHS Science & Technology Directorate

Within DHS, both the Science and Technology Directorate (S&T) and TSA have responsibilities for researching, developing, and testing and evaluating new technologies, including airport checkpoint screening technologies. Specifically, S&T is responsible for the basic and applied research and advanced development of new technologies, while TSA, through its Passenger Screening Program (PSP), identifies the need for new checkpoint screening technologies and provides input to S&T during the research and development of new technologies, which TSA then procures and deploys. Because S&T and TSA share responsibilities related to the research, development, test, and evaluation (RDT&E), procurement, and deployment of checkpoint screening technologies, the two organizations must coordinate with each other and external stakeholders, such as airport operators and technology vendors.

Air Cargo Security

Air cargo can be shipped in various forms, including unit load devices (ULD) that allow many packages to be consolidated into one container or pallet; wooden crates; or individually wrapped/boxed pieces, known as loose or break-bulk cargo. Participants in the air cargo shipping process include shippers, such as manufacturers; freight forwarders, who consolidate cargo from shippers and take it to air carriers for transport; air cargo handling agents, who process and load cargo onto aircraft on behalf of air carriers; and air carriers that load and transport cargo.[4] TSA's responsibilities include, among other things, establishing security requirements gov-

[3] GAO–10–401T; GAO–10–128; GAO–10–106; and GAO–09–422T.

[4] For purposes of this statement, the term freight forwarders only includes those freight forwarders that are regulated by TSA, also referred to as indirect air carriers.

erning domestic and foreign passenger air carriers that transport cargo and domestic freight forwarders.

Airport Perimeter Security and Access Control

Airport perimeter and access control security is intended to prevent unauthorized access into secured airport areas, either from outside the airport complex or from within. Airport operators generally have direct day-to-day responsibility for maintaining and improving perimeter and access control security, as well as implementing measures to reduce worker risk. However, TSA has primary responsibility for establishing and implementing measures to improve security operations at U.S. commercial airports—that is, TSA-regulated airports—including overseeing airport operator efforts to maintain perimeter and access control security.[5] Airport workers may access sterile areas through TSA security checkpoints or through other access points that are secured by the airport operator. The airport operator is also responsible, in accordance with its security program, for securing access to secured airport areas where passengers are not permitted. Airport methods used to control access vary, but all access controls must meet minimum performance standards in accordance with TSA requirements.

INCREASED DEPLOYMENT OF AIT HIGHLIGHTS THE IMPORTANCE OF OPERATIONAL TESTING AND COST-BENEFIT ANALYSIS PRIOR TO DEPLOYMENT

TSA Plans to Procure and Deploy 1,800 AITs by 2014 and Use Them as a Primary Screening Measure

In response to the December 2009 attempted terrorist attack, TSA has revised its procurement and deployment strategy for the AIT, increasing the number of AITs it plans to procure and deploy. In contrast with its prior strategy, the agency now plans to acquire and deploy 1,800 AITs (instead of the 878 units it had previously planned to acquire) and to use them as a primary screening measure where feasible rather than solely as a secondary screening measure. According to a senior TSA official, the agency is taking these actions in response to the Christmas day 2009 terrorist incident. These officials stated that they anticipate the AIT will provide enhanced security benefits compared to walk-through metal detectors, such as enhanced detection capabilities for identifying nonmetallic threat objects and liquids. TSA officials also stated that the AIT offers greater efficiencies because it allows TSA to more rigorously screen a greater number of passengers in a shorter amount of time while providing a detection capability equivalent to a pat-down. For example, the AIT requires about 20 seconds to produce and interpret a passenger's image as compared with 2 minutes required for a physical pat-down. A senior official also stated that TSA intends to continue to offer an alternative but comparable screening method, such as a physical pat-down, for passengers who prefer not to be screened using the AIT.

The AIT produces an image of a passenger's body that a screener interprets. The image identifies objects, or anomalies, on the outside of the physical body but does not reveal items beneath the surface of the skin, such as implants. TSA plans to procure two types of AIT units: one type uses millimeter-wave and the other type uses backscatter X-ray technology. Millimeter-wave technology beams millimeter-wave radio-frequency energy over the body's surface at high speed from two antennas simultaneously as they rotate around the body. The energy reflected back from the body or other objects on the body is used to construct a three-dimensional image. Millimeter wave technology produces an image that resembles a fuzzy photo negative. Backscatter X-ray technology uses a low-level X-ray to create a two-sided image of the person. Backscatter technology produces an image that resembles a chalk etching.

As of February 24, 2010, according to a senior TSA official, the agency has deployed 40 of the millimeter-wave AITs and procured 150 backscatter X-ray units in fiscal year 2009. In early March 2010, TSA initiated the deployment of these backscatter units starting with two airports, Logan International Airport in Boston, Massachusetts, and Chicago O'Hare International Airport in Des Plaines, Illinois. TSA officials stated that they do not expect these units to be fully operational, however, until the second or third week of March due to time needed to hire and train additional personnel. TSA estimates that the remaining backscatter X-ray units will be installed at airports by the end of calendar year 2010. In addition, TSA plans to procure an additional 300 AIT units in fiscal year 2010, some of which it plans to purchase with funds from the American Recovery and Reinvestment Act of 2009.

[5] See generally Aviation and Transportation Security Act, Pub. L. No. 107–71, 115 Stat. 597 (2001).

In fiscal year 2011, TSA plans to procure 503 AIT units. TSA projects that a total of about 1,000 AIT systems will be deployed to airports by the end of December 2011. In fiscal year 2014 TSA plans to reach full operating capacity, having procured a total of 1,800 units and deployed them to 60 percent of the checkpoint lanes at Category X, I, and II airports.[6] The current projected full operating capacity of 1,800 machines represents a more than two-fold increase from 878 units that TSA had previously planned. TSA officials stated that the cost of the AIT is about $170,000 per unit, excluding training, installation, and maintenance costs. In addition, in the fiscal year 2011 President's budget submission, TSA has requested $218.9 million for 3,550 additional full-time equivalents (FTE) to help staff the AITs deployed in that time frame. From 2012 through 2014, as TSA deploys additional units to reach full operating capacity, additional staff will be needed to operate these units; such staffing costs will recur on an annual basis. TSA officials told us that three FTEs are needed to operate each unit.

Because the AIT presents a full body image of a person during the screening process, concerns have been expressed that the image is an invasion of privacy. According to TSA, to protect passenger privacy and ensure anonymity, strict privacy safeguards are built into the procedures for use of the AIT. For example, the officer who assists the passenger does not see the image that the technology produces, and the officer who views the image is remotely located in a secure resolution room and does not see the passenger. Officers evaluating images are not permitted to take cameras, cell phones, or photo-enabled devices into the resolution room. To further protect passengers' privacy, ways have been introduced to blur the passengers' images. The millimeter-wave technology blurs all facial features, and the backscatter X-ray technology has an algorithm applied to the entire image to protect privacy. Further, TSA has stated that the AIT's capability to store, print, transmit, or save the image will be disabled at the factory before the machines are delivered to airports, and each image is automatically deleted from the system after it is cleared by the remotely located security officer. Once the remotely located officer determines that threat items are not present, that officer communicates wirelessly to the officer assisting the passenger. The passenger may then continue through the security process. Potential threat items are resolved through a directed physical pat-down before the passenger is cleared to enter the sterile area.[7] In addition to privacy concerns, the AITs are large machines, and adding them to the checkpoint areas will require additional space, especially since the operators are physically segregated from the checkpoint to help ensure passenger privacy. Adding a significant number of additional AITs to the existing airport infrastructure could impose additional challenges on airport operators.

TSA Recently Reported Efforts to Strengthen Its Operational Test and Evaluation Process, But It Is Not Clear Whether TSA Has Fully Evaluated the Relative Security Benefits and Costs of the AIT

In October 2009, we reported that TSA had relied on a screening technology in day-to-day airport operations that had not been proven to meet its functional requirements through operational testing and evaluation, contrary to TSA's acquisition guidance and a knowledge-based acquisition approach.[8] We also reported that TSA had not operationally tested the AITs at the time of our review, and we recommended that TSA operationally test and evaluate technologies prior to deploying them.[9] In commenting on our report, TSA agreed with this recommendation. Although TSA does not yet have a written policy requiring operational testing prior to deployment, a senior TSA official stated that TSA has made efforts to strengthen its operational test and evaluation process and that TSA is now complying with DHS's current acquisition directive that requires operational testing and evaluation

---

[6] There are about 450 commercial airports in the United States. TSA classifies airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the total number of takeoffs and landings annually, the extent to which passengers are screened at the airport, and other special security considerations. In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest.

[7] TSA stated that it continues to evaluate possible display options that include a "stick figure" or "cartoon-like" form to provide greater privacy protection to the individual being screened while still allowing the unit operator or automated detection algorithms to detect possible threats. DHS is working directly with technology providers to develop advanced screening algorithms for the AIT that would utilize Automatic Target Recognition to identify and highlight possible threats.

[8] *http://www.gao.gov/products/GAO-10-128*.

[9] Operational testing refers to testing in an operational environment in order to verify that new systems are operationally effective, supportable, and suitable.

be completed prior to deployment.[10] According to officials, TSA is now requiring that AIT are to successfully complete both laboratory tests and operational tests prior to deployment.

As we previously reported, TSA's experience with the explosives trace portal (ETP), or "puffers," demonstrates the importance of testing and evaluation in an operational environment.[11] The ETP detects traces of explosives on a passenger by using puffs of air to dislodge particles from the passenger's body and clothing that the machine analyzes for traces of explosives. TSA procured 207 ETPs and in 2006 deployed 101 ETPs to 36 airports, the first deployment of a checkpoint technology initiated by the agency.[12] TSA deployed the ETPs even though tests conducted during 2004 and 2005 on earlier ETP models suggested that they did not demonstrate reliable performance. Furthermore, the ETP models that were subsequently deployed were not tested to prove their effective performance in an operational environment, contrary to TSA's acquisition guidance, which recommends such testing. As a result, TSA procured and deployed ETPs without assurance that they would perform as intended in an operational environment. TSA officials stated that they deployed the machines without resolving these issues to respond quickly to the threat of suicide bombers. In June 2006 TSA halted further deployment of the ETP because of performance, maintenance, and installation issues. According to a senior TSA official, as of December 31, 2009, all but 9 ETPs have been withdrawn from airports, and 18 ETPs remain in inventory.

Following the completion of our review, TSA officials told us that the AIT successfully completed operational testing at the end of calendar year 2009 before its deployment was fully initiated. The official also stated that the AIT test results were provided and reviewed by DHS's Acquisition Review Board prior to the board approving the AIT deployment. According to TSA's threat assessment, terrorists have various techniques for concealing explosives on their persons, as was evident in Mr. Abdulmutallab's attempted attack on December 25, when he concealed an explosive in his underwear. While TSA officials stated that the laboratory and operational testing of the AIT included placing explosive material in different locations on the body,[13] it remains unclear whether the AIT would have been able to detect the weapon Mr. Abdulmutallab used in his attempted attack based on the preliminary TSA information we have received. We are in the process of reviewing these operational tests to assess the AIT's detection capabilities and to verify that TSA successfully completed operational testing of the AIT.

In addition, while TSA officials stated that the AITs performed as well as physical pat-downs in operational testing, TSA officials also reported they have not conducted a cost-benefit analysis of the original or revised AIT deployment strategy. We reported in October 2009 that TSA had not conducted a cost-benefit analysis of checkpoint technologies being researched and developed, procured, and deployed and recommended that it do so. DHS concurred with our recommendation. Cost-benefit analyses are important because they help decision makers determine which protective measures, for instance, investments in technologies or in other security programs, will provide the greatest mitigation of risk for the resources that are available. TSA officials stated that a cost-benefit analysis was not completed for the AIT because one is not required under DHS acquisition guidance. However, these officials reported that they had completed, earlier in the program, a life-cycle cost estimate and an analysis of alternatives for the AIT as required by DHS, which, according to agency officials, provides equivalent information to a cost-benefit analysis. We are in the process of reviewing the alternatives analysis that was completed in 2008 and life-cycle cost estimates which TSA provided to us on March 12, 2010, to determine the extent to which these estimates reflect the additional costs to staff these units. We estimate that, based on TSA's fiscal year 2011 budget request and current AIT deployment strategy, increases in staffing costs due to doubling the number of

---

[10] DHS Acquisition Management Directive 102–01, Jan. 20, 2010.

[11] We have previously reported that deploying technologies that have not successfully completed operational testing and evaluation can lead to cost overruns and underperformance. In addition, our reviews have shown that leading commercial firms follow a knowledge-based approach to major acquisitions and do not proceed with large investments unless the product's design demonstrates its ability to meet functional requirements and be stable. The developer must show that the product can be manufactured within cost, schedule, and quality targets and is reliable before production begins and the system is used in day-to-day operations. See *http://www.gao.gov/products/GAO-10-128* and GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition, http://www.gao.gov/products/GAO-04-386SP* (Washington, DC: Jan. 2004).

[12] TSA deployed the ETPs from January to June 2006.

[13] The results of TSA's laboratory and operational testing are classified.

AITs that TSA plans to deploy could add up to $2.4 billion over the expected service life of this investment.[14]

While we recognize that TSA is taking action to address a vulnerability of the passenger checkpoint exposed by the December 25, 2009, attempted attack, we continue to believe that, given TSA's expanded deployment strategy, conducting a cost-benefit analysis of TSA's AIT deployment is important. An updated cost-benefit analysis would help inform TSA's judgment about the optimal deployment strategy for the AITs, as well as provide information to inform the best path forward, considering all elements of the screening system, for addressing the vulnerability identified by this attempted terrorist attack.

TSA HAS MADE PROGRESS IN SECURING AIR CARGO AND AIRPORT ACCESS, BUT CHALLENGES REMAIN

TSA Has Made Progress in Meeting the Air Cargo Screening Mandate, But Faces Participation, Technology, Oversight, and Inbound-Cargo Challenges

As we previously reported in March 2009, based on preliminary observations from ongoing work, TSA has taken several key steps to meet the statutory mandate to screen 100 percent of air cargo transported on passenger aircraft by August 2010.[15] Among the steps that TSA has taken to address domestic air cargo screening, the agency has revised its security programs to require more cargo to be screened; created the Certified Cargo Screening Program (CCSP), a voluntary program to allow screening to take place earlier in the shipping process and at various points in the air cargo supply chain—including before the cargo is consolidated; issued an interim final rule, effective November 16, 2009, that, among other things, codifies the statutory air cargo screening requirements of the 9/11 Commission Act and establishes requirements for entities participating in the CCSP;[16] established a technology pilot program to operationally test explosives trace detection (ETD) and X-ray technology;[17] and expanded its explosives detection canine program.

While these steps are encouraging, TSA faces several challenges in meeting the air cargo screening mandate. First, although industry participation in the CCSP is vital to TSA's approach to move screening responsibilities across the U.S. supply chain, the voluntary nature of the program may make it difficult to attract program participants needed to screen the required levels of domestic cargo. Second, while TSA has taken steps to test technologies for screening and securing air cargo, it has not yet completed assessments of the various technologies it plans to allow air carriers and program participants to use in meeting the August 2010 screening mandate. According to TSA officials, several X-ray and explosives detection systems (EDS) technologies successfully passed laboratory testing, and TSA placed them on a December 2009 list of qualified products that industry can use to screen cargo after August 2010.[18] TSA plans to conduct field testing and evaluation of these technologies in an operational environment. In addition, TSA plans to begin laboratory testing for ETD, Electronic Metal Detection (EMD), and additional X-ray technologies in early 2010, and anticipates including these technologies on the list of qualified products the industry can use by the summer of 2010, before proceeding

---

[14] To estimate the cost of the additional staff needed to operate the AIT machines during their service life as a result of TSA's increased deployment of the AIT, we used information in the President's budget request for fiscal year 2011 and from interviews with TSA officials. We identified staffing costs to operate each AIT ($369,764) and multiplied this figure by the number of additional AITs that TSA has recently planned to deploy by 2014 (922 units) to calculate the additional staffing costs, which equaled $340,922,408. We then multiplied the additional staffing costs of $340,922,408 by 7 years to calculate the additional staffing cost to operate additional AIT units during their expected service life, which equaled $2,386,456,856.

[15] GAO–09–422T. The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act)requires that by August 2010, 100 percent of cargo—domestic and inbound—transported on passenger aircraft be physically screened. The 9/11 Commission Act establishes minimum standards for screening air cargo and defines screening for purposes of the air cargo screening mandate as a physical examination or nonintrusive methods of assessing whether cargo poses a threat to transportation security. Solely performing a review of information about the contents of cargo or verifying the identity of the cargo's shipper does not constitute screening for purposes of satisfying the mandate. See Pub. L. No. 110–53, § 1602(a), 121 Stat. 266, 477–79 (codified at 49 U.S.C. § 44901(g)). For the purposes of this statement, domestic air cargo refers to cargo transported by air within the United States and from the United States to a foreign location by both U.S. and foreign-based air carriers; and in-bound cargo refers to cargo transported by U.S. and foreign-based air carriers from a foreign location to the United States.

[16] See Air Cargo Screening, 74 Fed. Reg. 47672 (Sept. 16, 2009).

[17] ETD requires human operators to collect samples of items to be screened with swabs, which are chemically analyzed to identify any traces of explosives material.

[18] EDS uses computer-aided tomography X-rays to examine objects inside baggage and identify the characteristic signatures of threat explosives.

with operational testing.[19] As we previously reported, based on preliminary observations from on-going work, X-ray and ETD technologies, which have not yet been fully tested for effectiveness, are currently being used by industry participants to meet air cargo screening requirements.[20] We are examining this issue in more detail as part of our on-going review of TSA's air cargo security efforts, to be issued later this year.

Third, TSA faces challenges overseeing compliance with the CCSP due to the size of its current Transportation Security Inspector (TSI) workforce. Under the CCSP, in addition to performing inspections of air carriers and freight forwarders, TSIs are to also perform compliance inspections of new regulated entities that voluntarily become certified cargo screening facilities (CCSF), as well as conduct additional CCSF inspections of existing freight forwarders. TSA officials have stated that the agency is evaluating the required number of TSIs to fully implement and oversee the program. Completing its staffing study may help TSA determine whether it has the necessary staffing resources to ensure that entities involved in the CCSP are meeting TSA requirements to screen and secure air cargo.[21] As part of our on-going work, we are exploring to what extent TSA is undertaking a staffing study.

Finally, TSA has taken some steps to meet the screening mandate as it applies to in-bound cargo but does not expect to achieve 100 percent screening of inbound cargo by the August 2010 deadline. TSA revised its requirements to, in general, require carriers to screen 50 percent of nonexempt inbound cargo. TSA also began harmonization of security standards with other nations through bilateral and quadrilateral discussions.[22] In addition, TSA continues to work with Customs and Border Protection (CBP) to leverage an existing CBP system to identify and target high-risk air cargo. However, TSA does not expect to meet the mandated 100 percent screening level by August 2010. This is due, in part, to challenges TSA faces in harmonizing the agency's air cargo security standards with those of other nations. Moreover, TSA's international inspection resources are limited. We will continue to explore these issues as part of our on-going review of TSA's air cargo security efforts, to be issued later this year.

TSA Has Taken Actions to Strengthen Airport Security, but Faces Challenges That Include Assessing Risk and Evaluating Worker Screening Methods

In our September 2009 report on airport security, we reported that TSA has implemented a variety of programs and protective actions to strengthen the security of commercial airports.[23] For example, in March 2007, TSA implemented a random worker screening program—the Aviation Direct Access Screening Program (ADASP)—Nation-wide to enforce access procedures, such as ensuring that workers do not possess unauthorized items when entering secured areas.[24] In addition, TSA has expanded requirements for background checks and for the population of individuals who are subject to these checks, and has established a statutorily directed pilot program to assess airport security technology.[25]

As we reported in September 2009, while TSA has taken numerous steps to enhance airport security, it continues to face challenges in several areas, such as assessing risk, evaluating worker screening methods, addressing airport technology needs, and developing a unified National strategy for airport security.[26] For example, while TSA has taken steps to assess risk related to airport security, it has not conducted a comprehensive risk assessment based on assessments of threats, vulnerabilities, and consequences, as required by DHS's National Infrastructure Protection Plan. To address these issues, we recommended, among other things, that TSA develop a comprehensive risk assessment of airport security and mile-

---

[19] EMD devices are capable of detecting metallic-based explosives, such as wires, within a variety of perishable commodities at the cargo-piece, parcel, and pallet level.

[20] *http://www.gao.gov/products/GAO-09-422T*.

[21] For additional information on TSA's staffing study, see GAO, *Aviation Security: Status of Transportation Security Inspector Workforce, http://www.gao.gov/products/GAO-09-123R* (Washington DC: Feb. 6, 2009).

[22] The term harmonization is used to describe countries' efforts to coordinate their security practices to enhance security and increase efficiency by avoiding duplication of effort.

[23] GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls, http://www.gao.gov/products/GAO-09-399* (Washington, DC: Sept. 30, 2009).

[24] For the purposes of this statement "secured area" is used generally to refer to areas specified in an airport security program that require restricted access. See 49 C.F.R. §§ 1540.5, 1542.201.

[25] According to TSA officials, the agency established this program in response to a provision enacted through the Aviation and Transportation Security Act. See Pub. L. No. 107–71 § 106(d), 115 Stat. at 610 (codified at 49 U.S.C. § 44903(c)(3)).

[26] *http://www.gao.gov/products/GAO-09-399*.

stones for its completion, and evaluate whether the current approach to conducting vulnerability assessments appropriately assesses vulnerabilities. DHS concurred with these recommendations and stated that TSA is taking actions to implement them.

Our September 2009 report also reported the results of TSA efforts to help identify the potential costs and benefits of 100 percent worker screening and other worker screening methods.[27] In July 2009 TSA issued a final report on the results and concluded that random screening is a more cost-effective approach because it appears "roughly" as effective in identifying contraband items at less cost than 100 percent worker screening.[28] However, the report also identified limitations in the design and evaluation of the program and in the estimation of costs, such as the limited number of participating airports, the limited evaluation of certain screening techniques, the approximate nature of the cost estimates, and the limited amount of information available regarding operational effects and other costs. Given the significance of these limitations, we reported in September 2009 that it is unclear whether random worker screening is more or less cost effective than 100 percent worker screening. In addition, TSA did not document key aspects of the pilot's design, methodology, and evaluation, such as a data analysis plan, limiting the usefulness of these efforts. To address this, we recommended that TSA ensure that future airport security pilot program evaluation efforts include a well-developed and well-documented evaluation plan, to which DHS concurred.

Moreover, although TSA has taken steps to develop biometric worker credentialing, it is unclear to what extent TSA plans to address statutory requirements regarding biometric technology, such as developing or requiring biometric access controls at airports, establishing comprehensive standards, and determining the best way to incorporate these decisions into airports' existing systems.[29] To address this issue, we have recommended that TSA develop milestones for meeting statutory requirements for, among other things, performance standards for biometric airport access control systems. DHS concurred with this recommendation. Finally, TSA's efforts to enhance the security of the Nation's airports have not been guided by a National strategy that identifies key elements, such as goals, priorities, performance measures, and required resources. To better ensure that airport stakeholders take a unified approach to airport security, we recommended that TSA develop a National strategy that incorporates key characteristics of effective security strategies, such as measurable goals and priorities, to which DHS concurred and stated that TSA is taking action to implement it.

