No. 12-15893

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

JONATHAN CORBETT,
Petitioner,

v.

TRANSPORTATION SECURITY ADMINISTRATION,
Respondent.

On Petition For Review Of An Order Of
The Transportation Security Administration

ADMINISTRATIVE RECORD — PUBLIC MATERIALS (VOLUME 1B)

STUART F. DELERY
Principal Deputy Assistant
Attorney General

MARK B. STERN
(202) 514-5089
SHARON SWINGLE
(202) 353-2689
Attorneys, Appellate Staff
Civil Division, Room 7250
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530-0001

Corbett v. TSA, No. 12-15893 (11th Cir.)
Index to the Administrative Record --- Public Materials (Volumes 1A-1C)

Volume 1A

Item	AR Page #	Description	Date
1	000001	"Screening Individuals with Backscatter X-Ray Systems" by Daniel Strom, Health Physics Society, available at http://www.as-e.com/pdf/Health-Physics-Screening-Individuals.pdf.	February 3, 2005
2	000003	Report of Assessment of the Rapiscan Secure 1000® Body Scanner for Conformance with Radiological Safety Standards performed by the Ionizing Radiation Measurements Laboratory of the Food and Drug Administration's Center for Devices and Radiological Health (FDA/CDRH).	July 21, 2006
3	000034	TSA Whole Body Imager Operational Requirements Document.	July 31, 2006
4	000073	Government Accountability Office's Report to Congressional Requesters titled "Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved" (GAO-07-634).	April 1, 2007
5	000150	TSA Press Release titled "TSA, AAAE, ACI-NA and NATA Announce Industry-Cooperative Employee Screening Plan."	April 18, 2007
6	000152	TSA Press Release titled "TSA Announces Testing of New Passenger Imaging Technologies at Security Checkpoints."	July 31, 2007
7	000153	TSA Press Release titled "TSA Awards Multiple Contracts to Expand Suite of Security Technology. Five New Technologies Move Quickly from Pilot to Deployment."	October 3, 2007

Item	AR Page #	Description	Date
8	000155	TSA Press Release titled "TSA Tests Second Passenger Imaging Technology at Phoenix Sky Harbor Airport."	October 11, 2007
9	000157	Government Accountability Office's Testimony before the Committee on Oversight and Government Reform, House of Representatives, titled "Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process" (GAO-08-48T).	November 15, 2007
10	000171	Privacy Impact Assessment for TSA Whole Body Imaging program, by the Transportation Security Administration (TSA), Department of Homeland Security (DHS).	January 2, 2008
11	000180	Excerpts from TSA presentation titled *TSA's Security Technology: Presentation for the House Committee on Homeland Security.*	March 7, 2008
12	000182	TSA Blog entry titled "The First Significant Deployment of Aviation Security Technology Since the 1970s."	April 15, 2008
13	000213	TSA Blog entry titled "Catch a Wave and Avoid a Pat Down."	April 17, 2008
14	000294	TSA Press Release titled "TSA Announces Bi-coastal Launch of Millimeter Wave Imaging Technology."	April 17, 2008
15	000295	TSA Blog entry titled "You Asked for It...You Got It, Millimeter Wave Images."	May 9, 2008
16	000355	TSA Press Release titled "TSA Reminds Summer Travelers of the Three Simple Steps to Security."	May 21, 2008
17	000357	TSA Press Release titled "TSA Ramps Up Deployment of Advanced Technology X-Ray Machines, Passenger Imaging Technologies, and Liquids Explosive Detection."	July 15, 2008
18	000359	TSA Press Release titled "TSA Pilots Millimeter Wave Technology at Miami International Airport; Advanced Technology X-Ray Also Deployed."	July 21, 2008

Item	AR Page #	Description	Date
19	000361	Government Accountability Office's Report to the Chairman, Committee on Homeland Security, House of Representatives, titled "TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests" (GAO-08-958).	August 8, 2008
20	000411	TSA Blog entry titled "Bar-coded Boarding Passes – Secure, Mobile, and On The Way."	September 16, 2008
21	000449	TSA Press Release titled "TSA Launches Millimeter Wave Technology at Raleigh-Durham International Airport."	October 15, 2008
22	000450	Privacy Impact Assessment for TSA Whole Body Imaging program, TSA, DHS.	October 17, 2008
23	000460	TSA Press Release titled "TSA Launches Millimeter Wave Technology at Hartsfield-Jackson Atlanta International."	November 13, 2008
24	000461	TSA Press Release titled "TSA Pilots Millimeter Wave Passenger Imaging Technology in Primary Screening."	February 5, 2009
25	000462	TSA Blog entry titled "Pilot Program Tests Millimeter Wave for Primary Passenger Screening."	February 20, 2009
26	000529	Action Memorandum from Gale D. Rossides, Acting Administrator, TSA, to Janet Napolitano, Secretary, DHS, regarding Whole Body Imagery Primary Deployment Evaluation.	February 27, 2009
27	000531	DHS Press Release titled "DHS Recovery Act Aviation Projects to Create 3,000 Jobs."	March 5, 2009