Project Newton May Result in New Explosives Testing Standards for TSA's Screening Technology

As we discussed in our October 2009 report, TSA and the DHS Science and Technology Directorate (S&T) are pursuing an effort—known as Project Newton—which uses computer modeling to determine the effects of explosives on aircraft and develop new requirements to respond to emerging threats from explosives.[30] Specifically, TSA and S&T are reviewing the scientific basis of their current detection standards for explosives detection technologies to screen passengers, carry-on items, and checked baggage. As part of this work, TSA and S&T are conducting studies to update their understanding of the effects that explosives may have on aircraft, such as the consequences of detonating explosives on board an in-flight aircraft. Senior TSA and DHS S&T officials stated that the two agencies decided to initiate this review because they could not fully identify or validate the scientific support requiring explosives detection technologies to identify increasingly smaller amounts of some explosives over time as required by TSA policy. Officials stated that they used the best available information to originally develop detection standards for explosives detection technologies. According to these officials, TSA's understanding of

---

[27] To respond to the threat posed by airport workers, the Explanatory Statement accompanying the DHS Appropriations Act, 2008, directed TSA to use $15 million of its appropriation to conduct a pilot program at seven airports. Explanatory Statement accompanying Division E of the Consolidated Appropriations Act, 2008, Pub. L. No. 110–161, Div. E, 121 Stat. 1844, 2042 (2007), at 1048. While the Statement refers to these pilot programs as airport employee screening pilots, for the purposes of this statement, we use "worker screening" to refer to the screening of all individuals who work at the airport.

[28] Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress* (Washington, DC, July 7, 2009).

[29] Among other things, the Intelligence Reform and Terrorism Prevention Act of 2004 directed TSA, in consultation with industry representatives, to establish comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems. See Pub. L. No. 108–458, § 4011, 118 Stat. 3638, 3712–14 (2004) (codified at 49 U.S.C. § 44903(h)(5)).

[30] *http://www.gao.gov/products/GAO-10-128.*

how explosives affect aircraft has largely been based on data obtained from live-fire explosive tests on aircraft hulls at ground level. Officials further stated that due to the expense and complexity of live-fire tests, the Federal Aviation Administration, TSA, and DHS collectively have conducted only a limited number of tests on retired aircraft, which limited the amount of data available for analysis. As part of this ongoing review, TSA and S&T are simulating the complex dynamics of explosive blast effects on an in-flight aircraft by using a computer model based on advanced software developed by the National laboratories. TSA believes that the computer model will be able to accurately simulate hundreds of explosives tests by simulating the effects that explosives will have when placed in different locations within various aircraft models. As discussed in our October 2009 report, TSA and S&T officials expect that the results of this work will provide a much fuller understanding of the explosive detection requirements and the threat posed by various amounts of different explosives, and will use this information to determine whether any modifications to existing detection standards should be made moving forward. We are currently reviewing Project Newton and will report on it at a later date.

Madam Chairwoman, that concludes my statement and I would be happy to answer any questions.

Ms. JACKSON LEE. The gentleman from Pennsylvania, the Ranking Member.

Mr. DENT. Thank you, Madam Chairwoman. Thank you for getting things started. I appreciate it. Apologize for my tardiness. I would like to ask unanimous consent to deliver my opening statement at this time.

Ms. JACKSON LEE. Hearing no objection, so ordered. The gentleman is recognized for 5 minutes for his opening statement.

Mr. DENT. Thank you, Madam Chairwoman, and happy St. Patrick's Day.

While I am sure——

Ms. JACKSON LEE. Thank you. Happy St. Patrick's Day to everyone. Do you have your green tie?

Mr. DENT. I have my green tie.

Ms. JACKSON LEE. Yes, you are.

Mr. DENT. I do.

Ms. JACKSON LEE. I am in green, too. Thank you.

Mr. DENT. Well, I am sure many in our—well, I am sure that many in our panels in the audience and perhaps even our staff are looking forward to the end of this workday. We have some pressing business, and I want to commend the Chairwoman for having such an important hearing. It is really very important.

I think it is critical to recognize, however, that no matter what screening technologies that we deploy here in the United States, none of these—none of these would have stopped Umar Farouk Abdulmutallab from boarding Northwest Airlines Flight 253 in Amsterdam with powdered explosives concealed on his person.

That responsibility fell to an overseas airport whose security, I might add, far exceeded minimum international security standards. For this reason I want to applaud Secretary Napolitano for her aggressive outreach to over 2 dozen countries since the attempted Christmas day attack in hopes of securing more stringent international minimal standards for aviation security.

We should never shy away from taking whatever immediate actions are necessary to protect Americans at home and abroad. This is why I was pleased to learn that just last week the Secretary signed a joint declaration of understanding with 16 other nations highlighting the need for the modernization of international aviation security standards.

Secretary Napolitano said, "The attempted terrorist attack on December 25 has global ramifications demonstrating the need for enhanced security standards, information sharing and screening measures throughout the international aviation system." I couldn't agree more.

This is an incredibly positive first step, but it is only a first step. The key is making sure future actions match the rhetoric, and I hope to see more of this kind of international engagement in the future. As this Congress, and particularly this committee, learned the hard way with its ill-advised international mandates on 100 percent air and maritime cargo scanning, consultation, and collaboration with our international partners is absolutely critical to improving security in the United States over the long term.

With respect to intradepartmental and external coordination, I recently asked my committee staff to take a closer examination of how the TSA communicates its needs at the Transportation Security Lab and the Department's Science and Technology Directorate. I also asked the staff to examine how those requirements were developed, how they are risk-informed, and if they include an open and honest dialogue with private industry.

The committee staff summarized the process "convoluted, confusing, and inconsistent." That is unfortunate. Over years after establishing the TSA with the passage of the Aviation and Transportation Security Act of 2001, I find this troubling. I hope we can explore ways to improve this process throughout this hearing.

Today we have with us representatives of TSA, concerned stakeholders, and representatives of industry. This is a diversified hearing with diversified testimony that I hope will answer one fundamental question. How can we improve the processes that bring state-of-the-art technology to bear on our most pressing security threats as expeditiously as possible without sacrificing quality controls? I would ask each of our witnesses to answer that question during the course of today's hearing.

Thank you again to our witnesses for joining us today.

I yield back the balance of my time. Thank you for the indulgence, Madam Chairwoman.

Ms. JACKSON LEE. I thank the Ranking Member.

I thank all the witnesses for their testimony.

I remind each Member that he or she will have 5 minutes to question the panel, and I will now recognize myself for questions.

Mr. Dent mentioned that we have a number of principals and stakeholders who are participating in this hearing today, and I add that we also are able to have an airport, one of the Nation's top airports, represented here today to contribute to what I think is a very vital discussion.

Let me begin the questioning with Mr. Kane. There is representation, I believe, that you say that the Department of Homeland Security and TSA intend to purchase 1,000 of the body scanners. Is that my understanding, or is that projected budget request?

Mr. KANE. We intend to purchase 500.

Ms. JACKSON LEE. You have 500 now, so you intend to have a total of 500?

Mr. KANE. Then the fiscal year 2011 includes an additional 500 in the administration's——

Ms. JACKSON LEE. So there are 1,000 over a 2-year period.

Mr. KANE. Yes, ma'am.

Ms. JACKSON LEE. How do you intend to select the airports that will be a recipient of the scanners?

Mr. KANE. We have gone through a process. Basically, we will use our risk prioritization process, but in this case you do phase constraints at airports. So these first 500 machines that we will be deploying this year, we have looked at the footprints, we have pulled out the designs for airports to look at the checkpoint footprint that they have.

We are spreading them somewhat throughout the system to (1) get better coverage of people with these 500. We get about 35 percent of passengers. But when you show up in an airport, you might have about a 90 percent chance of actually going through an AIT in the airport that you show up at, because we are targeting some of the larger airports down through the Cat-2s, so the Cat-Xs through the Cat-2s will have some.

Then we look at how to make sure we don't impact throughput, and so we have done designs that will set a walk-through metal detector alongside of the imaging technology, and we can use that as overflow device. So again, you won't know if you are going to get offered up to the imaging technology, but you may end up going through a walk-through metal detector as well.

After those first 500, we are working with industry to get auto detection capability that we would like to see the industry produce that, and (1) retrofit the 500 that we will put out into the field, and then for the next 500 we would like to see that capability in place by the time we deploy them.

Ms. JACKSON LEE. Do you have the list of the airports, or are you in the process of reviewing them as we speak?

Mr. KANE. I don't have the list with me. We have announced 11 of those airports. We have a longer list than that, a more complete list than that. Some of them will probably change around as reality meets design plans. That is when we go out and work with them.

Ms. JACKSON LEE. Well, would you provide this committee with both the process by which you made this election and as well the list?

Mr. KANE. Yes, ma'am.

Ms. JACKSON LEE. If you could do that as soon as possible, please.

In October 2009 the GAO reported that inconsistent communication, the lack of an overarching test and evaluation strategy has limited S&T's and TSA's ability to coordinate effectively with one another. What, if anything, has DHS done to facilitate communication and to improve coordination among TSA and S&T? What are the challenges that remain?

Mr. KANE. I think we have done a tremendous amount of work to mature those processes and that relationship with S&T in that oversight that they provide of our operational test and evaluation for the AIT in particular. We have worked through our acquisition process, we have tested it in the labs, we have tested it in our integration facility, and we have tested it out in the field.

Those test plans—while some of the testing is done by S&T, the test plans for out in the field are reviewed, and the results of those

are reviewed before we can make that investment decision in the investment process that DHS manages. So I think we have, you know, we are not where GAO reported we were back in October 2009 in this procurement or in our other procurements that I talked about.

Ms. JACKSON LEE. Do you have a direct point that you can give to this committee that says that the communication between S&T and TSA has improved? What is that one point?

Mr. KANE. When I go to the acquisition review board with the deputy secretary, S&T's representative for test and evaluation is sitting across the room, and they weigh in on those results that we are producing for making that investment decision, so we clearly have the communication sitting right in the same room with us when we are having our oversight within the Department.

Ms. JACKSON LEE. Let me quickly thank you.

Mr. Buswell, for AIT, the auto detect technology that is being piloted at the Amsterdam airport appears to eliminate most privacy issues that have been raised by introducing human screeners into the process only when prohibited items are detected. What is your opinion of the auto detect technology and what is S&T's current and planned role with this technology? Will this be piloted in the United States?

Mr. BUSWELL. Thank you, Madam Chairwoman. The decision on whether or not to pilot the technology is not ours. It will be TSA's. It will be based upon independent test and evaluation of those algorithms when they are ready at TSL and in the field that determine—and I would yield to Mr. Kane—but the criteria that we have discussed is it has to be as least as good as the human operator monitoring those images. So we won't deploy and rely on automatic target recognition algorithms that do a worse job than the human operators. Security is why we have these pieces of equipment.

Ms. JACKSON LEE. The human operators are the TSO officers?

Let me move quickly to Mr. Lord. My time is running out. GAO gave a very extensive report.

As I do that, let me submit into the record the statement—ask unanimous consent to submit into the record the statement of Colleen M. Kelley, National President, National Treasury Employees Union. Hearing no objection, this statement is put into the record.

[The statement of the National Treasury Employees Union follows:]

STATEMENT OF COLLEEN M. KELLEY, NATIONAL PRESIDENT, NATIONAL TREASURY EMPLOYEES UNION

MARCH 17, 2010

Madam Chairwoman and Ranking Member Dent, thank you for allowing me to share some thoughts on checkpoint security. As National President of NTEU, I represent thousands of TSOs at over 40 airports. Many of my members came to TSA when it was created, not long after 9/11. They came to TSA because they wanted to help keep this country safe. Despite the many hardships endured by TSOs—low pay, high on-the-job injury rates, terrible morale due to a culture of distrust—I think you would agree that they do an excellent job keeping us safe.

I believe that people, not technology, are our most important asset in combating terrorism. We need adequate staff and we need adequate training for that staff, and we need to treat them with dignity.

I met with my members recently, and we talked about the AIT machines that TSA is installing as a more efficient method of detecting objects hidden by terrorists. The TSA budget requests almost $530 million for fiscal year 2011 to purchase, install, and operate these machines. While we applaud the effort to upgrade technology and the increased staffing to accompany the machines, we would urge the committee to ensure that the machines are adequately tested before 500 more are purchased. GAO has indicated that TSA has not been able to verify how effective AIT scanners will be in detecting hidden explosives, for example. If AITs are used in primary screening, and they have vulnerabilities that have not been fully investigated, we will have wasted a vast sum of money.

With the increased staffing requested in the budget, there should be a major emphasis on training. I am very concerned about the training being conducted for these machines and we have not heard from TSA about the training program they have prepared. For the machines we have now, both at the checkpoint and in baggage, training is inadequate. Most of the training is done through on-line computers. In many of the airports, the number of computers is inadequate. Sometimes they are very far away from the work area, in a location difficult to get to. There is very little hands-on training. My members tell me that they find it much more helpful to be taught by a person, so that you can ask questions and discuss methods. Computers fulfill the paper requirement for training, but it is not ideal. If TSA put as much effort into training its TSOs as it does in evaluating its TSOs, it would have a stellar training program.

TSOs have a lot of experience in checkpoint screening, but without collective bargaining, their ideas are not considered, and that is TSA's loss. We look forward to a permanent administrator at TSA, who will provide much needed direction and leadership.

Collective bargaining for TSOs remains NTEU's main goal. NTEU appreciates the effort of your subcommittee in assessing checkpoint security. We know that you believe, as we do, that the people who work at TSA are its greatest asset. We are most secure when people drive technology, rather than technology driving people.

Ms. JACKSON LEE. As I put it into the record, Mr. Lord mentions that on all of this new technology, particularly the body scanners, AIT, if the personnel are not trained, right now it is represented the training is done by computers. Can you comment on the need for the training of the users of this equipment?

Could you quickly comment on the critical problem of the relationship between TSA and the DHS S&T Directorate and how can lawmakers or officials address this problem—training and the utilization of the product and the communication issue?

Mr. BUSWELL. Regarding your first question, Madam Chairwoman, the training is a very important component of AIT usage. Obviously, it does not have auto alarm capability. Therefore, it means you have to train people, and train, so it is very important you have a clear, consistent, systematic program. That is something that is not included in the hardware cost of AIT. Obviously, this is something that interests us.

Any time you have a human involved in anything, it introduces some inconsistencies potentially in your process, as humans are prone to, you know, error, distractions, et cetera. So I think a lot of people are focusing on the technology, but you have to be mindful you need an image operator to interpret the results. So that potentially introduces some inconsistency.

Your second question—this coordination issue between S&T and TSA and TSL—this is one we reported on extensively in our October 2009 report. The Department agreed that the coordination process needed to be made more transparent and streamlined. I think it is good news.

Robin is a part of the ARB process. He chairs the IPT Capstone priority setting process, but this is something we are going to have to continue to look at. Any time I see an organization chart with

dotted line relationships, it always raises a question in my mind like who is in charge? That is what one of the issues we highlighted in our report. The roles and responsibilities of all the players were not clear. Sounds like they have taken steps to address that, but I tend to be conservative on this, so let us give it a little more time.

Ms. JACKSON LEE. Thank you.

Mr. Dent is recognized for 5 minutes.

Mr. DENT. Thank you, Madam Chairwoman.

Although this hearing is really about checkpoint screening, committee staff has been advised that there is a vendor that has a promising piece of technology that could be used for the screening of palletized air cargo, but that S&T has decided not to invest any further in its development. With the 100 percent screening mandate for air cargo looming, why has S&T decided not to expend any funds in development of technologies for palletized cargo, Mr. Buswell, if you could address that?

Mr. BUSWELL. Sure. I don't know which technology that you are specifically referring to, but we are in fact investing a significant amount of money in air cargo screening, about $11 million this year, and in the President's request for fiscal year 2011 there is about $15 million for air cargo screening technology.

The focus of that screening technology is at looking at palletized and break bulk screening—through trace detection, primarily in mass spectrometry sorts of devices.

The other aspect of cargo that beyond the technology is very important is a canine aspect of explosive detection in cargo. We are investing also in advanced training aids. These are one of the highest priorities on TSA's list for our investment—training aids for canines as well as looking at how do we determine which canines are going to be good explosive detection instruments.

Are there certain behavioral characteristics that we can look at as puppies, you know? Are there DNA markers, those sorts of things that help us identify which, you know, which of these animals will go through the fairly expensive and extensive training?

So we are in fact investing. We are interested in all technologies. That is, you know, the private sector involvement, I think, is a win-win-win for the Department, the private sector, and the country, when you can get them involved.

My experience is the private sector involvement—we get results more quickly with the private sector involved. They have a profit motive that gets them to the, you know, gets them to the end point quickly. In fact under circumstances we can do this with very minimal investment of Government dollars with establishing the right kind of requirements and then offering our services at the TSL or other places to test their technology when it is ready.

If you have a constituent that thinks they have an answer, we are ready to listen. In fact, we have a long-range BAA that is open and provides an easy vehicle for them to get in front of us to look at their technology.

Mr. DENT. Well, thank you. Thank you, and appreciate that.

Mr. Kane, the President's fiscal year 2011 budget includes $214 million in funding for an additional 500 AIT machines and $235 million for an additional 3,700 FTEs to operate the machines. We

are concerned with the funding request for additional personnel, as we all are.

Does the request for additional personnel take into account deficiencies that may be gained by eventually reducing the number of magnetometers that will be removed or replaced with the AIT machines?

Mr. KANE. The request for personnel includes about an additional $1.25 person per checkpoint lane that has an AIT with the walk-through metal detector standing next to it. But it presumes we will have that auto detection capability as well.

Mr. DENT. So your funding request does take into account, then, the fewer personnel that will be needed when the AIT machines become operational with that auto detect feature?

Mr. KANE. Yes, sir.

Mr. DENT. Okay. Then, finally, did TSA look to identify any efficiencies in its current staffing models for it opted to ask Congress for the 3,700 new FTEs?

Mr. KANE. Congressman, yes, sir. TSA has been looking at those staffing models over the years quite extensively, and now, if you look at where we were a few years ago with 44,000 people in checkpoints and in the baggage screening rooms, that number is more like 39,000, and we have invested many of those resources into the other layers of security.

We continue to get savings with the inline systems that we are putting into airports, and we always reinvest those savings into other areas and take into account those savings with the additional requests that we have.

Mr. DENT. Finally, committee staff has reviewed correspondence between TSA and a certain vendor that essentially denied the vendor the opportunity to submit a white paper in technology for consideration, because a TSA solicitation was no longer active. The vendor was told to look on the Federal business opportunities website for future solicitations. I have a few questions related to this matter, which I think illustrates the problem.

Isn't TSA potentially missing promising or better and more efficient technologies by not accepting white papers in technologies on a rolling basis? Isn't that shortsighted?

Mr. KANE. We need to manage both of those things, Mr. Congressman. You know, I am a procurement organization to a large extent, and so most of the solicitations I do are to buy things already established on those QPLs.

But recognizing your concern and our own concerned with that, we look to S&T to do a lot of this type of work for us, so a lot of times I will refer folks back to S&T. But just this week TSA did issue a broad agency announcement that would allow such white papers to be submitted, and we would do an evaluation of them and determine whether they would be an effective capability that we would want to bring into the TSA fleet. Then we can explore further through that procurement process.

Ms. JACKSON LEE. The gentleman yields back.

I would now like to recognize the Chairman of the full committee, Chairman Bennie Thompson.

Mr. THOMPSON. Thank you very much, Madam Chairwoman. We have had an interesting set of witnesses, as well as some questions.

Let me go around very quickly. We are deploying this new technology for the next thousand machines—500 out of last year's, 500 out of this. What is the cost? Who will bear the cost of modifications at airports for these machines? What is the formula for the modification, Mr. Kane?

Mr. KANE. Mr. Chairman, we are looking at a number of different designs, and our goal through all of this is to minimize any infrastructure costs at airports. We think with the design so that we are working and by getting auto detection and getting rid of the walk-through metal detector when we get the auto detection, we will be able to minimize the impact on airports.

Minor infrastructure costs within the checkpoints, TSA works with the airports on who funds that. We are not planning to do major infrastructure programs to put the AITs into checkpoints.

Mr. THOMPSON. Okay. If there is a cost, who does TSA expect to bear that cost for any modifications?

Mr. KANE. I think if we get to the point where we find out we are going to have major infrastructure costs, we will have to have that conversation with an airport. TSA does not fund infrastructure costs at this point, though, and we have not in the past. So there is not an intent going forward to do that. The intent is to do designs that don't require that.

Mr. THOMPSON. But you know we have had very few designs that don't cost airports money. You are aware of that. Am I correct?

Mr. KANE. I would say much of the checkpoint technologies that we have invested in we work with the airports and pay the cost to install that equipment at the airports with little to no impact on the airport.

Mr. THOMPSON. Well, there are some differences. We talk to airports all the time, and they say that they cost. So what I would like for you to do for us is take the 10 largest airports and provide this committee with whether or not those airports have had to incur costs locally in implementing any of this new technology.

Mr. KANE. Mr. Chairman, we will definitely do that.

Mr. THOMPSON. Okay.

Next question is Mr. Lord talked about this same implementation process that somehow we didn't operationally test equipment before we installed it. Is he correct?

Mr. KANE. We operationally tested the AIT, both the manufacturers that are on our qualified products list back in the late summer, early fall in the airports, and we produced those test results for the acquisition review board that I referred to earlier, and they were reviewed by Mr. Buswell's staff as well.

Mr. THOMPSON. Mr. Lord, do you care to——

Mr. LORD. Yes, that is correct. The technology I was referring to was technology that preceded the AIT deployment, the so-called explosive trace portals or puffers. In contrast to the experience with the puffers, TSA has subjected them to a much more rigorous testing process based on the documentation we have reviewed.

Mr. THOMPSON. So you are satisfied with it.

Mr. LORD. Yes.

Mr. THOMPSON. Okay. Thank you.

I am not saying whether this will be Mr. Buswell's question or Dr. Hallowell. We get comments from small businesses, medium-

size businesses and some large that it just takes entirely too long to get new technologies through the system. Have we designed some kind of matrix or model that can give anybody who is interested in working in this area some idea of how long it might take?

Mr. BUSWELL. Mr. Chairman, we can give them an estimate. Let me just say that when it comes to evaluating technology at the Transportation Security Laboratory, Dr. Hallowell has essentially three sources of input.

One, it can come directly from TSA. In other words they have got a commercial product that they would like evaluated with respect to their desire, the capabilities, or their desired requirements. That is first.

Second, we may have a developmental technology within S&T that is ready for developmental test and evaluation or even independent test and evaluation, and that would be an input.

The third is industry coming straight to TSL and saying, "I have got the answer, and I would like you to evaluate my technology."

There are really two different paths that, regardless of where it is referred from, that we go through. One is on the developmental side, and I will call that research and developmental assessment or evaluation as opposed to true independent test and evaluation.

That is very collaborative, done under a Cooperative research and development agreements generally with people who are interested in having their technology assessed, or a bailment, where they will just turn over the equipment, you know, for our use temporarily. We will be, you know, as I said, very collaborative with them and providing them test results, briefing them on the results, the performance of their equipment.

When it becomes apparent that that equipment could solve a problem that TSA has or a requirement that TSA has established, then it enters the independent test and evaluation process. That is not collaborative. That is independent, and it is rigorous, and it is to the certification standards or the qualification standards that TSA has established.

So once a technology enters that process, they may not hear anything for a few months while it goes through it. The time that it takes depends on the—depends on the flow of materials through the TSL. I will let Dr. Hallowell talk about that, if you would like.

But they are somewhat resource constrained in their ability to—to throughput technology, so we haven't had to turn anyone away yet, but with the—with the increasing interest in this particular area, we are having to look at how we resource the lab, what kind of capital improvements we need to make at the lab in order to ensure that we can continue to provide that service for TSA and for the American people.

So, you know, I appreciate the question, and it is something that I think about regularly.

Dr. Hallowell, did you want to add anything on the time line?

Ms. HALLOWELL. Mr. Chairman, good afternoon. I just wanted to add that one of the things that is a big criteria in terms of how fast something travels through the laboratory has to do with the technology readiness level as well.

We see everything from things that are just beyond research concepts to bread boards to engineering prototypes, so depending upon

the maturity level, it depends on how long it takes for that technology to grow and mature to the point where it is capable of going into independent test and evaluation.

The role of the R&D test and evaluation portion of the laboratory is really to help our industrial partners mature technology. We do that very diligently. In many cases we offer up test articles such as IEDs or weapons or whatnot, so if there is any training involved so the technology can learn, if you will, develop the algorithms to actually find the bombs, that is available to them. So that can take a long time as well.

Mr. THOMPSON. Well, ma'am, I apologize for asking questions that ended up with such lengthy answers, but can you provide the committee, as best you can—I understand it is dependent on the situation—the range that a company could expect to work with you before a decision is reached?

What we hear is some of them have limited resources, and they are trying their best to comply with the request, but after they meet one, they say something else pops up. I wouldn't want us to miss out on some good technology because we were not clear as to how the vetting process for new technology goes.

So if you can just provide the committee with your best experienced guess at the time, it would help.

Ms. HALLOWELL. Well, let me respond to your question. We don't want to hinder any technology development, so we will certainly invite people to the laboratory regardless of how mature the technology is. But at the end of the day, there is a very rigorous protocol that is associated with TSA acquisition standards. That testing is done by the IT&E team, and it is a fairly rigid benchmark.

We did try to help companies understand what those requirements are and to help them grow. Sometimes without being able to go to a classified level, it is difficult. But we do try to step them through that. My experiences are we have seen everything from 3 to 4 years in collaborative research and development agreements to short periods of time—5 or 6 months, depending upon the technology maturity level, to get to IT&E.

Mr. THOMPSON. Thank you very much, Madam Chairwoman. I yield back. Thank you for being patient.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

I would like to recognize Mr. Austria for 5 minutes.

Mr. AUSTRIA. Thank you, Madam Chairwoman.

I appreciate our panel being here today and helping to clarify, I think, some of the concerns that we have had and the confusion about collaboration and working relationship between S&T, TSL, and TSA. In my opinion I think the process has not been clear, and it is not been accurately and practically defined. I appreciate you being here to help do that.

So let me, if I could, kind of pick up where the Chairman was with his comments towards Dr. Hallowell, if I could. I thank you for being here, and I know you are highly regarded by the staff, and I understand the staff had a very good visit to the Transportation Security Lab a few months ago.

But, Dr. Hallowell, the committee and I think some of the Members here are still concerned that despite best efforts and hard-working people at S&T and TSL and TSA, that the relationship be-

tween these parties is not adequately defined and working to the best possible extent.

I guess in a perfect world, right, if you had an ideal situation, how should that relationship be between S&T, TSL, and TSA? How should that work? Has there been anything that has changed or caused more urgency since the attempted Christmas day bombing that between the agencies you are now working even better or have changed the way you are working? If you could comment on that, please.

Ms. HALLOWELL. Yes, sir. I think that relationship is doing nothing but getting stronger and better even before the Christmas day incident. We have a program manager that works on my staff that spends half his time at either TSA or S&T that can directly communicate input from R&D land, from test and evaluation land, and at the same time can understand better what some of the concerns are from TSA. That has been very helpful.

Obviously, the incident of Christmas day has brought us all very close together, and it is not just the Capstone meetings or the sub-IPT meetings associated with checkpoint, but we do have daily conversations from my laboratory to TSA across all sectors, including cargo, checkpoint, and checked baggage.

Mr. AUSTRIA. If anyone else would like to comment on that as far as any new or promising technologies that you have been pursuing since the Christmas day event or any progress that you can report to this committee of things that you are doing differently now than prior to that incident?

Ms. HALLOWELL. In terms of technology or processes? I am sorry, sir.

Mr. AUSTRIA. Both, I think.

Ms. HALLOWELL. Well, we have certainly accelerated some of the test and evaluation to accommodate what is required from TSA. We have been working very hard on the second round qualification testing for detection performances as it relates to AIT, which Mr. Kane talked about.

We have been very involved otherwise with test and evaluation of explosive detection systems for checked baggage against a new certification standard that TSA has presented to us. So we have been quite busy in the laboratory and been doing double shifts, essentially, testing equipment.

Mr. AUSTRIA. Thank you for that.

Mr. Kane, let me ask you. TSA finalized a strategic plan for passenger checkpoint security in 2008, in August 2008. We understand that TSA has a risk-based approach to securing the most at-risk airports first. We also understand that the AIT or the advanced imaging technology has far superior detection capabilities than traditional metal detectors or detection.

If you think back to 9/11 in the World Trade Center, what happened there we all know, but it seems as though—and I have read reports where New York City still remains one of the top terror targets in the Nation, yet there, you know, there are concerns about that there is not one AIT machine that has yet to be deployed in New York City airport.

If you could comment on that and how that a risk-based approach, how this risk-based approach that you are taking is better protecting passengers.

Mr. KANE. Congressman, the risk-based approach we are taking with AIT in particular, we are spreading it throughout the system, so the New York airports will be on that larger list that I promised the Chairwoman earlier to some level.

We also need to face the constraints of what the airport, until we have auto detect capability, you know, being able to set an AIT next to a walk-through metal detector to make sure that you can still operate the airports with an AIT in the lanes. We are very sensitive to that. The folks who testify after us, I am certain are going to be very sensitive to that.

So we are working with all the airports. The larger airports, certainly, are high-risk airports on the way we do our risk models, and we would like to get as many passengers as possible through AIT, so that drives us to larger airports as well.

Mr. AUSTRIA. My time is up, so I will yield back to the Chairwoman.

Ms. JACKSON LEE. Thank the gentleman.

I am now pleased to recognize the gentleman from Oregon, and as I understand it, served as the Chairperson of the Aviation Committee on T&I for a number of years, Mr. DeFazio.

Mr. DEFAZIO. No, those were the bad old days. I was Ranking Member, but I was there when we conceived of the TSA.

Ms. JACKSON LEE. Oh, then I am half accurate. The Ranking Member, in my book, is equally placed. Thank you.

Mr. DEFAZIO. Thank you, Madam Chairwoman.

I have a question about the throughput on the AITs, because there seems to be considerable divergence. We are hearing from airports and others that they think that it is more like 45 seconds throughput, and TSA is saying 15 seconds. Can someone address the discrepancy? Mr. Kane, perhaps?

Mr. KANE. Congressman, I will address that, yes. Our modeling right now is around 20 to 22 seconds for AIT. It takes a few seconds in the machine—five-ish—and then that image operator we talked about takes time to review and interpret that image to determine whether is anomaly or not. So we have tested as one of the parameters that we measure in our operational test and evaluation.

Throughput is, obviously, you know, it is not just important to airports. It is important to TSA operation as well. We can't do our business if we can't get people through the checkpoints. So it is around 20 seconds.

If we get that auto detect—when we get that capability, that will speed that process as well. Then the other thing we are doing to manage the throughput that maybe I am just not doing a very good job so far of educating people about is the configurations for these first 500, and until we have an auto detection capability, will allow relief for going through the AIT versus going through a walk-through metal detector to ensure we managed that throughput at checkpoints and at the lanes with the AITs at checkpoints in particular.

Mr. DEFAZIO. Okay. Then, but then there is the third variant, which is you allow someone who has been designated to an AIT to choose a pat-down. You are getting a fairly low rate of refusal for AIT?

Mr. KANE. Yes, all of our testing today has shown over 98 percent acceptance by the passengers that are offered to the AIT.

Mr. DEFAZIO. I would be concerned about the 2 percent. Some it may be a privacy issue but, you know, knowing the pat-down regime now, I mean, at Heathrow I experienced much more intrusive pat-downs that are customarily conducted here in the United States, which probably would have found Mr. whatever-his-name-was, you know, the explosive.

But the way we do pat-downs, you probably wouldn't. So I would be concerned about those who were self-selecting out of the AIT. Now, does that cause you concern? Is there some, shall we say, more intrusive pat-down going on with those people?

Mr. KANE. Congressman, I would rather talk about that in a closed session or offline, if I could, sir.

Mr. DEFAZIO. Okay. Just so you hear my concern and you are accommodating it, but I would be happy to hear about it later.

Mr. KANE. Yes, sir. We understand your concern very well.

Mr. DEFAZIO. Okay. This new explosives trace device, the BLS–2, is that gate deployable?

Mr. KANE. The bottle liquid scanner is a liquid scanner.

Mr. DEFAZIO. Right.

Mr. KANE. Yes, it is a desktop machine, so you could, similar to what we are doing with——

Mr. DEFAZIO. Yes, well, because we have been doing these random things at gates with people. You acquire water in the terminal, okay, so you now have what you couldn't have brought through security outside. There is nothing to identify you bought it in the airport, and now you are being randomly, you know, searched with rubber gloves at the gate, and they pull out your 16-ounce bottle of water, and they put it back in, you know, if that could be a threat object. It would have been a threat object at regular security, but it isn't at the gate, because you could have bought it in the airport.

So my question would be are we going to be deploying these technologies to the gates, if we are going to do the random selection at the gates? It seems to me it needs to be technology assisted, not rubber gloves stadium searches.

Mr. KANE. Congressman, I will take that point as well, if I may. Any further discussion should probably be offline on that as well, though, sir.

Mr. DEFAZIO. Okay.

Mr. KANE. But I will again recognize the concern you addressed.

Mr. DEFAZIO. Okay. I will try dogs. Are we optimally utilizing dogs? I have a friend on the Science Committee, and they had a very long discussion of the attempt to construct a dog's nose that was mechanical and how expensive it would be, how long it would take, and how difficult it is. I guess what my colleague said was, "Well, why not more dogs?" They said, "Well, dogs get tired."

You know, I mean, what kind of a shift can a dog do effectively? Can you address that? I hope that shouldn't be classified, because, you know, it is like they are not tracking anything.

Mr. KANE. No, sir, but I am not the canine program manager, so I do apologize.

Mr. DEFAZIO. Okay. All right.

Mr. KANE. I am more into the technology realm, and as you——

Mr. DEFAZIO. Okay. All right.

Mr. KANE [continuing]. We haven't made those mechanical dogs yet.

Mr. DEFAZIO. All right. But I just want to make sure that, yes, I am concerned about whether having been, you know, having dogs and knowing how difficult they are, sometimes the mechanical dog could be a real problem.

Just one thing is blue sky under Capstone IPT, a next-generation, fully automated checkpoints for detecting weapons and explosives on people for aviation, mass transit, public gathering venues, and other potential areas. I am just concerned when I see, like, all those things in one place, and it is going to be fully—it starts sounding like Pentagon acquisition of stuff that never works.

I am hoping we are not putting, you know, I mean, either we are out with RFPs, but we are not actually doing the development or investing in the development ourselves, are we?

Mr. BUSWELL. I will take one.

Mr. DEFAZIO. Yes.

Mr. BUSWELL. We are investing in what we are discussing as the next generation of checkpoint. That is fundamental science and technology. We are looking at that from really a standoff detection standpoint. We have got now checkpoints where we put our bags through X-ray machines, we put our people through metal detectors and advanced amateurs. We have behavior detection officers, who try and assess where there is mal intent on the part of people as they approach the checkpoint.

So to what extent can we automate those things from a standoff position? Can we detect explosive traces from a distance? Can we detect the kinds of things that would be hidden under clothing that would be detectable at the checkpoint through the advanced imaging from a distance?

The reason we think that that is so valuable in that it has application not just to the aviation security checkpoint, but security checkpoints in general, whether it be mass gatherings or public transportation, mass transportation, or other kinds of applications. Secret Service is very interested, obviously, for, you know, for obvious reasons and those sorts of things—Customs and Border Protection.

So this, you know, this serves the Homeland Security enterprise at large to develop this ability to detect people who mean to do harm and the things that they would mean to do harm with from a distance. We think that that is the, you know, if you talk about homeland security 2027, I mean, if our checkpoints in 2027 look the way that they look today, you know, I will—you can fire me, because I haven't done my job.

So we are looking at the future.

Mr. DEFAZIO. Okay. But I just want to make sure, you know, we have some known technologies we haven't fully deployed. We are not diverting a lot of money into this future blue sky kind of thing, which may or may not happen.

You know, I mean, for instance, one last point, Madam Chairwoman, is I am really pleased to see that we are finally moving ahead with, you know, virtually, you know, comprehensive deployment of the advanced, you know, the AT X-ray at baggage screening.

That is something that the workers have needed for years. I have been beating on that for years. We threw out the kind of machines we used in the airports from the Capitol 10 years ago, because they didn't meet standards, and they slowed everything down, because you have to put the bags and move the bag that all that. So I am pleased to see we are finally rolling those out comprehensively. If we can do it even a little quicker than that, it would be great. Thank you.

Thank you, Madam Chairwoman.

Ms. JACKSON LEE. Thank the gentleman for his questions.

Now to the very patient Member from New Mexico, Mr. Luján. He is recognized for his 5 minutes.

Mr. LUJÁN. Thank you, Madam Chairwoman, I think.

Thank you to everyone who is also being here today.

Mr. Kane, we know that liquid explosives are posing a significant risk, a higher risk than ever before as well. Can you tell me what the S&T Directorate is pursuing in new technology that could potentially identify explosives? I think that some of those were mentioned in testimony as well.

In this specific case, can you describe how TSA has worked with S&T Directorate to define technical requirements and to coordinate the R&D and testing effort of this promising new technology?

Mr. KANE. Congressman, yes, sir. First off, just to be clear, imaging technology that we are rolling out to the field does detect liquids, so that is a technology that will detect all nonmetallic threats and metallic threats on passengers, including liquids, powders, gels, all the things we have been talking about recently.

The AT X-ray, those auto detect algorithms that we have been working with the manufacturers on, and S&T has been working with us and them on, include a liquid detection capability in there as well. They continue to work on developing those two an operational product that we can use in the field.

I can't go too far, because our detection standards are certainly sensitive, you know, but our explosive detection systems that we are using down in the bag areas for your checked baggage, we are also working. S&T is doing a tremendous amount of data collection and testing to characterize threats so that we can include those types of threats in those areas as well.

Mr. LUJÁN. Whoever wishes to answer this question, there was some discussion as far as the attention being brought to the number of metal detectors that will be deployed in other airports. Are there commercial airports now where passengers don't have to go through metal detectors to get on a plane?

Mr. KANE. Not in the United States, certainly.

Mr. LUJÁN. So will those metal detectors that we are talking about be deployed in the United States?

Mr. KANE. I am sorry, Congressman. I am not sure I understood the question in terms of more metal detectors.

Mr. LUJÁN. It sounds like at the beginning of the conversation today there was a commitment to the deployment of more metal detectors.

Mr. KANE. No, it is more than leaving them behind for now. So we would like to replace the metal detectors or incorporate them into the imaging technology capability, but——

Mr. LUJÁN. Very good. I just wanted to get that clarification.

As the Chairman was talking about the importance of the time frame associated with the amount of time it takes to get technology through TSA, through TSL to be approved and certified, Dr. Hallowell, if you could provide a framework indicating the amount of time it takes for technology to be certified and approved by TSL and TSA for use in the field, if you could submit that to the committee.

But if you could touch on as well, either Mr. Buswell or Dr. Hallowell, on the complexities associated with licensing and commercialization and how that impacts small business owners, entrepreneurs, scientists, physicists, other businesses that may be taking that technology out for deployment?

Mr. BUSWELL. Yes, sir. I can talk about that little bit. The small businesses in this market space have a very difficult time, and it is because we talk about being able to produce, you know, 1,000 advanced imaging technology devices over a 2-year period. Small businesses have a very difficult time doing that.

What they are very good at, and what you point out correctly, is the innovation. They are excellent at innovation. That is where true innovation happens. The big companies have less of a stomach for that. You know, my private sector history, I worked for General Electric, and one of the things that I did for General Electric was looked at small businesses and the technologies that they were developing, because we truly believed that they were more innovative than we were ever going to be able to come up with.

So licensing is one of the fundamental transition abilities that the small business has, working with a big equipment manufacturer to license their intellectual property or their ideas.

There are other vehicles or tools that we can use within S&T to help them. I mentioned cooperative research and development agreements where we provide something, and they provide something—whatever can change hands except for the Government doesn't provide any money. I mean, that is essentially what a CRADA is.

We can provide laboratory test facilities for their use. We can provide some technical expertise that can help them move things along. So there are a number of ways. For small businesses or for any size business, I would commend—we have put together a one-sheet piece of paper that—we have entitled it, "The Constituent Guide to Doing Business with DHS Science and Technology."

So we will fire these off in 100-round bursts, if you like. We have got many here to help you help your constituents get in the door,

because we don't care where the good ideas come from. We want to use them.

Mr. LUJÁN. Thank you. Just, Mr. Buswell, I want to tell you thank you very much for your positive comments regarding MagViz as well. I think that will be a game-changing technology.

Mr. BUSWELL. Mr. Kane just forgot to mention MagViz when he was talking about the liquid detection. We were all very enthusiastic about the half-scale testing that we think will go on this summer for MagViz.

Mr. LUJÁN. I appreciate that.

Madam Chairwoman, just one thing to point out that Mr. Buswell brought up is when we talk about the CRADAs, this is an area where back in the 1990s Department of Energy, National laboratories, the S&T Directorate, it was working. We saw a decline in the usage of this. These were where the big ideas came from. We need to look to see and get answers from inside, from those entities that are taking advantage of these programs, and see how we can use them to solve some of these big, big ideas and make this work again.

Thank you very much, Madam Chairwoman.

Ms. JACKSON LEE. I thank the gentleman for his very thoughtful analysis and your challenge that we have to get back to that. Now using it for the security of this Nation, I think, is a clarion call. I am disturbed by the suggestions of communication and the seemingly heavy-laden process that hinders inventiveness, small businesses, minority-owned businesses, women-owned businesses. So I join you in that.

I would like to ask Mr. Buswell to provide us—to the committee—the checklist that you just mentioned to Mr. Luján and so that we can review these materials and look—and be forward thinking.

My pleasure as well to yield to another very patient Member, which is indication of contributing Member, as I said for Mr. Luján, Ms. Titus of Nevada, yielded for 5 minutes.

Ms. TITUS. Thank you, Madam Chairwoman.

I would just like to continue along the same lines of discussion about helping the private sector, because it seems that reality is kind of contradictory to what you are espousing as your approach and your goal.

On November 16 of just this past year, Chairman Thompson and Chairwoman Jackson Lee sent a letter to the Acting Administrator Rossides regarding TSA's implementation of the mandate to screen 100 percent of the cargo transported on passenger aircraft. This deadline was to be this coming August.

In the letter TSA was asked to consider expanding the screening technology pilot program in order to provide small businesses with additional options that don't involve expensive equipment. Now, it is my understanding that proposals have been submitted for pilot programs that would assist in developing certification standards and testing of privately trained explosive detection canines.

I believe that enabling private canine companies to be certified would be of great assistance to you as you move towards this 100 percent cargo screening. That is certainly in keeping with the remarks of Mr. Buswell both about the value of dealing with the pri-

vate sector and this notion that now we need to profile puppies as we move more into this area.

It is my understanding that a development of these standards and scheduling of the pilot program have been stalled at DHS. It has been out there. You have had the information. Nothing seems to be happening. So I wonder if there is an explanation for this delay, because it wouldn't involve the kind of testing that Dr. Hallowell has mentioned, and what perhaps is the timeline for the completion of the certification project that—moving forward.

Mr. KANE. Congresswoman, I apologize. I am just not qualified to talk on the canine subject. I know those discussions are going on. It is a TSA issue, so I will save my S&T colleagues here. If I could take something for the record but if we could take something and get back to you, I would greatly appreciate that, because I just don't have the knowledge to answer that.

Ms. TITUS. Madam Chairwoman, would that be all right? Could we ask them to submit an answer to my question here shortly?

Ms. JACKSON LEE. Absolutely.

If you would, respond to the gentlelady's question and inquiry.

Mr. KANE. Yes, ma'am.

Ms. TITUS. Thank you very much. I yield back.

Ms. JACKSON LEE. On this very point, let me just to finish some questioning, but to make the point, several Members have asked what potentially may be classified inquiries, so I am going to ask the staff to set up a classified briefing on in particular the new screening equipment, body scan, other analysis that you are using in terms of airport selection and all of their intended practices around this new effort.

To that point, Mr. Kane, I am going to be interested in your analysis. I would like to track what Mr. Austria said. I was a little aghast that New York was not on the list and further aghast that Texas was not on the list. You have no Southwest representation, and those airports, many of them are international. So do you have any response regarding Texas?

Mr. KANE. I don't, Madam Chairwoman, at this time. I would be happy to offer the full brief on how we came to the airports we have and any of the classified information that we could discuss in closed session.

Ms. JACKSON LEE. Oh, I don't want you to give classified information today, but as you indicated to Mr. Austria that New York will be on the list, what are your plans for—do you have any way of projecting that Texas will be on the list?

Mr. KANE. Well, I can tell you Cat-X airports are certainly going to be on the list.

Ms. JACKSON LEE. I am sorry. Pardon me?

Mr. KANE. The largest airports will be on the list, and that is why I can speak to New York. I don't have that list, and I don't have the full knowledge of exactly what is on the list at this point for some of the other airports.

Ms. JACKSON LEE. Well, I think, without slighting any of my fellow cities, I think you might find DFW and IAH on the list of large airports.

Mr. KANE. Yes, ma'am.

Ms. JACKSON LEE. So I would suspect, if that was a fact, that you would expect to see Texas airports on the list?

Mr. KANE. Oh, yes, ma'am. I just don't know all Texas airports, but, yes, the large airports in Texas would certainly be on the list.