Item	AR Page #	Description	Date
28	000533	Government Accountability Office's Testimony before the House Subcommittee on Homeland Security, Committee on Appropriations, titled "Preliminary Observations on TSA's Progress and Challenges in Meeting the Statutory Mandate for Screening Air Cargo on Passenger Aircraft" (GAO-09-422T).	March 18, 2009
29	000557	Written Statement of Bradley I. Buswell, Acting Under Secretary, Science & Technology Directorate, DHS, before the House Subcommittee on Homeland Security, Committee on Appropriations, regarding "Science and Technology Research and Transitioning Products Into Use."	March 26, 2009
30	000575	Excerpts from the DHS report titled "Fiscal Year 2010 Congressional Justification."	May 7, 2009
31	000579	DHS Press Release, titled "DHS Announces First ARRA Transportation Security Technologies Awards."	May 8, 2009
32	000581	TSA Blog entry titled "CNN Article: Airport Security Bares All, or Does It?"	May 18, 2009
33	000611	TSA Blog entry titled "Will Children Be Screened by Whole Body Imagers?"	May 19, 2009

Volume 1B

Item	AR Page #	Description	Date
34	000685	TSA presentation for the Airport Consultants Council titled "ACC Technology Day: Passenger Screening Program."	July 17, 2009
35	000701	Privacy Impact Assessment Update for TSA Whole Body Imaging, TSA, DHS.	July 23, 2009

Item	AR Page #	Description	Date
36	000711	TSA presentation titled "Imaging Technology Airport Brief."	July 23, 2009
37	000727	TSA Press Release titled "TSA To Begin Testing Imaging technology at George Bush Intercontinental Airport."	July 31, 2009
38	000728	DHS Press Release titled "Secretary Napolitano Announces More Than $355 Million in Recovery Act Funding for Airport Security Projects."	October 1, 2009
39	000731	Government Accountability Office's Report to Congressional Requesters titled "DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges" (GAO-10-128).	October 7, 2009
40	000806	Johns Hopkins University Applied Physics Laboratory report titled "Radiation Safety Engineering Assessment Report for the Rapiscan Secure 1000 in a Single Pose Configuration."	October 30, 2009
41	000866	Testimony of Janet Napolitano, Secretary, DHS, before the Senate Commerce, Science &Transportation Committee, "Transportation Security Challenges Post- 9/11	December 2, 2009
42	000890	Government Accountability Office's Statement before the Senate Commerce, Science & Transportation Committee titled "DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity" (GAO-10-106).	December 2, 2009
43	000915	Letter from Robin Kane, Assistant Administrator, TSA, to Ralph Nader, EPIC, and incoming correspondence.	December 24, 2009
44	000921	Administrator's Daily Intelligence Briefing – Excerpts from OSO Executive Summary Recap for 28-DEC-09.	December 28, 2009

Item	AR Page #	Description	Date
45	000925	Presentation of AIT Incidents & Finds, June-December 2009.	December 31, 2009
46	000933	DHS Press Release titled "Secretary Napolitano Outlines Five Recommendations To Enhance Aviation Security."	January 7, 2010
47	000935	Gallup Poll Results, "In U.S., Air Travelers Take Body Scans in Stride."	January 11, 2010
48	000939	Letter from Janet Napolitano, Secretary, DHS, to Senator Dianne Feinstein, and incoming correspondence.	January 19, 2010
49	000943	Written responses by Janet Napolitano, Secretary, DHS, to Questions for the Record posed by the Senate Committee on Homeland Security and Governmental Affairs.	January 20, 2010
50	000973	Statement of Janet Napolitano, Secretary, DHS, before the Senate Committee on Commerce, Science, and Transportation, for "The State of Aviation Security – Is Our Current System Capable of Meeting the Threat?" hearing.	January 20, 2010
51	000988	Congressional Transcript containing testimony of Janet Napolitano, Secretary, DHS, before Senate Commerce, Science and Transportation Committee, during Hearing on the Northwest Flight 253 Bombing Attempt.	January 20, 2010
52	001063	Written Statement of Janet Napolitano, Secretary, DHS, before the Senate Homeland Security & Governmental Affairs Committee regarding "Intelligence Reform: The Lessons and Implications of the Christmas Day Attack."	January 20, 2010
53	001078	DHS Press Release titled "Press Briefing by Secretary Napolitano on Aviation Security."	January 26, 2010