Ms. JACKSON LEE. All right. That is very important to many of us, who are well aware of the different security assets that are in these areas, meaning particular entities that pose some danger. So we want to make sure that you have that broad breadth of analysis.

Let me just do two questions here to Mr. Lord.

I submitted to the record a statement of the president of the NTEU, and I don't know if you heard my question. It is represented that the training that is going on on technology is being done by computer. So I guess if I am sitting in the airport in Arizona and I am a TSO or the airport in Houston and I am a TSO, I go to a computer and learn.

With this new technology give me your assessment of the preferable mess of the human training, actual teacher that goes out and allows a question-and-answer period, the hands-on training. This is a very important issue for us, and I think it plays into the combination of man and machine, a woman and machine. Mr. Lord.

Mr. LORD. I understand the question. Unfortunately, I am not going to be able to opine on this. What I have evaluated, the content of the training and collecting a little more information, I think it is important to point out our own agency. We provide our employees with a mix of on-line training as well as self-taught training and teacher-led instructor training.

So my own agency uses a mix of tools, so I would have to find out a little bit more about the curriculum and what is actually being offered.

Ms. JACKSON LEE. Of course, the task of your agency and the task of security officers are somewhat different. Can we pass you then—I would like to add the request to the GAO for the analysis of the training, particularly as it relates to security training and in this instance the equipment that is under consideration at this hearing.

Mr. LORD. We would be glad to take a look at it.

Ms. JACKSON LEE. We would like you to do that.

Dr. Hallowell, then, let me add to the point that Chairman Thompson made. Are you all sensitive to the problems that small businesses have with the review of their inventions? The time is sometimes is the death of inventiveness in terms of the funding, in terms of what they do next. They are waiting on an answer.

As you do that, let me put into the record a statement by Mr. James P. Middleton, CEO and president, Secure Global Logistics, Houston, Texas.* His testimony—let me make a very strong statement of appreciation for the work that they do. They happen to be a CCSF, and we are just acknowledging so many small companies that are now engaged in serving their country by being a CCSF, and they had to obviously get the approval.

But the point is how are you being sensitive to these smaller companies and the slow process of S&T?

*The information was not available at the time of publication.

Ms. HALLOWELL. Yes, ma'am. We are very sensitive to small businesses. Our doors are open for people who think they have technology solutions. Particularly in the R&D part of test and evaluation, we are happy to work with every and all.

However, when you go down the R&D pipeline, you get to the test and evaluation portion associated with TSA acquisition, there are certain requirements such as the ability to turn out multiple copies of a configuration control device that sometimes small businesses do have problems with. I don't know that we can help with that part of it.

Ms. JACKSON LEE. Okay. Can you stop for a moment? I think all the small businesses that I hear from are asking us can you just tell us whether or not S&T has approved it? I know there are other steps, and certainly I think those are appropriate steps, which is can you produce the product? But can we have the first step of having the analysis of S&T so we know whether it is a viable product? That is where the holdup is. If there is a second tier of holdup, we will address that. But why is the S&T taking so long?

Ms. HALLOWELL. I don't know that I have encountered a situation where we have had trouble accommodating somebody that came in, because typically we will meet with them, we will find out whether or not the concept is feasible, any data, and we can bring it to the laboratory.

The snafu typically comes when a company offers a product that sees some subset of the larger mission space of IEDs that need to be detected, and that is frustrating. We can only help them by trying to help them mature the technology. But our door is open.

Ms. JACKSON LEE. But are you also assessing the validity of the technology?

Ms. HALLOWELL. Yes, ma'am. What we typically do is evaluate the sensitivity of it and the number of threats it can detect and give them a read as to whether it is getting close to something that is viable in terms of some acquisition plan, because I think that is where everybody ultimately wants to go, is to be able to provide a solution.

Ms. JACKSON LEE. Right. Well, let me quickly move on and just ask you to present this to us in writing again. Maybe we need to be better informed. Give us your step-by-step ABC of the XYZ small business, minority-owned business, woman-owned business, or business coming into S&T and from A to the completion. Let us try to see if we can understand that. Then we can interact with you.

We think there is a bump in the road, if we are continuing to hear across America that complaint about backlog, not being able to get through. Let us see how we can work together on that. So I would like that. I really would like that as expeditiously as possible, maybe preceding us going into a classified briefing.

Ms. HALLOWELL. Yes, ma'am.

Ms. JACKSON LEE. Let me finish with Mr. Kane.

I indicated—I hope I was heard, but I am asking unanimous consent to submit into the record testimony of Secure Global Logistics. But I do want to say that one of the testimonial points that was made is the economic challenge, the financial burden of purchasing expensive screening hardware, maintaining it, upgrading it, train-

ing of staff, maintaining facility security, and all the other obligations that go with being a front-line screening partner with TSA.

Now, we in the Federal Government established this relationship of a CCSF. Is there any effort to provide some financial support for the purchase of this equipment through TSA? Any thought about that? Any way we can think about that?

Mr. KANE. Madam Chairwoman, I know we initially for some of our pilot programs, we have provided fundings for some of the freight forwarders. We don't have anything in the budget right now to continue anything like that forward that I am aware of—certainly, not within my programs. I don't oversee that air cargo policy program, but I am unaware of any in TSA's budget to continue to any of that funding.

Ms. JACKSON LEE. Would you take the inquiry back to TSA and the appropriate persons for a response on whether or not that is something that we can project into the future? We are establishing more of these. We are asking more of these shippers. We are all moving toward 100 percent cargo inspection. We are moving it off airports into these CCSFs, and I think we need some kind of response as relates to a partnership.

Mr. KANE. Yes, ma'am. I will take that back.

Ms. JACKSON LEE. All right.

Let me thank all the witnesses. I think——

Mr. DENT. Could I make a comment, Madam Chairwoman?

Ms. JACKSON LEE. Yes, you certainly may.

Let me yield to the gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Just a real quick comment. Mr. Kane, when you provide that information to the Chair on the airports that will be receiving the AIT machines, could you share that with us as well?

Mr. KANE. Yes, sir.

Ms. JACKSON LEE. It will come to the committee, and we will share it with you.

Mr. DENT. I just wanted to make sure we are all going to get that.

Mr. KANE. Whatever the appropriate process is, I will endeavor to follow. Yes, sir. It will be writ large. It is sensitive information, you know, when you see a schedule, and so I know it is a little frustrating, but that is why you saw those first 11 announced, because pretty soon they will show up in the airports. There is no secret there anymore. But writ large, what we do in terms of deployment we do consider sensitive, because it does offer opportunity to see where we are in there.

Ms. JACKSON LEE. We will work through the staff, and they will appropriately handle the material that you are submitting to us. We do appreciate the sensitivity.

Mr. KANE. Yes, ma'am.

Ms. JACKSON LEE. I am sorry. I asked Mr. Lord, who is going to look at it, but I just want to make sure you are aware of the concern about on-line training for this sensitive equipment. Let me raise a concern that I would like to see a movement toward teacher on-site training.

Mr. Kane, do you have any response to that?

Mr. KANE. Yes, thank you for that opportunity, because I didn't have one earlier. But we absolutely have a robust Nation-wide roll-

out plan, and we are sending people to the sites to do the training. It does involve simulator training, but it is a 3-day training program, or almost 3 days. It does include some simulator training, but it also does include on-the-job training as well. So absolutely it is not just going to be a simulator training.

One of the very early lessons learned when we first put AIT out into the field as part of that original pilot was it has to be a great training program, and you really have to focus on those image operators to make the technology successful.

Ms. JACKSON LEE. Well, I hope the TSO officers across America have just heard you make that pronouncement. We will be monitoring that rollout and those faculty members that you will be sending out. I will burden you with another request. Please give us a report on how that is proceeding and when you expect to complete the training even as you do the rollout.

Mr. KANE. Yes, ma'am. It will be an on-going training process as we roll out. We will certainly submit you that report, and it is—obviously it is important to us to have some of those metrics of how successful we are as we roll that technology out.

Ms. JACKSON LEE. Let me thank all the witnesses for their testimony and as well to make the point that I made earlier that your testimony is enormously valuable and as well that we will hope if you have additional material that you would like to submit into the record, we would ask that you would provide that to the staff.

As I see that there are no further questions for our first panel, I thank the witnesses for appearing before us today. Members of the subcommittee may have additional questions for you, and we ask that you respond to them expeditiously in writing.

We now welcome our second panel to the witness table. We understand that because the panel has expanded, we will need to provide additional microphones, so we will take just a moment to get that done.

Thank you again for your testimony today.

[Break.]

Ms. JACKSON LEE. I welcome our second panel of witnesses. Our first witness is Mr. Kevin Dunlap, director of security at the International Air Transport Association. He is responsible for planning and executing the North American aviation security strategy of the association on behalf of 230 global airlines. Mr. Dunlap will discuss security procedures at foreign airports and the role of DHS.

Our second witness is Mr. Charles Barclay, president of the American Association of Airport Executives. Mr. Barclay will discuss how DHS interfaces with airports and how the roll-out of the new security procedures and technologies impacts airports.

Our third witness is Mr. Eric Potts, interim aviation director of the Houston Airport System. Mr. Potts will be able to discuss how DHS strategies and policies with checkpoint security have impacted the airports specifically.

Our fourth witness is Mr. Marc Rotenberg. Mr. Rotenberg is executive director of the Electronic Privacy Information Center. Mr. Rotenberg will provide perspective on how developments in screening procedures and technologies may impact privacy rights. Mr. Rotenberg teaches information privacy law at Georgetown Univer-

sity Law Center and has testified before Congress on many emerging privacy and civil liberties issues.

Our fifth witness, invited by the minority, is Mr. Brook Miller, vice president for government affairs at Smiths Detection. Mr. Miller will discuss his firm's interaction with the Department as it has developed screening technologies.

Our sixth witness, also invited by the minority, is Mr. Mitchel Laskey, president and CEO of Brijot Imaging Systems. He, too, will discuss his firm's interaction with the Department as it has developed screening technologies.

Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize your statement for 5 minutes, beginning with Mr. Dunlap. If any of you desire to take a shorter period than 5 minutes, we would take up your time in questioning. We do expect votes to ring, and we want to give the witnesses their time both in testimony, but also in questioning.

I would also like to acknowledge the presence of Mr. Lungren of California, a Member of this committee.

Thank you. Thank you for your presence here. My statement earlier was that all of us in this room are committed to the security of America, and your presence here will help us continue to be on the front lines securing this Nation.

If I may, I would like to begin with Mr. Dunlap. We are now asking you to summarize your statement, and you are recognized for 5 minutes.

STATEMENT OF KENNETH J. DUNLAP, DIRECTOR OF SECURITY, INTERNATIONAL AIR TRANSPORT ASSOCIATION

Mr. DUNLAP. Thank you, Chairwoman Jackson Lee, Ranking Member Dent and distinguished Members of the subcommittee. Thank you for the opportunity to testify at this hearing.

The International Air Transport Association, IATA, appreciates the leadership of the subcommittee in addressing this critical issue. It is our hope that today's hearing launches a much-needed international dialogue on the future of passenger screening. IATA and our 230 U.S. and foreign member airlines have a vision of future passenger screening that is based on a paradigm shift in the principles behind checkpoint operation.

We believe that next generation checkpoints must focus on looking for bad people, and not just bad things. I would ask that you consider our vision of an effective checkpoint, which focuses on finding bad people rather than bad things. Passengers are treated with dignity. Babies and children with names similar to adults on the no-fly list pass through screening uneventfully. Toenail scissors and nail clippers do not trigger an interrogation.

In this scenario the airport security checkpoint is no longer the first line of defense, but a second look. The dots are connected by intelligence agencies before passengers reach the checkpoints. Plots are disrupted long before the airport, and screeners look for behavioral clues warranting a closer inspection of the passenger.

The committee is asking today are our airports keeping passengers safe? The short answer to this question is absolutely yes. Today's checkpoints work, and we are not advocating immediately discarding it for a next generation checkpoint. However, the day is

rapidly approaching where the 40-year-old concepts served as the underpinnings of our current checkpoints will become obsolete.

The next checkpoint should rely on several and pervasive passenger observation and detection. We believe highly trained behavior detection officers, who question passengers and observe their mannerisms throughout the screening process, would add a strong layer of detection. Tomorrow's checkpoint would enhance behavior detection by providing screeners with contextual background information on the traveler to assist in the questioning process.

This type of intelligence-based behavior detection would increase both the fidelity and also the objectivity of passenger screening. The system here envisions security for tomorrow's passenger as a road bump in the journey rather than a mountain. We believe the components of this checkpoint are available, but they require the will to be assembled and delivered to our airports.

I would like to say a few words about technology in general. Security and technology are often confused. IATA remains concerned that new technology is being viewed as the silver bullet for the future, but there is no silver bullet. For every technology with exciting detection capabilities, there are complementary vulnerabilities.

Also we must not overlook the process through which technology moves from the laboratory to the airport. Fundamentally, this journey takes too long, it is tainted by challenging and changing regulatory requirements, and it often produces a product which doesn't work in the real world. An unfortunate example mentioned here was the recent failure of the so-called puffer explosive detection machine.

IATA applauds Secretary Napolitano, Chairman Thompson, and Chairwoman Jackson Lee for refocusing DHS to a more forward-thinking and globally oriented department. There are no better examples than IATA's testimony here today and Secretary Napolitano's joint global security summit in Geneva with IATA.

IATA has provided Secretary Napolitano with five specific recommendations to strengthen commercial aviation security. Our recommendations briefly are: Formal consultation with foreign airlines, refining existing TSA emergency orders to better address the international environment, eliminate inefficiencies in the DHS passenger data collection program, strengthen government-to-government outreach to harmonize and coordinate on security issues, and finally, over the long term, focus on developing the next generation checkpoint.

As this subcommittee reviews the events post-December 25, we expect many in Washington will seek short-term fixes to security checkpoints. However, new technology cannot guarantee better security. It cannot detect bad people and is not the only solution for the future. The solution lies in a paradigm shift in how we screen and protect our passengers. Thank you.

[The statement of Mr. Dunlap follows:]

PREPARED STATEMENT OF KENNETH J. DUNLAP

MARCH 17, 2010

INTRODUCTION

Chairwoman Jackson Lee, Ranking Member Dent, and distinguished Members of the subcommittee, thank you for the opportunity to testify at this hearing: "An Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe?" The International Air Transport Association (IATA) appreciates the leadership and the foresight of the subcommittee in addressing this critical issue in the wake of the attempted bombing on Christmas day. It is my hope that today's hearing launches a much-needed international dialog on the future of passenger screening and results in even better screening for this generation and the next. I urge you and your colleagues to seize this opportunity.

IATA represents some 230 U.S. and foreign air carriers and has offices in over 70 countries. IATA's mission is to promote safe and secure air travel. Through our work, we have changed the way people fly around the globe. In fact, your last trip across the United States or across an ocean was touched by IATA. The airline on which you flew most likely participated in the IATA Operational Safety Audit (IOSA). This is an internationally recognized and accepted evaluation system designed to assess the operational management and control systems of an airline. IATA replaced paper tickets with e-tickets which allow you to fly using just your identification and a boarding pass. IATA has enabled passengers to check in at home and to use boarding passes displayed on a Blackberry or PDA through our standard-setting processes and committees.

These initiatives embody one of IATA's core competencies, which is to develop the processes that help passengers and their bags move through airports more efficiently. Through IATA's flagship programs, Simplifying the Business (StB) and Fast Travel, we work to make passenger travel through the aviation system faster and simpler. Through our work in areas such as boarding pass encryption and checkpoint entry lanes, we work to make travel more secure. This experience serves as the foundation for the ideas we are presenting to you this afternoon.

IATA'S VISION OF THE FUTURE

IATA has a vision of future passenger screening that is based on a paradigm shift in the principals behind checkpoint operation. We believe next generation checkpoints must focus on looking for "bad people" and not just "bad things." If we have learned anything from the last decade, it is that a passenger with toe nail clippers is not automatically a threat to aviation.

As the subcommittee reviews the events post-December 25, we expect many may seek short-term fixes to security checkpoints. In fact, some procedural changes may be warranted. However, simply dropping new technology into a checkpoint is not the answer for the future and does not guarantee improved security. Even the best technology cannot detect bad people. This Congress cannot allow calls for new equipment to mask the fact that a long-term change is required for security checkpoints.

Consider our vision of an effective checkpoint, which focuses on looking for bad people rather than for bad things: "Passengers are treated with dignity. Babies and children sharing a name found on the no fly-list pass through screening uneventfully. Toe nail scissors and nail clippers do not trigger an interrogation."

In this scenario, the checkpoint is no longer the first line of defense, but a second look. The dots are connected by intelligence agencies before passengers reach the checkpoints, plots are disrupted long before the airport, and screeners look for behavioral clues warranting a closer inspection of the passenger.

IATA believes the key to this future lies in leveraging all of the passenger information currently collected by a government before the start of the trip. Data collected in the name of customs and immigration needs to be merged with data collected for security. Then this comprehensive data should be analyzed by government intelligence agencies before a "cleared to board" decision is issued. The general results of this vetting should be made known to the screener at the checkpoint who will decide if a more thorough physical search is warranted. This process, combined with advanced behavior detection, would make for a stronger and more efficient checkpoint.

Certainly, all the parts of this notional checkpoint exist today. However, Government and industry need to work together to integrate these elements into a single, useable process. We believe Congress should make this integration a priority.

TODAY'S DEPARTMENT OF HOMELAND SECURITY (DHS)

IATA applauds Secretary Napolitano, Chairman Thompson, and Chairwoman Jackson Lee for refocusing DHS to a more forward-thinking and globally-oriented Department. There are no better examples than IATA's testimony today and Secretary Napolitano's joint Global Security Summit in Geneva with IATA. The industry has noticed this new approach and looks to heightened engagement to make the checkpoint of the future a reality.

RECOMMENDATIONS TO CONGRESS AND TO THE DEPARTMENT OF HOMELAND SECURITY

During our Summit, IATA offered five principles and recommendations to DHS to guide commercial aviation security post-Christmas day. We believe these guidelines apply both locally and also globally. Our five principles include:

1. Define a Risk-based Approach

Aviation security resources in terms of people and funds are limited. Regulators and industry must focus these on the most probable threats to aviation as demonstrated by past threats and future capabilities. This requires that industry and Government work in partnership to identify and to prioritize the threats we expect to face and the responses we expect to implement.

2. Act Globally

Aviation is a globally interconnected enterprise that supports 32 million jobs and $3.5 trillion dollars in economic activity.[1] As such, this global network will only be as strong as its weakest link. Regulators must secure this system with internationally implemented standards and recognize the comparable security measures of other States. Security resources should not be wasted duplicating the efforts of other competent regulators.

3. Regulators Must Share and Be Open to Best Practices

Globally, air transport is more secure than ever in its history. IATA applauds the many States that have raised the bar on their security programs. However, we often see the "not invented here" mentality preventing wider adoption of new and innovative security methods. IATA encourages States to use the International Civil Aviation Organization (ICAO) more effectively on security to develop harmonized security policies and to spread best practices.

4. Work With Industry on Practical Solutions

The best security is based on procedures and equipment that work in concert with the complex operating environment within which global aviation operates. IATA urges regulators to tap into industry experience and expertise to deploy efficient and effective security measures.

5. Act Strategically

Security incidents should not be met with reactive and unilateral Government actions. Often, the most ineffective measures are written immediately following a security breach. Industry and Government must focus on making existing processes and resources even more effective. At the same time we must not be afraid to look at the whole system when we have evidence and technology to support generational change to meet new threats.

Certainly, these are high level principles, but they must form the cornerstone of aviation security policy and be supplemented with specific recommendations. To that end, IATA provided Secretary Napolitano with five specific recommendations to strengthen security in the future. These are addressed to DHS and TSA, but should serve as the foundation for the efforts of other regulators as well. Our recommendations are:

1. Formal consultation with foreign carriers

Regulators must understand that aviation is a globally interconnected enterprise and must write security regulations that reflect this reality. Most often, new rules are written without industry input and review. This deprives the regulatory process of the operational insight and expertise the airline industry can provide. Greater collaboration would ensure more effective and more efficient security measures.

In the long term, consultative public/private partnerships can define and promote a unifying security vision, which can be reflected in National policy. In the short-term, stakeholders can create "playbooks," which respond to threats to aviation proactively rather than reactively.

---

[1] IATA Economics 2010.

IATA believes that industry consultation must be regular, formal, and empowered. Collaboration must be tied into policy, which is then seamlessly tied into regulation. DHS has a stakeholder body known as the Sector Coordination Council (SCC), which attempts to provide a public/private partnership. However, it is neither integrated firmly into security policymaking nor does it include foreign representation. Rarely does the SCC process produce more efficient regulations or more refined National policies.

Finally, we believe other like-minded regulators could benefit from their own SCC-type National organizations. We believe ICAO is uniquely positioned to create a template for such organizations and to promulgate them internationally.

IATA recommends that DHS engage in formal and continuous consultation on aviation security matters with all air carriers through a cooperative and deliberative process. We are asking DHS to:

- Formally establish an international aviation workgroup under the DHS Aviation Security Advisory Committee (ASAC);
- Revitalize and empower the Sector Coordination Council (SCC) to play a definitive role in aviation security policymaking;
- Allow foreign airlines, under the coordination of IATA, to join and participate as full members of the SCC.

2. Refine existing TSA emergency orders to better address the international environment

Airlines operate across the globe under extremely different environments: Laws, infrastructures, and cultural diversity should all be taken into account. Airlines have hands-on experience in these different environments. However, TSA imposes one-size-fits-all measures on international carriers, which often simply cannot be implemented in certain airports, countries, or regions.

Moreover, although DHS is using risk management principles in targeting passengers from a list of 14 States for further screening, we believe the country "blacklist" approach is counter-productive. Our experience with blacklists in the safety field shows they can do more harm than good and can lead to diplomatic actions, such as retaliation. Instead, targeting people for screening should be based on the individual through the better use of passenger data. IATA recommends that DHS:

- Move toward risk-based and "performance-based" regulations, which would be flexible enough in their wording to allow carriers to make sure DHS's objective is reached in a way, which complies with local specificities;
- Make better use of passenger data rather than subjecting passengers from whole States to enhanced screening;
- Increase security focus on high-risk areas of the world instead of relying on one-size-fits-all directives.

3. Eliminate inefficiencies in the passenger data collection process

Under existing U.S. regulation, carriers serving the U.S. market are required to provide extensive data relating to all persons traveling on flights to, from, and within the United States. Whether that information is provided to meet requirements for PNR access, APIS Quick Query (AQQ) or TSA's Secure Flight, the data provided is largely the same. We need the ability to transmit data in a consistent format to a single DHS portal.

As evidenced on December 25, agencies failed to identify the potential threat, even with the provision of vast amounts of personal data at least 3 days before the flight. As indicated in the White House Review Summary to President Obama on January 7, 2009, this failure to "connect the dots" was primarily due to fragmentation within the United States Government and the inability to fully share information across agencies. We advocate deployment of more robust systems within DHS that better analyze and synthesize the data already transmitted to DHS's component agencies. IATA recommends:

- DHS collect a single set of information on each passenger from carriers that can be shared widely and seamlessly among DHS and intelligence agencies.

4. Strengthen government-to-government outreach to harmonize and to coordinate on security issues

The United States takes a different approach from most countries, because it mandates security procedures for incoming flights. The European Union, for instance, takes the stance that it can only regulate flights departing its territory.

The extraterritorial approach to security is problematic, mostly because U.S. requirements can conflict with national norms. One example of this has been the 2005 U.S. requirement for PNR data, which conflicted with EU data privacy directives. A similar example with today's situation is that in many countries, such as Germany, airlines are not allowed to perform physical screening on passengers. If a gov-

ernment were to ask an airline to conduct such screening in Germany, that airline would be caught in the middle and placed in an impossible situation.

DHS should reach out to governments around the world before imposing new extraterritorial procedures on the airlines. One way to do this would be to make full use of ICAO's Aviation Security "Point of Contact" network. This would allow DHS and TSA to evaluate whether a new procedure is feasible at the world's airports. It would also increase the readiness of countries to assist airlines in complying with U.S. requirements.

5. Over the longer term, focus on developing a next generation checkpoint

The December 2009 Detroit incident demonstrates that in the future aviation may need smarter and faster, next-generation passenger screening measures to confront new and emerging threats. While our current screening systems are serving us well, their underlying operational concepts and architecture are beginning to show their age, and they need to be replaced.

IATA is asking DHS to begin to look forward to field a new checkpoint. In the interim, we need to enhance the capabilities of the current system to extend its useable lifetime and increase its detection capabilities.

IATA recommends to the Department of Homeland Security (DHS) that this effort be accomplished in close cooperation and partnership with industry. Stakeholders at the highest level must develop an integrated vision and a road map for moving forward.

PRINCIPLES OF NEXT GENERATION SCREENING

The subject of today's hearing is, "An Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe?" The short answer to this question is absolutely, "yes." The American public needs to understand that their security is the utmost concern of the airlines on which they fly and the airports in which they transit. Twenty-four hours a day, 365 days a year, professionals are standing watch to ensure their security. The procedures, processes, and technology deployed since 9/11 have made this industry the most secure in its history.

Yet, those who would do us harm by injuring innocent passengers and by disrupting our economies are not standing still, and neither should our checkpoints. Today's checkpoint works and we are not advocating immediately discarding it for the next generation checkpoint. In fact, there is still service life left in these checkpoints. However, the day is rapidly approaching where the 40-year-old concepts which serve as their underpinning will become obsolete. As Congress discusses novel drop-in technology for checkpoints, we believe it is essential to not mask the need for a new philosophy behind checkpoint architecture. For these reasons, we urge Congress to launch the process to build a next generation checkpoint capable and flexible enough to handle new and emerging threats to air transport.

We recommend that the next generation checkpoint be based on intelligence and supported by technology. Screening would consist of looking for bad people rather than bad things. We believe the volumes of passenger data currently collected by governments could be leveraged to make decisions about boarding pass issuance long before a passenger arrives at the airport. However, unlike today, the next generation checkpoint would require the U.S. Government to:

- Align passenger data collections programs within DHS and between DHS and other departments;
- Screen passenger data more thoroughly against intelligence information and law enforcement data;
- Develop a "red flag" system, which would objectively identify the level of screening a passenger would require before boarding.

The next checkpoint should also rely on thorough and pervasive behavior detection. We believe highly trained behavior detection officers who question passengers and observe their mannerisms throughout the screening process would add a strong layer of detection. Tomorrow's checkpoint would enhance behavior detection by providing screeners with contextual background information on the traveler to assist in the questioning process. This type of intelligence-based behavior detection would increase both the fidelity and also the objectivity of screening.

Screening technology supports intelligence in the next generation checkpoint by providing screeners with enhanced baseline methods for identifying explosives and firearms. This equipment would be in the primary screening lanes through which all passengers would quickly pass with little interruption. Additionally, the checkpoint would have enhanced lanes designed to inspect those passengers of whom little is known or of whom questions are raised, most likely at a slower rate with more fidelity.

The system described here envisions security for tomorrow's passenger as a road bump in the journey rather than a mountain. We believe the components of this checkpoint are available, but they require the will to be assembled and delivered to our airports.

Security and technology are often confused. IATA remains concerned that novel technology is being viewed as the silver bullet for the future. However, there is no silver bullet in security. For every technology with exciting detection capabilities there are complementary vulnerabilities, which can be open to exploitation. We urge this subcommittee to challenge technology advocates to fairly assess capabilities against vulnerabilities.

Finally, we must not overlook the process through which technology moves from the laboratory to the airport. Fundamentally, the journey takes too long, and it is tainted by changing regulatory requirements, often producing a product which doesn't work in the real world.

Promising technology needs to pass the O'Hare test before it leaves the lab: It must perform its functions reliably and accurately under the same passenger load it would experience at O'Hare the day before Christmas. Perhaps such a test would have kept the explosive puffers purchased by the TSA out of long-term storage.

CONCLUSION

The security and safety of the flying public is the top priority of IATA and the aviation industry as a whole. The procedures, processes, and technology deployed since 9/11 have made this industry more secure than ever before. However, there is a clear need for continued vigilance and constant revision to ensure an even more secure future. Regulators worldwide must focus on improving intelligence communication and passenger screening programs in order to stay one step ahead of those whom would wish harm on our passengers.

As the subcommittee reviews the events post-December 25, we expect many will seek short-term fixes to security checkpoints. However, new technology cannot guarantee better security, cannot detect bad people, and is not the only solution for the future. Any new equipment must be fully vetted in the operational environment and justified in fulfilling a clear need and producing a clear enhancement at the checkpoint. Overall, we urge Congress to promote long-term improvements to intelligence coordination, to interdepartmental cooperation, and to security checkpoints in order to achieve the highest level of security for the flying public.

Ms. JACKSON LEE. Mr. Dunlap, let me thank you for your testimony.

I now recognize Mr. Barclay to summarize his statement for 5 minutes.

STATEMENT OF CHARLES BARCLAY, PRESIDENT, AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

Mr. BARCLAY. Thank you, Madam Chairwoman and Members. It is always a privilege to be here before the committee.

I will make just four very brief points from our testimony. First is that airport executives support the deployment of AIT, and we commend the efforts of the leaders of DHS and TSA in both the decision-making and the consulting with industry here in Washington.

Second, while we are complimentary of their sincere efforts to coordinate with us and do as much planning as they can here in Washington, there is still a great need for consultation and getting the agreement of individual airports at each location. We have learned that the hard way from the deployment of that baggage screening technology from 2000 to still today that there is no substitute for the specific individual airport knowledge blueprints don't give you as far as getting these installations actually done. We would recommend strong consultation language aimed at TSA for all these deployments.

Third, DHS needs to budget realistically for these deployments. The true costs of the installations do include the terminal modifications and terminal space that is going to be necessary, certainly, in some locations. We think they have done a lot of planning, and they are sincere in trying to find locations where they can do the initial installations without a great impact on those locations, but we know that they are going to run into places where there will be significant modifications. Again, with the experience from baggage screening, this is going to be an expensive alteration in a number of locations, and we think those costs have to be covered by the Department and included in their planning.

Then finally, airport executives continue to be concerned about throughput. As the economy comes back, passenger numbers go back up. We realize they are doing the planning on throughput of these systems. We continue to be concerned that all of that proves out realistically in the real world, and we think we have got, as was mentioned by the previous witness, we have got to make the screening process one that considers both security and the efficiency of transportation. Speed is what we are all about in this business, and we need to provide good customer service as well. So we hope we will keep our eye on those throughputs. Thank you.

[The statement of Mr. Barclay follows:]

PREPARED STATEMENT OF CHARLES BARCLAY

MARCH 17, 2010

On behalf of the American Association of Airport Executives (AAAE) and the thousands of men and women the Association represents who manage and operate primary, commercial service, reliever, and general aviation airports across the country, I want to thank the subcommittee for the opportunity to participate in this important hearing to assess passenger security checkpoints. Airport executives appreciate your interest in this topic, and we are eager to work with Congress, the Department of Homeland Security, and the Transportation Security Administration to ensure the success of on-going efforts to upgrade the equipment and protocols in place at screening checkpoints across the country.

While responsibility for passenger and baggage screening are by law the sole responsibility of TSA, airports play a critical role in partnering with the agency to help it meet those core missions. The significant changes that have taken place in airport security since 9/11 have been aided dramatically by the work of the airport community, and we look forward to continuing to serve as a partner to the agency as it seeks to upgrade its checkpoint capabilities in the wake of the attempted Christmas day attack on Flight 253.

In addition to partnering with TSA to help the agency meet its passenger and baggage screening mandates, airports as public entities with public safety as a key mission, also perform a number of inherently local security-related functions at their facilities, including incident response and management, perimeter security, employee credentialing, access control, infrastructure and operations planning, and numerous local law enforcement and public safety functions. These critical public safety duties have long been local responsibilities that have been performed by local authorities in accordance with Federal standards under Federal oversight. Airport operators meet their security-related obligations not with an eye on profit or loss but with a sharp focus on the need to secure public safety, which remains one of their fundamental missions.

With that as background, let me begin by complementing DHS and TSA for their swift response to the attempted Christmas day attack and for the efforts undertaken since that time to engage airports on charting a course forward—particularly as it relates to the wide-scale deployment of Advanced Imaging Technology (AIT) at airport checkpoints. As the subcommittee is well aware, the agency has greatly expedited plans to deploy AIT equipment, with some 500 machines expected to be deployed by the end of 2010 and another 500 scheduled to follow in 2011. Many airports are eager to have AIT equipment in their facilities in recognition of the secu-

rity benefits this technology provides in detecting threats highlighted by the Christmas day attack.

DHS Secretary Janet Napolitano, TSA Acting Administrator Gale Rossides, and the senior leadership at the Department and at TSA have made concerted efforts to include AAAE and other industry groups in discussions regarding AIT deployment plans and to seek airport input on how best to move forward. In particular, I want to complement and thank TSA Assistant Administrator Robin Kane, who is testifying today, for his practical, results-driven approach and for his efforts to seek input from airport management at key stages in the initial planning process.

AIRPORTS ARE CAUTIOUSLY OPTIMISTIC ABOUT AIT DEPLOYMENT BUT HAVE CONCERNS

Airport executives are encouraged by these early outreach efforts on AIT deployment and commend the agency for the thorough work that has been undertaken to this point with general checkpoint designs and deployment strategies. While careful planning at headquarters is certainly important, the greatest challenges lie ahead as TSA attempts to move from the drawing board to the "real world" at hundreds of widely divergent airport facilities across the country with the deployment and operation of AIT equipment.

Beyond the limited number of airports that currently have or are scheduled to soon receive AIT equipment, TSA's outreach efforts have not yet been widely extended to individual airports to discuss specific plans for deployment of equipment at their facilities, leaving many airport executives with significant concerns about potentially costly structural modifications that may be necessary to accommodate AIT equipment in already crowded airport terminals. Additionally, airports have questions about the ability of TSA to efficiently process passengers through updated checkpoints given the size of the new machines, the number of TSA personnel required to operate them, the slower throughput levels of the machines relative to existing magnetometers, and significant changes to divestiture procedures for passengers. These challenges will become more acute as passenger levels continue to rise at airports across the country.

To this point, TSA maintains that there will be minimal impact on the checkpoint footprint and on passenger throughput levels through screening checkpoints—particularly at the airports slated to receive the 500 machines scheduled for delivery during 2010. Airport executives believe that TSA is earnest in its view that it has considered these issues, and we readily acknowledge that there won't be significant challenges at every airport. With that said, it is evident that placing new equipment, building image viewing rooms, and accommodating teams of new personnel in already crammed checkpoint screening areas will be difficult if not impossible at some critical airports across the country. TSA has acknowledged that the agency will face challenges, particularly in 2011, as they move toward the end of the deployment schedule.

Unfortunately, TSA has yet to begin planning to tackle some of these issues, which we believe are inevitable. Looking forward to 2011—the budget year that Congress is currently considering—the agency has requested significant resources to procure and install AIT equipment ($215 million) and to support the additional 5,355 TSO positions the agency says are necessary to operate the AIT machines ($315 million). The administration has not, however, requested funding to pay for either the space or terminal modifications that may be necessary at airports to accommodate AIT equipment. Administration officials have made clear their view that airports should be required to pay for some if not all of these costly items.

PREVIOUS EFFORTS ILLUSTRATE THE IMPORTANCE OF AIRPORT INVOLVEMENT AND FEDERAL FUNDING

To understand the pitfalls of moving forward with the wide-scale deployment of technology in the airport environment without adequate airport consultation at the local level and in the absence of sufficient Federal funding, one need only to consider the experiences with TSA's roll-out of explosives detection systems (EDS) for checked baggage earlier this decade. Insufficient airport involvement at individual facilities with the planning, design, and deployment of that equipment and a lack of Federal funding to support critical project elements led to "temporary" solutions at numerous airports with bulky machines being placed in crowded airport terminal areas—a situation that created numerous safety, security, and efficiency issues. As the subcommittee knows well, we've spent the better part of the past 8 years trying to clean up the mess at great expense, and we still don't have it right in many locations.

Airports have seen this movie before, Madam Chairwoman, and we don't like the ending. The good news is that we are at the beginning of the AIT deployment proc-

ess with the opportunity to get it right this time around. Along those lines, we offer several specific recommendations for your consideration:

Give Airports a Direct Role in Developing and Approving AIT Deployment Plans.—Airports have long supported the expedited deployment of advanced technology as a means of enhancing security and efficiency, and airports are generally enthusiastic about the deployment of AIT equipment at their facilities. Airports also believe strongly that individual airport authorities must be actively involved in the planning and design of projects at their facilities to ensure upgrades are completed in a timely manner and in a way that limits disruptions to checkpoint operations and costly terminal modifications.

Airport professionals have a unique understanding of their facilities and should be counted on as a resource as TSA seeks to deploy technology at checkpoints or other areas of an airport. In addition to their expertise as facility managers, airport professionals share the same public safety mission as the Federal Government and should be relied on as a full partner in these efforts.

In recognition of those facts and in an effort to ensure that the consultation and airport involvement at the local level is meaningful and productive, we encourage the subcommittee to consider giving airport authorities a direct role in developing and approving deployment plans at their facilities. Such a move will ensure that TSA and its contractors are working directly with airports to establish realistic plans that take into account unique facility and operational considerations. Careful coordination and cooperation between the Federal Government and airport operators is the key to the successful deployment of technology in the airport environment.

Require TSA to Pay for Space & Terminal Modifications Necessary to Accommodate AIT.—Not surprisingly, airport executives are very concerned about a lack of Federal funding to support the acquisition of space and costly terminal modifications that will likely be necessary to accommodate AIT equipment in numerous airport locations. As all of you know as frequent travelers, many airport terminals are already at their breaking point in terms of space, and adding bigger machines, personnel, and image viewing rooms—among other necessary changes—will likely require significant terminal modifications.

Given the acknowledged importance of these projects to National security, airport executives believe that it is imperative that the Federal Government step up to the plate to finance necessary space acquisition and terminal modifications required to accommodate AIT equipment. The current assumption that airports should be responsible for those significant expenses ignores reality.

Setting aside the fact that passenger and baggage screening are the direct responsibility of the Federal Government, airport financing simply isn't feasible at most airports—many of which have already deferred major capital projects because of economic realities. Plowing new resources into helping the Federal Government meet its obligations in this area would take even more money away from critical safety and capacity-enhancing projects and put an additional burden on our partners in the airline industry for an item that everyone acknowledges is necessary for homeland security. I would also note that airports collectively have already invested billions of dollars over the past decade on a number of important security improvements at perimeters and throughout the airport environment and to assist TSA in its passenger and baggage screening efforts.

In our view, Federal funding for space and terminal modifications are unlikely to materialize without support from Congress. That fact is evident to us based on budget documents and recent discussions with key Department and agency leaders. With that in mind, we urge the subcommittee to push for changes requiring TSA to pay for these critical project elements. Without adequate Federal support, we face a situation where deployment decisions could be based on where machines can be accommodated easily in airports as opposed to where they make sense from a security perspective.

It is worth noting that in the case of checked baggage systems, TSA acknowledged the problems that a lack of Federal funding would create with its deployment plans and initially supported paying for terminal modifications and other costs through a multi-year letter of intent (LOI) process that was created with the strong support of Congress. Unfortunately, the important LOI program was opposed by the Office of Management and Budget, and an important tool in financing projects was left unutilized—a result that slowed the deployment of in-line baggage systems at airports across the country. Those experiences illustrate the importance of placing a provision in law that requires TSA to pay for space and terminal modifications in airports necessary to accommodate AIT equipment.

Proactively Address Passenger Throughput Issues.—One of the biggest concerns that airport executives have with the wide-scale deployment and utilization of AIT

equipment is passenger throughput levels. While wait times at screening checkpoints are currently manageable in most cases, airports see a potential storm brewing with new equipment, new divestiture procedures, and steadily increasing passenger levels as the economy recovers.

Airport executives question the optimistic assumptions that TSA has made in this area, and we urge the agency to begin serious contingency planning to deal with slower processing times and increasing passenger levels. Airports have long supported the establishment and adherence to specific wait time thresholds at airports and believe that this important tool—which TSA no longer measures—should be reinstituted.

On the throughput issue, airport executives have placed a great emphasis on TSA efficiency to improve the experience of passengers at airports. Improved customer service is clearly an important consideration. In our view, however, improving the efficiency of the screening process goes hand-in-hand with the goal of enhancing the security and safety of airport facilities and the aviation system. Long lines and poor customer service do not equate to better aviation security. To the contrary, long lines in airport terminals and at security screening checkpoints are targets for terrorists as past experiences prove.

Long-term, Focus Must Move Beyond Finding Dangerous Things.—It is clear that terrorists continue to focus on commercial aviation as a primary target and that the threats are evolving at an increasingly rapid pace. As local airports and DHS continue to work together to address these emerging novel attacks, it is a well-established imperative that the Federal Government maintain an active pipeline of the latest innovative technologies to stay a step ahead while supporting a healthy and efficient aviation system. However, our collective detection, deterrence, and response capabilities, as advanced and accurate as they are, will only take us so far as we attempt to combat a new generation of terrorists and methods apparent in the attempted Christmas day attack.

Looking forward, we must continue our efforts to focus on identifying dangerous people in addition to dangerous things. With the deployment of AIT equipment at numerous airport locations, we have virtually reached the limits of our ability to identify dangerous things at screening checkpoints. While additional detection capabilities are certainly critical, we must also seek to do ever more to identify those who intend to do our aviation system and Nation harm and to continue to develop a broad array of approaches to subject potential threats to additional scrutiny. Similarly, we must do more to better align security resources to address appropriately those in the traveling public that pose little threat to the system.

Part of the answer in the long-run is to integrate into a seamless approach the many security tools at our disposal that operate now largely in isolation. It is no longer enough for TSA to research and deploy new physical threat detection technologies, vet traveler's backgrounds against terrorist databases, and unpredictably screen and observe travelers in terminal and gate areas. While these programs have made us more secure over the past 8 years, the fact that they currently operate largely independent of each other creates limitations. Ultimately, we must tie all of these tools together to create a more targeted application of screening processes and a true risk-based approach.

We look forward to working with the subcommittee as efforts in that regard continue. Again, I appreciate the opportunity to participate in today's hearing and look forward to answering any questions you have.

Ms. JACKSON LEE. Thank you for your enormously important and succinct testimony. We look forward to exploring those points.

It is my pleasure now to yield to one of my neighbors in Houston. Colonel Eric Potts is the interim director of the Houston Intercontinental Airport. As he well knows, I am always going to make note of the fact that he served 27 years in the United States Army, retired as a colonel with a number of merit recognitions for his service to this Nation.

Colonel Potts, you are yielded 5 minutes for your testimony.

STATEMENT OF COL. ERIC R. POTTS (RET), INTERIM AVIATION DIRECTOR, HOUSTON AIRPORT SYSTEM

Mr. POTTS. Good afternoon, Madam Chairwoman and Members of the committee. Thank you for inviting me today to testify.

The Houston Airport System is the fourth-largest multi-airport system and the Nation and the sixth-largest in the world. Our flagship——

Ms. JACKSON LEE. Please turn your mic on, Colonel Potts.

Mr. POTTS. Start over—domestic and international passengers. It is the Nation's eighth-largest passenger airport, and the world's 16th. In 2009 our airports in Houston served approximately 48 million passengers, and projections show about 80 million passengers by 2020.

We generate 151,000 regional jobs and contribute over $24 billion to the local economy. Houston is also a DHS-designated Tier 1 Urban Area Security Initiative city. According to the 2007 regional threat and vulnerability assessment, IAH is the highest at-risk asset in the entire Southeast Texas area. Given that the Houston metropolitan area has the Nation's fourth-largest population and is home to the essential elements of our energy supply and refining capacity, effective passenger screening at our airports is one of our top priorities.

There are four key points I want to share with you today. First, let me say that over the past 8 years we have seen many improvements to the aviation security improvements. We work closely with our Federal counterparts in the Department of Homeland Security and the Transportation Security Administration. It is a partnership we value greatly.

For example, in Houston we have recently partnered with TSA to implement explosive detection system baggage screening solutions in both the major airports, IAH and William P. Hobby. We are also actively working with the TSA on the airport surveillance program, a project which provides funding for the enhancement to the airport's existing closed-circuit televisions and related reporting systems. The TSA is preparing to implement full body scanning equipment at both IAH and Hobby.

But major impediments remain that need to be addressed, and soon. It is on these issues that I want to ask for the assistance today because, as you know, while the Federal Government plays a key role in airport security matters, Federal law imposes the responsibility of local airport operations for securing the National aeronautical domain, the NDA, within their particular regions.

We have identified impediments that could be minimized by the procurement of security technologies and the institution of certain Federal initiatives relative to intelligence sharing, risk assessment, and in critical infrastructure protection fielded, based, aviation security compliance technology.

Then there is the issue of the costs associated with the measures of our first priority in ensuring effective passenger screening is the lack of timely and consistent dissemination of National threat intelligence information to airport security directors.

In Houston we have more than 200 security personnel. They are on the ground and on the front lines and yet, despite high-level clearance, they generally do not receive intelligence sharing from the Federal counterparts to the degree and in a timely fashion that will allow them to take desired proactive approaches.

Part of the reason for this gap is the absence of appropriate secure technology. To correct this, certain technologies must imme-

diately be made available to the local airport security directors. This includes security terminal equipment telephones, a secure fax, and connections to the Homeland Security data network and the secret internet protocol router network.

The lack of intelligence sharing is further exacerbated by the fact that there is no current Federal standard for utilization of the risk assessment methodology across the air domain. What is needed is a National intelligence lead risk-based security doctrine that targets the mitigation of and vulnerabilities in a proactive and recurrent fashion.

To close the loop and begin the benefits of good, timely intelligence information and uniform risk assessments into the field, we also need the prompt implementation of uniform, new field-based technologies which capture raw data by security area, category, and department.