Item	AR Page #	Description	Date
54	001085	Government Accountability Office's Statement for the Record to the Committee on Homeland Security, House of Representatives, titled "Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security" (GAO-10-401T).	January 27, 2010
55	001111	Material from TSA webpage maintained at http://www.tsa.gov titled "Imaging Technology."	January 31, 2010
56	001118	DHS Press Release titled "Secretary Napolitano Announces Fiscal Year 2011 Budget Request."	February 1, 2010
57	001121	DHS Press Release titled "Fact Sheet: Secretary Napolitano Announces Fiscal Year 2011 Budget Request."	February 1, 2010
58	001126	DHS Press Release titled "Transcript of Background Call with Senior DHS Officials on the Department's Fiscal Year 2011 Budget Proposal."	February 1, 2010
59	001135	Excerpts from DHS report titled "Fiscal Year 2011 Congressional Justification."	February 2, 2010
60	001140	Letter from Gale D. Rossides, Acting Administrator, TSA, to Representative Bennie G. Thompson, and incoming correspondence.	February 24, 2010
61	001147	Statement for the Record by Janet Napolitano, Secretary, DHS, before the Senate Committee on Homeland Security and Governmental Affairs.	February 24, 2010
62	001166	Written Statement of Janet Napolitano, Secretary, DHS, to House Homeland Security Committee.	February 25, 2010
63	001185	TSA Fiscal Year 2010 Report to Congress entitled *Advanced Imaging Technologies: Passenger Privacy Protections*.	February 25, 2010

Item	AR Page #	Description	Date
64	001197	Excerpts of Acquisition Decision Memorandum from Elaine C. Duke, Under Secretary for Management, DHS, to Gale D. Rossides, Acting Administrator, TSA, regarding Passenger Screening Program Acquisition Review.	February 26, 2010
65	001204	Written Statement of Gale D. Rossides, Acting Administrator, TSA, to the House Subcommittee on Homeland Security, Committee on Appropriations.	March 4, 2010
66	001210	Testimony of Gale D. Rossides, Acting Administrator, TSA, before the House Subcommittee on Homeland Security, Committee on Appropriations.	March 4, 2010
67	001264	DHS Press Release titled "Readout of Secretary Napolitano's Meeting with Airline Industry CEOs on Strengthening International Aviation Security."	March 4, 2010
68	001266	DHS Press Release titled "Secretary Napolitano Announces Deployments of Recovery Act-Funded Advanced Imaging Technology."	March 5, 2010
69	001269	Written Statement of Gale D. Rossides, Acting Administrator, TSA, to the Senate Committee on Homeland Security and Governmental Affairs.	March 10, 2010
70	001281	TSA Blog entry titled "Advanced Imaging Technology: 'Radiation Risk Tiny.'"	March 11, 2010
71	001349	Letter from Kevin Janet, FOIA Officer, TSA, to John Verdi, EPIC Open Government Project, providing copies of passenger complaints in response to EPIC's request for material under FOIA.	March 15, 2010

Item	AR Page #	Description	Date
72	001352	Government Accountability Office's Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives, titled "TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain" (GAO-10-484T).	March 17, 2010

Volume 1C

Item	AR Page #	Description	Date
73	001373	Letter from Janet Napolitano, Secretary, DHS to Representative Jane Harman, and incoming correspondence.	March 22, 2010
74	001375	DHS Press Release titled "Readout of Secretary Napolitano's Meeting With National Academy of Sciences President Ralph Cicerone and National Academy of Engineering President Charles Vest."	March 29, 2010
75	001377	TSA Blog entry authored by Gale D. Rossides, Acting Administrator, TSA, titled "Advanced Imaging Technology - Yes, It's Worth It," available through http://www.tsa.gov/blog/.	March 31, 2010
76	001448	DHS Press Release titled "Secretary Napolitano Announces New Measures to Strengthen Aviation Security."	April 2, 2010
77	001451	TSA web-page on tsa.gov titled "TSA Guidance for Passengers on New Security Measures for International Flights to the U.S."	April 2, 2010
78	001453	TSA Press Release titled "Secretary Napolitano Announces New Measures to Strengthen Aviation Security."	April 2, 2010
79	001455	Letter from Gale D. Rossides, Acting Administrator, TSA, to Mr. Gary C. Kelly, Southwest Airlines Co., and incoming correspondence.	April 9, 2010
80	001459	DHS Press Release titled "Secretary Napolitano Meets with African Officials in Nigeria on Ways to Bolster International Aviation Security."	April 12, 2010
81	001461	DHS Press Release titled "Secretary Napolitano Announces Recovery Act Purchase of 1,200 Explosives Trace Detection Units to Bolster Aviation Security."	April 15, 2010
82	001463	Prepared remarks by Janet Napolitano, Secretary, DHS, at Harvard University's John F. Kennedy Jr. Forum.	April 15, 2010