The final point I would like to make is that the close attention needs to be paid to ensuring that the necessary funding accompanies these and other new measures. For example, we are encouraged by the TSA's recent announcement of its plan to install advanced imaging technology, AIT, at security checkpoints to replace current walk-through metal detection devices.

Unlike metal detectors, AIT can detect prohibited items that have little or no metallic content, and AIT will also allow passengers with surgical implants to avoid the invasive physical patdown inspections that come with walk-through metal detectors.

In addition to the terminal modifications, we are concerned about the throughput time that may be required to process passengers through AIT units as opposed to the time it takes to process them through walk-through metal detectors. TSA has said that they can process a passenger in 15 seconds. Some airports that already have the units at these checkpoints have said that in reality it can take as long as 45 seconds to process one passenger.

So with that, thank you, Madam Chairwoman and committee Members, for the opportunity to testify before you. In terms of priorities, I would like to conclude by asking the committee to focus on intelligence sharing matters first, the identification of particular risk assessment methodology second, and the technology base compliance program to follow.

Finally, please remember that the fragile state of the aviation industry today cannot sustain the financial impact that the implementation of overall security strategies will require. The burdens fall primarily on our Nation's airports, and considerable additional resources are required.

Ms. JACKSON LEE. Colonel, if you can wrap up, I appreciate it.

Mr. POTTS. I would ask the Congress not to impose any further unfunded mandates on either the commercial aviation industry or the local airport operators that are the cornerstone of the industry. Thank you.

[The statement of Colonel Potts follows:]

PREPARED STATEMENT OF ERIC R. POTTS

MARCH 17, 2010

Good afternoon, Madam Chairwoman and Members of the committee. Thank you for inviting me to testify today. The Houston Airport System is the fourth-largest

multi-airport system in the Nation and the sixth-largest in the world. Our flagship airport—George Bush Intercontinental or "IAH"—is one of the country's largest gateways for both domestic and international passengers. It is the Nation's eighth-largest passenger airport, and the world's 16th-largest. In 2009 our airports in Houston served approximately 48 million passengers, and projections show some 80 million passengers by 2020. We generate some 151,000 regional jobs and contribute over $24 billion to the local economy. Houston is also a DHS designated tier-1 urban area security initiative city. According to a 2007 regional threat and vulnerability assessment conducted by *Digital Sandbox, Inc.,* IAH is the highest at-risk asset in the entire Southeast Texas area. Given that the Houston metropolitan area has the Nation's fourth-largest population and is home to essential elements of our energy supply and refining capacity, effective passenger screening at our airports is one of our top priorities.

Over the course of the past 8 years many improvements have been made to the aviation security environment. We work closely with our Federal counterparts in the Department of Homeland Security (DHS), and it's a partnership we value greatly. For example, in Houston we have recently partnered with the Transportation Security Administration (TSA) to implement Explosive Detection System (EDS) baggage screening solutions in both major airports (IAH and William P. Hobby Airport (HOU)). Additionally, the Houston Airport System (HAS) and the TSA are actively working together on the Airport Surveillance Program, a project which provides funding for enhancements to the airports' existing Closed Circuit Television (CCTV) and related recording systems, and the TSA is preparing to implement full body scanner equipment at both IAH and HOU.

But while aviation security has improved significantly since 9/11/2001, the threat is an evolving one and much remains to be done. In the past year alone there have been numerous plots to destroy U.S. aviation assets. On an international level, the attempted bombing of a U.S. airliner on Christmas day reminds us that the aviation sector remains vulnerable to exploitation and attack, and within the Texas region, an airport in Dallas was initially assessed as a terrorist target by a self-radicalized extremist who had overstayed his visa.

Airports face special challenges in ensuring airport security. While the Federal Government plays a key role in airport security matters, Federal law imposes principal responsibility on local airport operators (under 49 CFR §§ 1540 and 1542) for securing the National Aeronautical Domain (NAD) within their particular region. As such, the Houston Airport System has identified many impediments that still exist regarding aviation security—impediments that could be minimized by the procurement of certain security technologies and the institution of certain Federal initiatives relative to: (1) Intelligence sharing, (2) risk assessment/critical infrastructure protection, and (3) field-based aviation security compliance technology.

There are four key points I want to share with you today, and they all have to do with essential needs that airports such as ours in Houston face. They are the need for:

- Improved, timely intelligence sharing and acquisition of appropriate secure communications equipment to facilitate this;
- Development by DHS of a standardized computer-based risk assessment methodology targeted at threats facing airports;
- Field-based devices for use by local airport security personnel that enable real-time, proactive use of current threat data; and
- Funding to cover the associated costs of these measures and of deployment of TSA's Advanced Imaging Technology units.

Allow me to begin by identifying the single most critical issue for airport operators and their local security directors: the lack of timely and consistent dissemination of National threat intelligence information. This remains a constant frustration—one that even predates the tragedy of 9/11. On the State and local level, intelligence sharing has seen some improvement, but obstacles remain. As the committee well understands, the primary objective of intelligence sharing in the aviation security industry is to allow for a proactive approach in driving the security posture and program that is implemented at the ground level. However, airport security directors—i.e., the force with the most available security assets at an airport—generally do not receive the information from Federal sources that they deem necessary or on a timely basis, even though airports such as HAS employ personnel cleared to the appropriate Federal level; at IAH we have more than 200 security personnel, for example.

As a result, airports often are able only to serve as a reactive force as opposed to the preferred proactive security model that we seek to field on a daily basis. The lack of adequate intelligence sharing renders airport security operators in the position of primarily conducting random baseline security measures. But if we received

timely and accurate intelligence information we could adjust the airports' security posture to better counter current and evolving threats. Equally, understanding the potential efficacy of various threat streams would enable airport security authorities to proactively devise and employ appropriate countermeasures. The lack of timely and adequate information thus severely limits the proactive role that airport security directors can play, and overall reduces the efficacy of the available resources. This is a major gap in the system and it needs to be closed, and now.

The absence of appropriate secure technology is a major impediment to the sharing of this information, and we understand the challenges that our Federal counterparts face in this regard. Unfortunately, comprehending threat, risk, and vulnerability—and thus being able to act on that information—has been greatly restricted due to technology and communication gaps caused by the bureaucracy involved in funding and obtaining the equipment needed to receive classified information. To correct this, certain technology must be made immediately available to the local airport security directors. This includes Secure Terminal Equipment (STE) telephones, a Secure Fax, and connections to the Homeland Secure Data Network (HSDN) and Secret Internet Protocol Router Network (SIPRNet). For example, for nearly 4 months now in Houston, HAS' intelligence coordinator, who possesses a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance, has been working with DHS to procure the equipment needed to transact secure communications, but no DHS entity has been willing to provide the sponsorship needed for these acquisitions. While in this case both Federal and local intelligence partners have the desire to work collaboratively in the exchange of intelligence information, the systems do not appear to exist that would ensure the prompt and efficient acquisition of the necessary technology at the local level. This requires immediate attention.

The lack of intelligence sharing is further exacerbated by the fact that there is no current Federal standard in the utilization of a particular risk assessment methodology across the air domain. While some U.S. airports may have incorporated a risk management program, there has been no standard risk assessment methodology prescribed by DHS. What is needed is a National, intelligence-led, risk-based security doctrine that seeks to target and mitigate vulnerabilities in a proactive and recurring fashion. We believe that DHS should adopt a standard risk assessment methodology for use across the NAD in order to facilitate a fair, equitable, and consistent comparison of commercial aviation facilities across the United States. The utility of this security construct is two-fold: (1) It would increase the overall security posture of the National aviation system, and (2) it would enable DHS to allocate scarce funding resources more fairly, consistently, and efficiently in addressing deficiencies from one airport facility to another. The integration of effective intelligence technologies and the identification of a particular risk assessment methodology would ultimately provide a more robust means by which to identify and implement appropriate countermeasures in the field, a duty which again is the primary responsibility of the local airport security operator.

To close the loop and bring the benefits of good, timely intelligence information and uniform risk assessments into the field, we also need the prompt implementation of new technology. Therefore, we believe that an additional critical element of a well-constructed aviation security program would be the implementation of a standardized National aviation security compliance technology. For example, we would support the uniform implementation of a field-based hardware device loaded with software for data tracking/compliance to capture and data mine relevant security information throughout the aviation threat arena. The field-based reporting system we would support should be capable of capturing instant raw data by security area, category, and department. This raw data could then be used to generate predictive trend analysis and, if tied to a National database, could provide valuable real-time information that could also be analyzed and formed into risk assessment and compliance verification product at the National level. The compliance component of this software would ensure that standard, baseline security protocols mandated by TSA are being met, as well as any other unique local response protocols developed as a result of this intelligence-led, risk-based process.

We are encouraged by the TSA's recent announcement of its plan to install Advanced Imaging Technology (AIT) at security checkpoints to replace current walk-though metal detection devices. This technology has the potential to enhance security and deserves further consideration. The airport industry has always been supportive of TSA's evaluation and installation of new technology to enhance security at the checkpoint and efficiency for the passenger. Unlike walk-through metal detectors, AIT can detect prohibited items that have little or no metallic content. AIT will also allow passengers with surgical implants to avoid the invasive physical pat-down inspections that come with walk-through metal detectors. TSA has now deployed the units to more than 19 airports, and is slated to deploy units at several more airports

throughout this calendar year. Airports have encouraged TSA to pursue enhancements to checkpoint technology that will increase effectiveness, efficiency, and passenger throughput while continuing to provide passengers the option of alternate screening methods, and we see this development as very positive.

However, several concerns remain that require immediate attention. First, many airports have severe limitations on the space requirements needed to install AIT units. Of the airports that responded to a recent survey conducted by Airports Council International—North America (the Nation's primary airport trade association), about half reported having limited checkpoint space. In order to accommodate AIT, some airports will lose concession space. This will mean a loss of non-aeronautical revenue during a time when airports are already experiencing extremely tight budgets and traffic declines due to the economy. For others, it will mean a complete reconfiguration of their checkpoint areas or reinforcing their terminal floors in order to support the weight of the units; this also is very expensive. Where will the funding come from for these changes? Many airports already face critical financial challenges, and these will be exacerbated by these additional security requirements. Airports are already severely limited by law in how they can fund their operations, and often face severe opposition when they attempt to increase user fees to accommodate the growing needs of our air transportation system. It is critical that Congress and DHS fully understand and provide for the significant costs associated with additional security requirements; this is not an issue that can be ignored. We need Congress and the DHS/TSA to work with airports to provide funding for the airport modifications necessary for installation of AIT units at airport checkpoints.

In addition to terminal modifications, we are concerned about the throughput time that may be required to process passengers through AIT units as opposed to the time it takes to process them through walk-through metal detectors. TSA has stated that they can process a passenger in 15 seconds; some airports that already have the units at their checkpoints have said that in reality it can take as long as 45 seconds to process one passenger. Airports will continue to work with TSA locally to ensure that passenger queue time remains as efficient as possible, but ultimately airports have no control over the actual processing and utilization of TSA's equipment. Congress needs to provide the direction to DHS/TSA to ensure that these challenges are addressed speedily.

In response to these concerns raised by airports at a recent meeting, Secretary Napolitano asked TSA to create a working group comprised of airport and TSA representatives to develop a coordinated plan for AIT deployment that considers passenger throughput and the costs associated with facility modifications. Although TSA, at the first working group meeting, confirmed that it plans to deploy the first 500 AIT units only to airports that have available checkpoint space and do not need facility modifications, the issue of checkpoint space and modifications will continue to be challenging for other airports, particularly small airports; this issue requires on-going attention. Given the lack of available funding necessary for facility modifications at checkpoint locations where space is limited, we hope that the working group process will result in a cooperatively developed technology deployment plan that identifies airport checkpoint locations where AIT can be readily deployed. We do ask however, that TSA provide funding, where necessary, for any terminal modifications or enhancements that may be required in order to properly install AIT units at airport checkpoints across the Nation. Congress needs to ensure that the security of our airports does not become an unfunded mandate left for our local communities.

In conclusion, allow me to thank you for the opportunity to testify before the committee today. In terms of priorities I would like to conclude by asking the committee to focus on intelligence sharing matters first, the identification of a particular risk assessment methodology second, and the technology-based compliance program to follow. Finally, please remember that the fragile state of the aviation industry today cannot sustain the financial impact that the implementation of this overall security strategy will require; the burdens fall primarily on our Nation's airports, and considerable additional resources are required. Consequently, I would ask Congress not to impose any further unfunded mandates upon either the commercial aviation industry or the local airport operators that are the cornerstone of the industry.

Madam Chairwoman and committee Members, thank you for your attention to these important issues. We greatly appreciate your consideration of these needs, which affect all of us and our Nation's security as a whole. We stand ready to work with you as necessary to achieve the appropriate solutions.

Ms. JACKSON LEE. Thank you very much. Thank you for your testimony.

If the three witnesses would be kind enough to as quickly as possible summarize your testimony so that we can ask questions, we expect a series of votes, and we would like to show consideration of your presence here today. Thank you.

Mr. Rotenberg, you are now recognized for your testimony.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Madam Chairwoman, Members of the subcommittee, thank you for the opportunity to be here today. I will be brief.

The issue of body scanners in the U.S. airports is one that my organization has studied since 2005. We began to pay particular attention in spring 2009 when the TSA announced that it would become the primary screening device for American air travelers here in the United States.

We undertook a series of Freedom of Information Act requests. We brought suit against the Department of Homeland Security. We were trying to determine whether the privacy safeguards that had been incorporated in these devices worked as the TSA claims that they worked.

I think it is very important for this committee to know, based on the documents that we have obtained from the TSA, that these devices as per the TSA technical specification requirements, have the capability to store and record and transmit the images that are captured on American air travelers in U.S. airports. This is contrary to what the TSA has told the American public.

I also would like to share with the committee the complaints that the agency has received from American air travelers, who have been told by the agency that American air travelers much preferred these devices to the pat-down search. But if you read through the complaints that the agency has in fact received, you will find that not only do people object to the use of these devices, in many instances they are not even told of the alternative of the pat-down search. So we believe these consumer complaints should be considered as well.

I would also like to point out that last year before the December incident, more than 30 organizations wrote to Secretary Napolitano and urged her to undertake a public rulemaking so that the public would have the opportunity to comment on the proposed deployment of the body scanners in the U.S. airports and so that technical experts would also be given an opportunity to give their independent evaluation of the proposal.

The Secretary chose not to undertake the public rulemaking and went ahead with this very expensive, very intrusive, if I may say, uniquely intrusive technology for airport screening. We think this is particularly unfortunate.

There is one other document that I would like to call to the committee's attention, and it was in fact not something we were looking for when we undertook the Freedom of Information Act request. Our primary concern is, of course, the privacy protection for American air travelers. But when we obtained the technical specification for the devices, we found something very interesting.

That is that if you look at the requirements—this is the July 2006 TSA technical specification document, and I will be pleased to provide copies of this to the committee—you will see that the devices are intended to target explosives, weapons, liquids, and other anomalies. But there is no mention of powders, no mention of PETN, no mention in fact of precisely the threat that presented itself on December 25.

Our initial conclusion was that in fact these devices were not designed to detect that type of explosive material, that the TSA was pursuing other technologies such as the puffer devices to deal with that risk. Our suspicion, I think, has been corroborated by the GAO report, which seemed to reach a similar conclusion about the capability of these devices to detect the materials that were used on December 25.

If that is the case that the devices cannot detect powdered explosives and that they are unduly intrusive, then we think it would be important to reconsider at this point whether the proposed deployment to U.S. airports really make sense. If they are not effective, if they are overly intrusive, we think this is not the best screening technology for U.S. airports. Thank you.

[The joint statement of Mr. Rotenberg and Ms. Coney follows:]

JOINT PREPARED STATEMENT OF MARC ROTENBERG AND LILLIE CONEY

MARCH 17, 2010

EPIC is non-partisan public interest research organization, based in Washington, DC. Founded in 1994, EPIC was established to focus public attention on emerging privacy and civil liberties issues. EPIC has a particular interest in techniques for screening passengers and other practices of Federal agencies that implicate privacy interests. This is a summary of our prepared statement.

First, we are grateful to the subcommittee for holding this hearing. The recent report of the Government Accountability Office (GAO) has made clear that there are important questions that need to be asked about the effectiveness of checkpoint security. EPIC believes that the deployment of whole body imaging devices in U.S. airports illustrates the challenges facing DHS.

Second, as a result of an extensive Freedom of Information Act lawsuit that EPIC has pursued against the Department of Homeland Security, we have obtained documents concerning the TSA screening practices and the use of body scanners that we believe are of interest to the committee. Based on these documents, which include the TSA Procurement Specifications, the TSA Operational Requirements, and vendor contracts, we have determined that:

- The device specifications for body scanners include the ability to store, record, and transfer images, contrary to the representations made by the TSA;
- The device specifications include hard disk storage, USB integration;
- Ethernet connectivity that raise significant privacy and security concerns;
- The device specifications include "super user" ("Level Z") status that allows TSA employees to disable filters and to export raw images; and
- The DHS Privacy office failed to adequately assess the privacy impact of these devices.

Third, the documents EPIC obtained also raise the question of whether in fact whole body imaging systems, either millimeter wave or backscatter X-ray, could detect the powdered explosive PETN that was involved in the December 25 incident. We noted that the procurement specifications described devices that were capable of detecting "explosives," "weapons," and "liquids" but not "powders." Our finding is similar to the preliminary conclusion of the GAO and independent experts.

Fourth, EPIC subsequently obtained from the TSA records of complaints from travelers who went through the devices. Travelers reported that they were not told about the pat-down alternative or that they were going to be subject to a body scan by TSA officials. Travelers also expressed concern about radiation risks to pregnant women and the capture of images of young children without clothes. And travelers have expressed religious objections to body scanners.

Fifth, EPIC and other organizations have recommended that the deployment of body scanners be suspended, pending an independent review to evaluate health impacts, privacy safeguards, and effectiveness. We hope that the subcommittee will have the opportunity to review these issues in more detail at a subsequent hearing.

In conclusion, we favor the use of airport screening techniques that are minimally intrusive and maximally effective. Unfortunately, the body scanners now being deployed in the Nation's airport are almost the exact opposite—they are uniquely intrusive as they allow the Government to photograph air travelers stripped naked regardless of suspicion. And serious questions have been raised about the effectiveness of these devices to detect and prevent a person from boarding a plane with a powdered explosive.

EPIC would be pleased to provide to the subcommittee the documents we have obtained in our open government lawsuit concerning the use of body scanners in U.S. airports.

Thank you for the opportunity to participate in the hearing today.

REFERENCES

EPIC—Whole Body Imaging Technology and Body Scanners ("Backscatter" X-ray and Millimeter Wave Screening) *http://epic.org/privacy/airtravel/backscatter/*

EPIC—Nader Letter to President Obama Urging Suspension of Body Scanners (Feb. 24 2010) *http://epic.org/privacy/airtravel/backscatter/EPIC-Nader__WBI__Letter.pdf*

GAO, "Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security" (Jan. 27, 2010) *http://www.gao.gov/products/GAO-10-401T*

[Additional attachments will include documents obtained by EPIC under FOIA].

Ms. JACKSON LEE. Thank you very much. We are very much interested in Mr. Miller and Mr. Laskey, if they could be abbreviated so that we can pose questions. Otherwise, we have five votes that will be at least 45 minutes or so for the committee to be in recess.

Mr. Miller, you are now recognized.

Thank you, Mr. Rotenberg, for your testimony. I hope that you will be able to submit the material that you have on the FOIA request to the committee and if the staff can work with you on that.

To Colonel Potts, I believe H.R. 2200 has an intelligence sharing component to it, and we hope the Senate will pass that legislation.

Mr. Miller, you are recognized.

STATEMENT OF HASBROUCK B. MILLER, VICE PRESIDENT, GOVERNMENT AFFAIRS, SMITHS DETECTION

Mr. MILLER. Thank you very much. Good afternoon, Chairwoman Jackson Lee, Ranking Member Dent and Members of the subcommittee. My name is Brook Miller, and I am a vice president of Smiths Detection. I appreciate the invitation to testify here today.

As the subcommittee develops policy on checkpoint security, we urge you to keep in mind three points. First, Smiths Detection strongly supports a multi-layered approach to screening checkpoint both in the United States and abroad that includes a combination of best-in-class technologies. Multiple layers are important, because despite recent significant technological leaps forward, there is no one silver bullet.

Second, Smiths believes homeland security and personal privacy are not mutually exclusive.

Third, while Smiths and DHS are strong and long-standing partners, we believe there are ways to foster additional dialogue between us that would promote the development of security solutions.

Before going into some detail, I will brief you now on Smiths Detection. We manufacture state-of-the-art detection products around the world, including Maryland, Tennessee, Connecticut, and Rhode Island. Having customers around the globe gives us a new, unique depth and understanding of security practices and technology use. In the United States DHS is one of our leading partners. We are pleased to have customers TSA, CBP, and other DHS components, as well as the U.S. Military Transit Authority, first responders, among many others.

To elaborate on the key points for a multi-layered approach, the first vital layer is disseminating actionable intelligence to TSA personnel on the front lines.

Second, we must not lose sight of the key role that TSA screeners play. We share your commitment to ensuring TSA personnel are recognized for the critical work they do and receive the best possible training.

Third, and with the combination of advanced technologies, we can both promote security and address passenger frustrations. These advanced technologies include advanced X-ray technology, bottle liquid scanners for carry-on bags, advanced imaging technology, and expanded use of explosive trace detection for passenger screening.

For screening of carry-on bags, Science and Technology and TSA work with Smiths and others to develop the next generation of AT. Our system, known as atix, allows for multiple angled views of each carry-on bag with a ready ability to upgrade the system with advanced software and algorithms. We ask the subcommittee's support in ensuring continued deployment of AT, which maximizes the chance of detection on carry-on threats.

Smith has also worked with DHS on developing bottle liquid scanners, which are being actively installed in airports today and allow for screening of containers that passengers would otherwise be barred from taking beyond the checkpoint.

Moving to passenger screening, we applaud the expanded use of trace detection, which is a well-established and effective means of detecting explosive residue.

Lastly, on advanced imaging technology, also known as body scanners, we support TSA's plans to deploy upward of 1,000 units by the end of next year, utilizing the technology for primary screening. This technology significantly increases the likelihood of detecting on individuals plastic explosives and other threats undetectable by conventional metal detectors.

Smiths AT is known as eqo. It currently is in the TSL lab evaluation stage of approval. This next generation technology allows for a small physical footprint and real-time imaging capabilities with the promise of faster throughput.

Smiths is encouraged that travelers have become increasingly comfortable with AIT when they experience it for themselves. As with any technology or procedure, both operators and the traveling public need to get some time to get comfortable and efficient with its use, including the right of passengers to opt for an alternative screening method. Near-term deployment of automated threat detection should further enhance security needs and address more privacy concerns.

AIT, of course, is an essential component of an effective multi-layered approach, but we must not lose sight of the urgent need to coordinate international aviation security standards. We support DHS and Department of State's continuing and active efforts to harmonize security standards and practices around the world, and especially at airports which originate flights to the United States.

Chairwoman Jackson Lee, Ranking Member Dent and Members of the subcommittee, thank you for the opportunity to testify. I look forward to your questions.

[The statement of Mr. Miller follows:]

PREPARED STATEMENT BY HASBROUCK B. MILLER

MARCH 17, 2010

I. INTRODUCTION TO SMITHS DETECTION'S ROLE IN U.S. HOMELAND SECURITY

Good afternoon, Chairwoman Jackson Lee, Ranking Member Dent, and Members of the subcommittee. My name is Hasbrouck "Brook" Miller, and I am vice president for government affairs for Smiths Detection, Incorporated.

I sincerely appreciate your invitation to testify here today on aviation checkpoint security. This is always a critical subject for Smiths Detection, this subcommittee, and the Transportation Security Administration ("TSA"), and it is one that has rightly garnered increased media attention after the attempting bombing on Northwest Airlines Flight 253 on December 25.

Before I delve into how the private sector, the U.S. Government, and foreign governments have addressed and can address the vital issues the Christmas day attack brought back to the forefront, I thought I would start by providing some background on Smiths Detection. Our company is part of a set of several technology and engineering enterprises known collectively as Smiths Group. Smiths Detection (or "Smiths," for short) specializes in making best-in-class detection-oriented products to help bolster our Nation's homeland security and defense capabilities. Smiths is headquartered in the United Kingdom.

Smiths has customers worldwide, approximately 90 percent of which are national governments. The U.S. Government is by far our largest customer. The U.S. Department of Defense has procured several types of chemical detection equipment from Smiths to help protect our troops in the field.

The Department of Homeland Security ("DHS") is an equally significant partner of Smiths. First, we work closely with the Science & Technology Directorate ("S&T") to develop state-of-the-art detection technologies. When we bring those technologies to market, the Transportation Security Administration ("TSA"), Customs and Border Protection ("CBP"), the Federal Protective Service ("FPS"), the Secret Service and Capitol Police and other DHS components, not to mention DHS transit authority and first-responder grant recipients at the State and local level, procure detection equipment from Smiths to augment our Nation's aviation, mass transit, port, and border security.

II. SMITHS SUPPORTS A MULTI-LAYERED APPROACH TO CHECKPOINT SECURITY

Many airports in the United States and abroad use similar Smiths equipment to scan carry-on bags at aviation security checkpoints, which brings us to the subject of today's hearing. To maximize our aviation security while keeping passengers moving and protecting their privacy, Smiths strongly supports a multi-layered approach at the screening checkpoint.

Members of the subcommittee, you have heard other speakers today mention the importance of one of those layers: Collecting, coordinating, distilling, and disseminating actionable intelligence to and within DHS, including to the TSA personnel on the front lines. We at Smiths could not agree more.

Another vital layer is the human layer. Simply put, Smiths views those TSOs on the front lines as irreplaceable. Madam Chair and Congressman Dent, we share in your commitment to ensuring that TSA personnel are recognized for the critical work they do, including by working hand-in-glove with technologies every day, and that they receive the best possible training to do it. Furthermore, to help guide their efforts and ours, Smiths also shares your desire for the Senate to confirm a TSA Administrator as soon as possible.

Let me now turn to the layers of checkpoint security Smiths knows best: Employing the best possible technologies to help detect anomalies and potential threats on passengers and in carry-on bags.

III. DETECTING THREATS IN CARRY-ON BAGGAGE THROUGH ADVANCED TECHNOLOGY (AT)

Before examining the headline-grabbing issue of Advanced Imaging Technology (AIT) "body scanners" and other aspects of on-body detection, I would like to mention the innovations that DHS, Smiths, and other industry members have undertaken recently with regard to examining carry-on items. Specifically, Advanced Technology (AT) systems represents a significant leap forward for screening carry-ons, as part of a multi-layered approach to checkpoint security.

For the last several years, S&T and TSA have worked with Smiths and others to develop the next-generation of bag-scanning technology, known as AT. Smiths' AT equipment is known as the "atix," a type of AT equipment that uniquely allows for multiple-angled views of each carry-on bag. Since early 2008, TSA has deployed the atix in multiple U.S. airports, including Baltimore-Washington, Denver, and Albuquerque.

In Smiths' view, AT and atix offer many new benefits compared to the alternatives, which include previous-generation X-ray technologies and more expensive Computer Tomography (CT). In fact, descriptions of AT from TSA itself may say it best:

> "Advantages of AT X-ray include a greatly enhanced image with the ability to target novel threat items resulting in fewer bag checks and faster throughput, and the ability to upgrade the system with enhanced algorithms . . .".[1]
>
> " . . . smaller than previously available explosive detection systems."[2]
>
> "AT systems are highly cost-effective . . . AT training is relatively easy . . .".[3]

By the end of 2009, TSA was scheduled to have deployed approximately 900 AT units for the approximately 2,200 commercial aviation checkpoints in the United States. Smiths strongly supports TSA continuing to deploy ATs to examine carry-on bags. As part of its deployment plan, Madam Chairwoman and Ranking Member Dent, we trust you will join us in looking forward to TSA deploying AT units that maximize the chances of detection and deterrence of carry-on threats.

Smiths is also excited about our work with S&T and TSA to develop and deploy another form of Advanced Technology: Bottle Liquid Scanners ("BLS"). TSA recently decided to procure some of Smiths' portable "RespondeR" BLS units, which are manufactured in Danbury, Connecticut. The RespondeR uses spectrometry technology to look through passengers' liquid containers without opening or damaging them, in order to identify and distinguish safe liquids from those containing threatening substances. BLS will increase both convenience and safety for the traveling public.

IV. ENSURING SECURITY AND PRIVACY WITH ADVANCED IMAGING TECHNOLOGY (AIT) AND TRACE

IV.A. Ensuring Security

The final aspect of multi-layered checkpoint security, Madam Chairwoman and Ranking Member Dent, is the one that may have received the most attention in the aftermath of the attempted attack on Northwest Flight 253 on December 25: Scanning the passenger for on-body threats, including the use of Advanced Imaging Technology (AIT). In fact, on January 7, 2010, President Obama himself called for " . . . greater use of the advanced explosive detection technologies that we already have, including imaging technology, and working aggressively . . . to develop and deploy the next generation of screening technologies."

Smiths believes the administration's current and future deployments of AIT, also known as Whole Body Imaging or "body scanning," are a vital part of a comprehensive, layered detection capability. We particularly support TSA's new approach of combining AIT deployments with increased use of other technologies that also can identify non-metallic, on-body threats at the airport checkpoint, such as trace explosives detectors.

While AIT and trace are not full-proof, nothing by itself is, they significantly increase the chances of detecting on-body plastic explosives, such as the PETN compound allegedly used by Umar Farouk Abdulmutallab. Those non-metallic threats are simply undetectable by conventional metal detectors.

---

[1] *www.tsa.gov/press/releases/2008/0715.shtm.*

[2] Id.

[3] *http://www.tsa.gov/approach/tech/advanced_technology.shtm.*

As a result, Smiths strongly supports TSA's deployment schedule for AIT. In 2009, TSA deployed 40 millimeter wave AIT systems, at six U.S. airports for primary screening and at the other 13 as an alternative to pat-downs for secondary or random screening. TSA plans to deploy approximately 450 AITs, using millimeter wave or the alternative backscatter technology, in fiscal year 2010. In its fiscal year 2011 budget request, DHS has called for $214.7 million to fund the procurement of 500 additional AIT units. If Congress funds the fiscal year 2011 request, TSA is expected to have ordered approximately 1,000 AITs by the end of fiscal year 2011, which would cover almost half of the approximately 2,200 U.S. checkpoints. Industry is fully capable of meeting, or even exceeding, that deployment schedule, and Smiths supports the administration's request.

Smiths also supports DHS's $60 million request for portable trace detection equipment. Trace can augment checkpoint security by detecting explosive particles on travelers' hands, clothing, or luggage, since explosives can be sticky enough to remain there, even after repeated washing.

Smiths also encourages DHS and the Department of State to continue their important efforts to foster international standardization on and deployment of AIT, trace, and other checkpoint technologies and practices. Fortunately, the United Kingdom, the Netherlands, Ireland, and other countries are partnering with the administration in this effort, but it is clearly in its initial stages.

As a company with a global presence, Smiths knows all too well that many airports, including those hosting U.S.-bound flights and especially in the developing world, have a long way to go to match up to the steps that DHS is taking in the United States. It may be time to examine the possibility of further U.S. assistance to spur upgrades in the developing world's security infrastructure.

IV.B. Smiths' "eqo," Next-Generation AIT

Madam Chairwoman, let me turn to Smiths Detection's specific work on AIT. Smiths' AIT product is known as the "eqo," which we developed after licensing the basic technology from Argonne National Laboratory several years ago. President Obama was right in his January 7 speech: Partnering with the National Labs can produce results. The end result for Smiths in this case is the eqo, a next-generation AIT system that uses safe millimeter waves to generate three-dimensional images of a person's body, in order to look for anomalies such as explosives, weapons, drugs, or other contraband.

The eqo possesses a couple of key attributes that distinguish it as a next-generation AIT. First, as a flat-panel system with a metal-detector-like arch, the eqo is small and checkpoint-friendly. This is an especially important feature for smaller airports where real estate is tight. Second, the eqo generates real-time, moving images, which allow for better angles to detect anomalies. Third, those real-time images, by definition, require no downloading time. Smiths estimates this development will lead to faster throughput when the eqo undergoes field testing in U.S. airports.

Prior to field testing, the Transportation Security Lab ("TSL") in Atlantic City has been testing the eqo in the lab for several months. Madam Chairwoman and Ranking Member Dent, we would like to find out more details about DHS's time line for its lab testing and subsequent field testing of the eqo.

IV.C. Ensuring Privacy

At the same time, Members of the subcommittee, while Smiths believes that AIT brings an important new technological capability to the airport checkpoint, we also believe that homeland security and personal privacy are not mutually exclusive concepts. The traveling public deserves to be assured the AIT equipment used by the TSA is capable of guarding their privacy and their security simultaneously. Therefore, Smiths also supports the robust dissemination, or even the codification, of TSA's privacy protections for AIT. These protections are already in place, but not always widely publicized or consistently implemented. Again, the traveling public deserves no less.

Smiths is encouraged that travelers become increasingly comfortable with AIT when they experience it for themselves. According to TSA, over 98 percent of passengers who have experienced AITs prefer them to alternative screening methods.[4] In comparison, a January Gallup/USA Today poll finds 78 percent of U.S. all air travelers, including those who have not undergone AIT screening, approve of the AIT concept.[5]

---

[4] *http://www.tsa.gov/approach/tech/imaging_technology.shtm.*
[5] *http://www.usatoday.com/travel/flights/2010-01-11-security-poll_N.htm.*

Still, Smiths wants to ensure passengers are as informed as possible when using AIT technology. Therefore, to supplement the efforts of TSA and the Congress, Smiths adheres to its own "Seven Points of Privacy" when discussing the use of AIT:

(1) AIT equipment should blur all facial features on its images. TSA and the Smiths eqo take this approach.

(2) TSA officers should view AIT images at remote locations, where no cameras or cell phones are permitted. AIT equipment should transmit all images to that remote location via a secure connection. TSA and the eqo take this approach.

(3) TSA officers viewing the images from that location should talk by wireless headset to TSA personnel at the checkpoint to clear the traveler if nothing suspect appears on the image. TSA and the eqo take this approach.

(4) TSA should have sufficient resources to support a policy that would require male TSA personnel to view male images and female personnel to view female images. TSA does not currently implement this policy.

(5) TSA should disable AIT equipment for field use to make it incapable of saving, e-mailing, or printing any images. TSA and the eqo take this approach, although TSA understandably temporarily enables AITs to save images during earlier off-airport training of TSA personnel.

(6) AIT equipment should automatically and irrevocably delete each image after TSA clears the passenger. TSA and the eqo take this approach.

(7) TSA should provide travelers with an alternative for primary screening: A combination of a metal detector, trace detection, and a pat-down. TSA and S&T should partner with industry to continue to develop computer-driven auto-detection capabilities and to provide other comparable technological alternatives. DHS and Smiths take this approach.

However, as the Members of the subcommittee know, a floor amendment added last June to the House TSA reauthorization bill (H.R. 2200), if enacted into law, would bar AIT from serving as a primary screening option. The language would permit AIT to be used only "for-cause" secondary screening. Smiths views the amendment's approach as problematic. Since metal detectors cannot detect plastic explosives or other non-metallic weapons, TSA may never pull aside for secondary screening a potential assailant, especially a professional who does not appear agitated. That could leave us with a problem comparable to the one we faced on Christmas when, as has been reported, Mr. Abdulmutallab never went through the AITs deployed at Amsterdam's Schiphol Airport.

Instead, Smiths urges the Congress to advance alternative language to enhance security, protect privacy, and codify TSA policy on AIT. We support legislation to encourage comprehensive deployments of multi-layered, advanced technologies, with passengers choosing among suitable options for primary screening.

Chairwoman Jackson Lee, Ranking Member Dent, and Members of the subcommittee, thank you very much for the opportunity to testify. I look forward to your questions.

Ms. JACKSON LEE. Thank you very much, Mr. Miller.

Mr. Laskey.

STATEMENT OF MITCHEL J. LASKEY, PRESIDENT AND CEO, BRIJOT IMAGING SYSTEMS, INC.

Mr. LASKEY. Thank you, Chairwoman Jackson Lee, Ranking Member Dent and Members of the subcommittee. Thank you for the opportunity to address you today.

Brijot Imaging Systems has developed an advanced imaging technology called the Brijot SafeScreen. It does not reveal any anatomical detail of the traveler being screened or emit radiation. Using passive millimeter wave technology, the solution detects anomalies in temperatures by measuring natural millimeter wave energy emitted by the human body.

In addition to protecting the privacy of the traveler, passive millimeter wave technology is better at detecting hidden objects than the current imaging technologies currently deployed.

Active millimeter wave scanner technology showers passengers with either microwave energy or ionizing radiation. Those systems produce images by looking at the energy reflected back off the body and searching for any shapes on the body that don't belong. This technique can run amiss for explosives that are concealed in certain ways.

Passive millimeter wave technology, on the other hand, detects the difference between the millimeter waves your body emits naturally and the hidden object, making it more likely that a powder or liquid will be found.

As evidence of the public acceptance of our technology, it has been approved for use as safe by the Kingdom of Saudi Arabia, where more than 90 percent of the population is Muslim. I have also submitted a letter for the record from the testing laboratory at the Vatican that approves passive millimeter wave technology for use.

Compared to the currently deployed advanced imaging technologies, Brijot's SafeScreen has a smaller footprint, takes up less than two-thirds of the space that is planned for TSA requirements. It increases throughput by two-fold and has a lower total cost of ownership.

In addition to deployments to airports in the United Kingdom and Indonesia and as evidence of the international demand for passive millimeter wave technology, we have responded to multiple requests and conducted trials throughout both Europe and the Asia-Pacific region. We continue to have pending requests for future trials in places like France, Germany, Poland and Romania, Taiwan, Sri Lanka, and Vietnam.

In the mean time we are also moving forward with TSA as part of their qualified products list process to receive the necessary approval to deploy systems in the U.S. airports. As a small company doing business with TSA for the first time, I can say that the process has sometimes appear daunting. I think that our colleagues at the TSA will agree that we had a lot to learn about the process, and they probably have a lot to learn about passive millimeter wave technology.

Our first opportunity to be considered by TSA for approval was in 2006 when TSA issued a broad agency announcement for what was referred to as whole body imagers. Due to the relative newness of our passive millimeter wave technology at that time, the specifications that were written did not match up with what we had to offer, and therefore we were unable to respond.

Two technologies were approved during this initial process, however, and they remain the only two advanced imaging technologies that are available for implementation in U.S. airports today.

In April 2008 TSA reopened and reentered the qualified products list process. Again, as a small company that had never done business with TSA, we had a lot of questions and I think it is fair to say have experienced a couple of snags as we learned how to navigate through this process.

I am pleased to report that Brijot SafeScreen has been in testing at TSA in a simulated checkpoint environment to evaluate how it will perform under various concepts of operation and to collect operating metrics such as throughput and false alarm rates.

While we are encouraged with our progress within TSA, the events of Christmas day have changed the international landscape and provided an unintended advantage of the two technologies that were approved as part of the initial certification process begun in 2006.

Prior to Christmas day our international business prospects were booming. Governments wanted a security solution that provides privacy and protect health. However, given the recent renewed prominence of TSA's role in establishing international aviation security standards, we are now being told by our partners overseas that we must first receive TSA approval before our technology can be deployed at airports. We are, as you can possibly imagine, anxious for this approval and eager to work together with TSA toward earning it.

I am very grateful for the opportunity to share our story with you today and thank you for all your time.

[The statement of Mr. Laskey follows:]

PREPARED STATEMENT OF MITCHEL J. LASKEY

MARCH 17, 2010

Chairwoman Jackson Lee, Ranking Member Dent, and Members of the subcommittee, thank you for the opportunity to address you today.

Brijot Imaging Systems was established in 2004. We are a small business in every sense of the word, with approximately 50 employees working directly for the company. Brijot Imaging Systems is a global leader in passive millimeter wave technology, with customers in the global homeland security, loss prevention, and DoD markets. I expect our company to triple in size over the next 2 years as the demand for screening technology that protects both privacy and health continues to grow domestically and internationally.

We have developed an advanced imaging technology system, called SafeScreen, for use at airport checkpoints. Passive millimeter wave technology is unique in that it does not reveal the anatomical details of the individual being screened, nor does it emit radiation. Instead, it detects anomalies in temperature by reading the natural millimeter wave energy emitted by the human body.

In addition to protecting the privacy of the traveler, passive millimeter wave technology is safe and better at detecting hidden objects than current advanced imaging technologies.

Active millimeter and backscatter technologies shower passengers with either microwave energy or ionizing radiation. Those systems produce images by looking at the energy reflected back off of the body, and searching for any shapes on the body that do not belong. This technique can miss explosives that are disguised in certain ways.

Passive millimeter wave technology, on the other hand, detects a difference between the millimeter waves your body emits naturally and the energy emitted from a hidden object, making it more likely that a powder or liquid will be found.

Compared to currently deployed advanced imaging technologies, SafeScreen has a smaller footprint, taking up less than two-thirds of the space that is planned for in the Transportation Security Administration's (TSA) requirements; increases throughput by two-fold; and has a lower cost of ownership.

We received SAFETY Act certification in April 2009, and have been tested and approved for use by the Sandia National Laboratories, the U.S. Air Force Research Laboratory, the U.S. Marshal Services, as well as by the governments of Israel, France, Germany, Scotland, and Italy.

In September 2007, the U.K. Home Office Scientific Development Branch also tested and approved our technology for U.K. government purchase. In December of that year, Brijot received a contract to deploy systems nationally to U.K. seaports and airports.

We have submitted a statement for the record from John Whyte, the past Deputy Director of Her Majesty's Revenue & Customs and Chair of Detection Technology Board, who believed that this technology can detect not only drugs and currency concealed on the body, but would also be useful in meeting the other requirements of the U.K. border agency, including the detection of hidden documents. He said:

"The testing program for this equipment was rigorous and it was clear that Brijot listened and responded to our needs. This approach was most welcome and an integral part of our decision to purchase Brijot's equipment."

Without releasing sensitive information, I can share that large currency and drug seizures have resulted from our technology's deployment at U.K. ports of entry.

Our first system designed for an airport security checkpoint was deployed to Heathrow Airport in 2006 on a trial basis. Based on the same passive millimeter wave technology that is currently being tested by TSA for deployment to U.S. airports, this particular piece of equipment was designed to meet U.K. border agency requirements. It has a very small footprint, is mobile, and able to operate on batteries. Our systems are still deployed at Heathrow, as well as six other airports in the U.K. today.

As evidence of public acceptance of our technology, it has been approved as safe to use by the government of Saudi Arabia, where more than 90 percent of the population is Muslim.

It has also been tested and approved for use by the testing laboratory of the Vatican.

As further evidence of the continued international demand for passive millimeter wave technology, we have responded to requests and conducted trials at airports in China, Italy, India, Malaysia, the Middle East, and the Philippines. We also have pending requests for future trials in France, Germany, Poland, Romania, Ireland, Taiwan, Kenya, Sri Lanka, and Vietnam.

Although not the purpose of this hearing, I think it is worth briefly mentioning the use of passive millimeter wave technology as a loss prevention measure in the commercial market, where it is much easier to identify Return on Investment (ROI). Our systems are deployed to large distribution centers for global retailers across the country and typically achieve ROI within 3 months of implementation due to reduced shrinkage. Brendan Alexander, the Director of Loss Prevention for Best Buy Canada, said:

"As a retailer that has relied on more traditional security measures such as metal detectors for the past 20 years, we have evolved our screening process by incorporating less intrusive, faster and more accurate technology measures as those offered by passive millimeter wave systems."

In the meantime, we are also moving forward with TSA as part of their Qualified Product List (QPL) process to receive the necessary approval to deploy systems to U.S. airports.

As a small company doing business with TSA for the first time, I can say that the process has sometimes appeared daunting. I think our colleagues at TSA will agree that we had a lot to learn about the process, and they probably had something to learn about passive millimeter wave technology.

Our first opportunity to be considered by TSA for approval was in 2006 when TSA issued a Broad Agency Announcement for what was then referred to as "Whole Body Imagers (WBIs)." Due to the relative "newness" of our passive millimeter wave technology at that time, the specifications that were written did not match up with what we have to offer and we were unable to respond.

Two technologies were approved during this initial process, and they remain the only two whole body imaging technologies that are currently available for implementation at U.S. airports today.

In April 2008, TSA reopened—and we entered—the QPL process for whole body imaging technology. Again, as a small company that had never done business with TSA, we had a lot of questions and I think it's fair to say—have experienced a couple snags as we learned how to navigate the process. By 2008 we developed a new product called SafeScreen, using the same passive millimeter wave technology, that conformed to the TSA requirements and specifications.

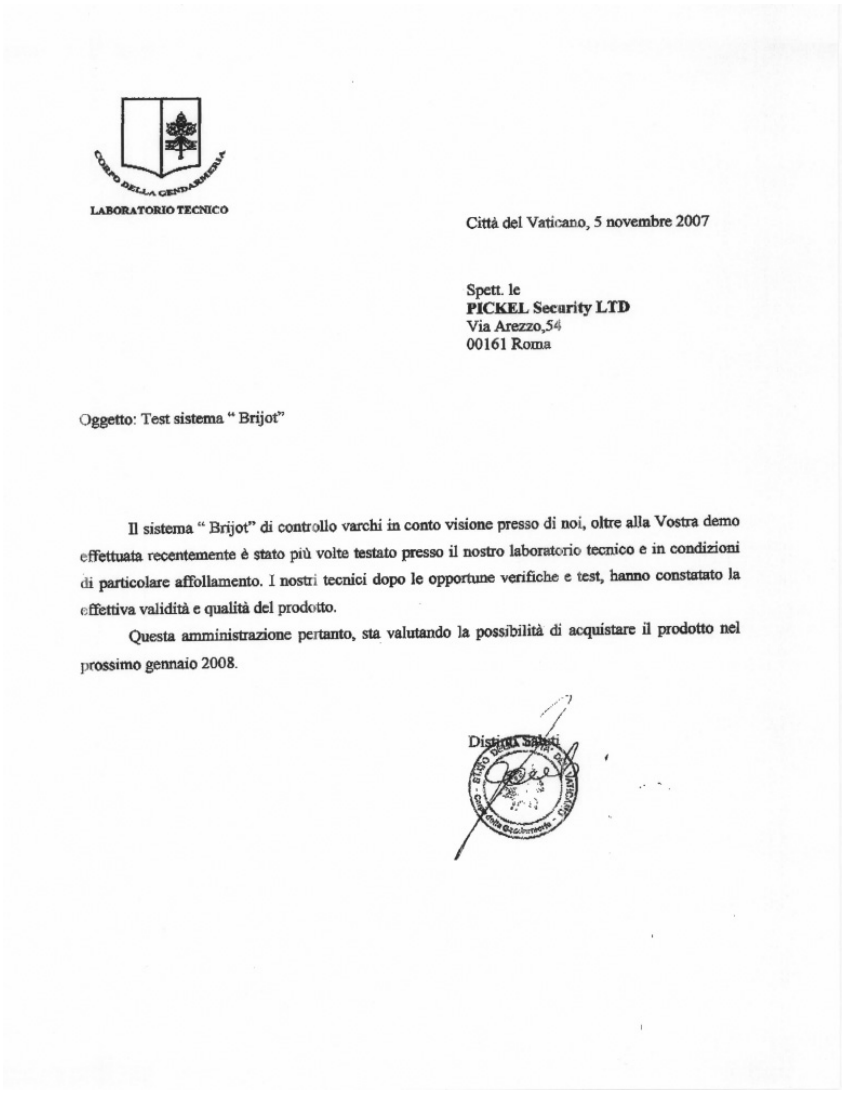
I am pleased to report that SafeScreen has been in testing this week at TSA in a simulated checkpoint environment to see how it will perform under various concepts of operation and to collect operating metrics such as throughput and false alarm rates.

While we are encouraged with our progress within TSA, the events of Christmas day have changed the international landscape and provided an unintended advantage to the two technologies that were approved as part of the initial certification in 2006. Prior to Christmas day 2009, our international business prospects were booming—people wanted a security solution that provided privacy and protected health. However, given the recently renewed prominence of TSA's role in establishing international aviation security standards, we are now being told by our part-

ners overseas that we must first receive TSA approval for our technology before it can be deployed at their airports.

We are, as you can imagine, anxious for this approval and eager to work with TSA toward earning it.

I am grateful for the opportunity to share our story, and thank you for your time today.



CORPO DELLA GENDARMERIA

LABORATORIO TECNICO

Città del Vaticano, 5 novembre 2007

Spett. le
PICKEL Security LTD
Via Arezzo,54
00161 Roma

Oggetto: Test sistema " Brijot"

Il sistema " Brijot" di controllo varchi in conto visione presso di noi, oltre alla Vostra demo effettuata recentemente è stato più volte testato presso il nostro laboratorio tecnico e in condizioni di particolare affollamento. I nostri tecnici dopo le opportune verifiche e test, hanno constatato la effettiva validità e qualità del prodotto.

Questa amministrazione pertanto, sta valutando la possibilità di acquistare il prodotto nel prossimo gennaio 2008.

Distinti Saluti

Access On Time
Transportation & Language Services

(SEAL)

Police Department
Technical Laboratory

Vatican City, November 05, 2007

Dear
PICKEL Security LTD
Via Arezzo, 54
00161, Roma

Re.: Test System "Brijot"

The Brijot's gate control system obtained by us for inspection purposes only, in addition to your demo done recently, has been repeatedly tested at our technical laboratory, particularly under overcrowding conditions. Our technicians, after the appropriate checking and testing, have verified the product's effectiveness and quality.

This administration is therefore considering the possibility of acquiring the product this coming January, 2008.

Kind regards,
(Seal)
Vatican City State
Police Department
Illegible Signature

3210 Lake Emma Road • Suite 3090 • Lake Mary, FL 32746
TOLL-FREE 1.888-748-7575 • www.accessontime.com

Ms. JACKSON LEE. Let me thank you all for your testimony. We are going to stand in recess. We will return for questions on all the witnesses. Thank you. The committee stands in recess.

[Recess.]

Ms. JACKSON LEE. The hearing is reconvened. Thank you for your patience. We will now proceed with the questions.

Mr. Dunlap, you have expressed concerns about the throughput rate of passengers through the AIT machines, but would you agree that AIT offers better screening technologies than the current walk-through metal detectors?

Mr. DUNLAP. What I agree is that it is an interesting, new, and novel technology that gives us detection capabilities that we don't

have right now. But AIT is not a new technology, as you know. AIT has been in various degrees of investigations since 1994. I believe that the first meeting that was had in the city under the FAA was in 1995.

So there has been a period of 15 years where we have been able to examine both the strengths and vulnerabilities of this technology. Soon we would be putting a technology into our airports in which the vulnerabilities have been studied by our adversaries for a number of years. That would give us concern.

Ms. JACKSON LEE. Is concern a pathway toward prohibition?

Mr. DUNLAP. No, not at all. I think as you take a technology like AIT and drop it into a checkpoint, you need to make two fundamental calculations. First calculation is are there more strengths than weaknesses? The second calculation would be what is the effect on passenger throughput? You know, ideally, we would like to see throughput around 200 passengers an hour, but we understand right now some of the systems are only at 160 passengers per hour.

Second, the thing that doesn't get talked about is that AIT is going to require a different way that a passenger will have to present themselves at the checkpoint. So right now if we read the TSA's website, it says, "Please take all the metallic objects off your body." Under AIT you will have to say, "Take off your metallic objects. Take off any kind of hard plastic, non-metallic objects." That is going to have to go somewhere. That is going to have to go into our X-ray machines.

So if you drop AIT in, the next calculation you will have to have is what is the effect of AIT on the X-ray machines? Most probably that will mean they will have to deal with more bins, they will have to deal with more objects. So you will have to strengthen the screening training of the screeners at the X-ray machine to take a look at this new range of nonmetallic objects that are there. So I think there are a number of factors that you have to think about on how the overall screening system operates.

Ms. JACKSON LEE. Do you think the Department has been successful in its outreach to foreign airports and airlines since Christmas day? Do you have any suggestions for improvement?

Mr. DUNLAP. Yes, Madam Chairwoman, we certainly do. One of the things that we can say is we understand that a Government needs to have a strong reaction whenever a terrible incident like this happens. But what we really believe is that the best response is one that is preplanned with the stakeholders well in advance so that you have playbooks to rely on, so you have coordination in place, so that when that incident happens, you have an effective response and an efficient response.

If there is a criticism that can be made of the response to December 25, it is that speed won out over efficiency and effectiveness. What we would ask the Department to do and what we would ask this committee to do is ask for 360 review of all those measures that have been implemented since Christmas and find out what is needless duplication and what are those that need to be enhanced, so we don't find ourselves in a position where regulations that are made in the heat of battle wind up becoming National policy, because we think those are the worst security regulations that we can have.

Ms. JACKSON LEE. Mr. Barclay, what are your comments on what Mr. Dunlap has said? But more particularly, you expressed concerns about the cost of the modifications, terminal modifications to accommodate the AIT machine. That may be perceived as a cost of doing business. How much of that do you think the airport should bear and what is your assessment about the comments of, if you will, convenience to a certain extent or accommodation that Mr. Dunlap has said about the AIT machines?

Mr. BARCLAY. Well, on addressing Mr. Dunlap's comments, I think all of the criticisms you hear have merit to them. Airport executives look on AIT as one new, enhanced, useful tool as part of the whole screening process that we need keeping passengers safe. So we agree with the fundamental decision to go to more deployment of the AIT.

On the costs of the terminals themselves, currently, what we think we are hearing is that, well, we don't have any of that in the budget, so the airports will have to cover everything in terms of the capital costs of terminal modifications. At some locations, that will be significant.

Here at Washington, the people on the committee would recognize you might expect the old terminal at National to require modification, but according to the director here, even the brand-new facility at Dulles looks like, under some assumptions, it won't have all the space needed for putting in AITs as the primary source for screening.

So we are talking about very significant costs, and airports have shown in the past we are willing. We have spent over $4 billion on costs associated with security, but there is not a lot of money left in the system to direct to this project, or we are going to be pulling away from runway safety areas and terminal expansions, meeting capacity and other things that are needed.

Ms. JACKSON LEE. So how valuable do you think this new technology would be?

Mr. BARCLAY. Well, we are relying on the experts. We are not the technical experts in these systems, and we are relying on them and their valuation that this is a useful new tool. Our members are treating it like that, that they would like to see it in their airports as one of the tools used so that we can continue to enhance security.

Ms. JACKSON LEE. Do you think there should be a grant program for security projects like the FAA programs for security, safety in airport terminal projects?

Mr. BARCLAY. Yes, we started out the right way on the baggage screening installations with—TSA wanted to do letters of intent with the airports. These are capital construction projects, so they can get paid out over many years covering debt service. You don't have to come up with all the money up front.

That program, which did fund that $2 billion of the cost of explosive detection systems, was eventually wound down. We have got strong support from this committee and Congress, got strong support from TSA initially, but people that OMB and higher up the food chain kept pushing back against that program, and it was simply a budget matter of trading off it against other costs.

Our point is just you can't pretend those costs aren't there, because they don't fit in your budget. They are real. Somebody is going to have to cover them. Airports believe it should be the responsibility of the Department.

Ms. JACKSON LEE. So you are saying that a grant program would be something that you would welcome.

Mr. BARCLAY. Absolutely, yes.

Ms. JACKSON LEE. Mr. Potts, did your airport, which if you—I didn't hear you say what size it is in the scheme of National airports, if you would put that into the record for me, please. But did you all make any effort to be a pilot program for the AIT?

Terminal modification costs that your airport pays impacts the rent. I understand that you charge your airlines. If that is correct, you can add that in your response. Should AIT installation terminal modifications costs be a cost of doing business, meaning that you would pass it on to the airlines, or would you expect to have some compensation from the Federal Government for reimbursement?

Mr. POTTS. I would, No. 1, for the last question, Madam Chairwoman, would like to see that we have some sort of reimbursement for the efforts that we would have to do to adjust our facilities to take on the new technology to be a grant program as we have had, as mentioned. I think that would be a fair way of doing it for the airports.

You will have airports that are large airports that might be able to do it but they, too, have to weigh the terminal improvement projects. Some of them, if you see one airport, you see one airport. All of us are configured in a different configuration, and some of these, because the power requirements and all of the different sundry things that have to go on with addition of new material, we would like to see a grant program.

As far as how big we are, we are still the eighth-largest at IAH. We are the fourth-largest airport system in the country and the sixth-largest in the world, so we do see a lot of international traffic as well, and so we have to consider that as we go forward.

Ms. JACKSON LEE. So did you previously seek to be in the pilot program for body scanning AIT technology?

Mr. POTTS. Yes, ma'am. We were at the front end of the test case. We had it for about 60 days, and then they take the machines out, and they were gone.

Ms. JACKSON LEE. That was—you were testing, that was the end of it.

Mr. POTTS. Yes, ma'am.

Ms. JACKSON LEE. Which we need to beg the question as to why we have these kinds of fleeting and temporary efforts, and then we don't come back, return, answer any questions, say what is going to happen.

The other point, however, I think, to both Mr. Barclay and Colonel Potts, I know that vast numbers of airports were obviously built before 9/11, and we understand that, though CIP, capital improvement projects, in cities sort of on-going since that time.

I would just offer to say to you—Mr. Barclay, you might want to comment—airports have to have vision, too. We live in another world after 9/11, and it is not always the Federal Government that

should take the brunt of non-visioning about what you may prospectively have to do as it relates to security.

I do think it is worthy of looking at a construct that is a match or a grant program, which I am going to be talking to staff on how we could advocate for that. But airports need to envision, too, and take some of the responsibility for spacing that would be required for new technology.

Mr. BARCLAY. Yes, ma'am. That is why I mentioned that airports have spent billions on the improvements to security already and we will continue to do that, but we appreciate any consideration on a program that sees that this is a shared responsibility, the Federal Government and local government.

Ms. JACKSON LEE. Well, I would hope and I appreciate what you are saying, that we could be partners. I think that would be the best format going forward. We learn from you, and you learn from us, and we hopefully will be able to be constructive in providing security for those airports.

Let me finish by asking Mr. Rotenberg, are you wanting to ban all forms of equipment that require scanning?

Mr. ROTENBERG. Not at all, Madam Chairwoman. In fact, we have made a number of recommendations to promote the use of new techniques that can help detect, for example, explosive materials that might not otherwise be located.

Our concern about body scanners is that they are uniquely intrusive among all of the various airport security techniques. That is the reason for the focus on this particular technology. We have looked closely at the privacy safeguards, because the vendors have said that the privacy concerns have been addressed through the blurring of images and other techniques, and we wanted to evaluate those claims.

We concluded that if it was possible to store the raw images or disable the filters, that in fact the privacy safeguards weren't adequate. So if those problems can be solved, I think there are scenarios under which the scanning technologies could be used.

Ms. JACKSON LEE. Well, I think your input is constructive. I am sure that we are going to take a look at your analysis and ask some more probing questions on this issue. I think your testimony is very helpful to us today.

With that, let me recognize the Ranking Member, Mr. Dent.

Mr. DENT. Thank you, Madam Chairwoman.

Thanks to all of you for being part of this panel this afternoon. Thank you for waiting for us.

My question is to Mr. Miller. You know, TSA has spent 4 years examining this advanced imaging technology. I understand the science behind this technology is decades old. While these new technologies like your ecosystems bring state-of-the-art applications to that science, the threat it addresses is not a new threat.

Is the Department of Homeland Security as a whole, including those agencies represented in our first panel, dedicating sufficient resources to explore new and emerging technologies to address these well-documented threats?

Mr. MILLER. Thanks for the question. Our observation is that the trend is very good in terms of how they are addressing and how

they are prioritizing different technologies, so that that answer is yes, we think that they are looking at an awful lot of things.

They are somewhat under-resourced—we are living in an under-resourced world—in many areas, and so by and large they are trending in the right way by looking at an awful lot of new technologies, experimental technologies, but they can only do so much with the laboratory systems and the like that they have available to them now.

Mr. DENT. How has TSA or S&T communicated the current threat environment to you?

Mr. MILLER. I mean, that is an area for improvement, I would think, overall. But again, the level of communication with industry and between Science and Technology or TSA or the other components of DHS has been better considerably over the past couple of years. There is a better level of communication not only on the threats, but what their plans are and how they would like to see technology development.

Mr. DENT. So would you say they are, then, exploring new and emergent technologies?

Mr. MILLER. They are.

Mr. DENT. Okay. To what extent has TSA and/or the S&T Directorate had conversations with Smiths, addressing the threats associated with weapons concealed in body cavities?

Mr. MILLER. The conversation started some months ago, actually, about what the available—in our view, and I am certain that they asked other industry participants—what was available to try and address that particular threat area. We have had conversations with them. We have meaningful conversations, and they are looking at the efficacy and the direction of things that might be available here and now and what might be available in the coming few years.

Mr. DENT. Thank you.

I would like to move to Mr. Laskey right now. Your company is probably one of the smallest companies trying to navigate this very complex, convoluted, complicated process between TSA and the S&T Directorate. I understand that in 2008 you went to TSA and asked if they would consider your passive millimeter wave technology, and they wouldn't consider it.

The acting administrator for acquisitions wrote you and said that since you did not support your tactical data in July 2006, you would be excluded from the process until they reopened a new solicitation.

Mr. Laskey, are you familiar, I should say, with Moore's Law, which in general states, computing speed doubles every 2 years?

Mr. LASKEY. Yes, sir I am familiar with the law, and I will tell you that from my own experience and I think the experience of our company, that is not necessarily the case. Technology continues to evolve. There is a process, a continuous process improvement. As we develop new technologies, we implement them into our systems and into solving the problems that we have to solve.

You know, the threat environment has continued to evolve and change, and as we are closing one door, there is another door that is opening. So you have to continue to evolve your technology to solve these problems.

Mr. DENT. In the 2 years from your original solicitation for data in 2006 to your product's development in 2008, were new and different technologies developed that might have improved passenger screening capabilities?

Mr. LASKEY. You know, I wouldn't say new. I would say evolving. We have continued to improve the algorithms, probabilities of detection, the elimination of false alarms, and the way that we package our solutions to meet the needs of the customers.

Mr. DENT. Finally, and in your opinion, how might the solicitation process be improved? Do you believe that solicitation should be kept open so that emerging, promising technologies could be considered instead of technologies that are, as of now, about 4 years old?

Mr. LASKEY. Right. Well, certainly, sir, you know, an open process would be very, very preferable. I do agree with Mr. Miller that the process over the last couple of years has gotten much more visibility in terms of the long-term plan and some of the short-term plans. But certainly, you know, having the ability to test vendors in a parallel fashion so that there is an equal opportunity would very much be preferable. Then have the door open for new and young and emerging companies to join that process would be much more preferable.

Mr. DENT. Finally, you mentioned that there were snags in the process to getting your technology certified for possible inclusion on the qualified products list. Can you please give us an example of what some of those snags were and how they affected you as a small business?

Mr. LASKEY. I can think of one most particularly, and that had to do with the requirement for the floor space, the square footage requirements for this AIT solution. When we answered our solicitation, our technical data package, we believed that we met the specification and indeed, we did meet the specification in terms of the square footage requirement, but come to find out that the shape of our floor plan was more rectangular, and TSA was looking for a more square implementation, so it has to go back and re-craft our solution set to meet that specification.

You know, frankly, for a small company, that was, you know, fairly insignificant expenditure. So had the specification, you know, called out that specific requirement, I think we would have been able to do it a lot better on the first try around.

Mr. DENT. Mr. Miller, has Smiths had similar experiences?

Mr. MILLER. Indeed. You know, an area of improvement which, again, has gotten better. The trend is okay, but is to get in front of the data requirements and so forth before they travel on to the acquisition process. Have industry, large and small, have more open conversations with what they are really seeking earlier on in the process would be a marked improvement.

Mr. DENT. Thank you.

I yield back. Thank you, Madam Chairwoman.

Ms. JACKSON LEE. Thank you very much, Mr. Dent.

Let me just finish with Mr. Laskey, see if I understood Mr. Dent's question to you.

One of your concerns as a small or a large entrepreneur is the safety of your proprietary information as you would submit it to the Federal Government. Therefore, are you asking that everyone

who is interested be in the same pool and are assessed at the same time?

Mr. LASKEY. Well, I think certainly, you know, you always have to have cutoffs. I think that there, you know, there is a process by which you are going to have testing and certification for a particular product like the AIT. To the extent that manufacturers are ready, willing, and able to sit together to define their answers to the specific requirements, they should be tested together so that their certifications will come out together and therefore, you know, inadvertently give somebody an unfair competitive advantage by having that, you know, seal of approval by the TSA before others might have that opportunity.

Ms. JACKSON LEE. Let me thank you. We would welcome an expansion of your testimony to brief that particular point as it relates to small businesses and of our emphasis that we are interested in expanding the opportunities for inventiveness in technology.

Mr. Barclay, if I could, do you think it is important in airports, the vast types of airports across America, the international travel, that a technology is there that is able to detect the types of explosives and plastics that were represented to have been utilized or allegedly tried to be utilized by the Christmas day bomber?

Mr. BARCLAY. Our members do. To ignore that threat at this point would just be foolish. Also, to spend all the kingdom's gold on only that threat would be foolish as well. So taking a smart approach to utilizing the technology and putting it in in a discreet fashion is one we agree with. We think the leaders at TSA and DHS are trying to do that.

Ms. JACKSON LEE. Is there any comment, Colonel Potts, that you want to make on the importance of equipment that may be utilized for the unknown future or the alleged tactics that the Christmas day bomber was trying to use?

Mr. POTTS. We use a layered approach, and all technologies that can help us reduce the amount of risk that we are subject to in this current environment would be helpful to help us do our job every day.

Ms. JACKSON LEE. Mr. Rotenberg, how do you think we can strike a balance between the necessity of screening for explosives and privacy?

Mr. ROTENBERG. Well, Madam Chairwoman, I said in my statement that obviously techniques that are most effective in detecting threats are the most valuable, and techniques that are most intrusive are of the greatest concern. I think we have had the experience in developing technologies that don't require us to trade off. I think that is where we get into trouble. To simply say to passengers, if you give up a lot of privacy, that will make you safer, with a technology that it in fact is not more effective is not a good deal.

So we think techniques that focus in particular on threats and, as other witnesses have said, a multi-layered approach that involves human observation, baggage screening is the best approach.

Ms. JACKSON LEE. I don't know if we will completely agree with the totality of your testimony, but I will assure you that it will be a constructive element of our analysis on the utilization of these machines and also the points that were made by witnesses on the

funding of technology that airports need. I think that is extremely important.

I am going to end with Mr. Barclay on the point of training with TSO officers. I know that there is an integration between airport staff and TSO officers. They have to work together. Do you believe enhanced professional training will make their jobs and their productiveness better and add to the collaboration between airports and the TSA?

Mr. BARCLAY. Absolutely. We find that with airport employees, investments in training just create great payback in terms of being able to do things, frankly, with fewer staff, but also with people who enjoy their jobs more. They do better jobs. Training is one of those things you can always get better at, and TSA, I think, believes that. But we can keep pushing them to do even better.

Ms. JACKSON LEE. Well, I would encourage you to be an advocate for H.R. 2200, which you realize that we passed out of this Congress, this House, and is waiting for approval in the Senate, that has a very large component of training that I think will be very helpful in the Nation's security.

Before I gavel this hearing down to a close and express my appreciation to the witnesses, since we are in a Homeland Security hearing, allow me to introduce and have him stand along with his members, Jeff Caynon, who is president of Local 341 Firefighters from Houston, Texas. If all of them would stand, be reflected on the record that there are four members from the Houston firefighters and that we are very grateful for the service of firefighters both in Houston and in Texas and around the Nation.

[Applause.]

Ms. JACKSON LEE. I want to thank the witnesses for their testimony and for the opportunity that you have given us to be able to review some very important points that have been made. Again, this effort, the war on terror, but more importantly, securing America is a team effort, and each of you are very much a part of it. This hearing will show that in its assessment and how we move forward in providing more security for the American people.

With that and the acknowledgment that there may be additional questions by a variety of Members, we would ask that the witnesses would respond to them expeditiously in writing. There were several requests that we made in writing. Our staff—made orally, excuse me—our staff will follow up so that you can present them in writing, both the first panel and the second panel.

As I indicated, today's conversation has helped to bring all of the relevant stakeholders together, and I hope that this energy can be harnessed so the security of our airports can be upgraded successfully and efficiently. We want to ask the hard questions, but we also want them answered quickly so we can again serve the American people.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 5:47 p.m., the subcommittee was adjourned.]

○