Item	AR Page #	Description	Date
83	001468	Prepared remarks by Janet Napolitano, Secretary, DHS, at the National Press Club.	April 16, 2010
84	001473	Letter from Gale D. Rossides, Acting Administrator, TSA, to Representative John L. Mica, and incoming correspondence.	April 20, 2010
85	001480	Written Statement Janet Napolitano, Secretary, DHS, before the Senate Subcommittee on Homeland Security Appropriations on President Obama's (FY) 2011 Budget Request for the Department of Homeland Security	April 21, 2010
86	001493	DHS Press Release titled "Readout of Secretary Napolitano's Remarks to the Aero Club on DHS Efforts to Bolster Aviation Security."	April 26, 2010
87	001495	Letters from Secretary Napolitano to Senators Jon Kyl, Susan Collins, and Saxby Chambliss, and incoming correspondence.	April 27, 2010
88	001500	DHS Press Release titled "Readout of Secretary Napolitano's Remarks on Bolstering Aviation Security at the National Chamber Foundation's Annual Aviation Summit."	April 28, 2010
89	001502	TSA Blog entry titled "TSA Purchases Additional Advanced Imaging Technology Units (and a Quick Word on Automated Target Recognition)."	April 30, 2010
90	001582	TSA Brief to the National Governors Association, titled "Technology Overview."	May 13, 2010
91	001593	DHS Press Release titled "Secretary Napolitano Announces Additional Deployments of Recovery Act-Funded Advanced Imaging Technology."	May 14, 2010
92	001596	TSA presentation at the Eighty-Second American Association of Airport Executives Annual Conference, titled "Technology Overview."	May 17, 2010
93	001603	Department of Homeland Security's "Standards and Testing for Radiation Safety for Airport Backscatter X-Ray Systems."	May 21, 2010

Item	AR Page #	Description	Date
94	001605	National Council on Radiation Protection and Measurements press release regarding Commentary No. 16, Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems.	May 26, 2010
95	001606	Joint TSA/Customs & Border Protection Press Release titled "CBP, TSA Provide Reminders and Travel Tips to Summer Travelers."	May 27, 2010
96	001609	TSA presentation to the Regional Transportation Authority- Regional Airlines Association Annual Conference, titled "Advanced Imaging Technology (AIT)."	May 27, 2010
97	001632	Letter from Francine J. Kerner, Chief Counsel, TSA, to Mark Rotenberg, EPIC, and incoming correspondence.	May 28, 2010
98	001652	Pilot Plan - Characterization of Individuals Ages and Dress on the Checkpoint Security Process Pilot Plan.	June 30, 2010
99	001655	Presentation re AIT Discoveries & Incidents, January-June 2010.	July 2010
100	001662	AIT Sustainability Plan.	July 15, 2010
101	001691	Proposed Pat-down Procedures Operational Evaluation at LAS/BOS - Summary.	August 17, 2010
102	001693	Informal Assessment of Pat-down Pilot Program at LAS.	August 21, 2010
103	001695	JSP Letter to Sen. Collins re Backscatter AIT safety.	September 7, 2010
104	001703	Info. Memo re Implementation of JHU-APL Recommendations.	October 7, 2010
105	001709	Letter responding the UCSF Scientists' Letter of Concern.	October 12, 2010
106	001718	Document entitled "TSA Statement on New Pat-down Procedures," available at http://www.tsa.gov/press/happenings/ 102810_patdown.s htm	October 28, 2010

Item	AR Page #	Description	Date
107	001719	Pistole's Testimony & Questions for the Record, Senate Committee on Commerce, Science, & Technology Hearing re TSA Oversight.	November 17, 2010
108	001789	TSA Administrator's Statement Regarding Passenger Screening.	November 21, 2010
109	001790	TSA webpage on tsa.gov titled "Before You Go." (This version of the web page was posted from December 14, 2010 through at least June 26, 2012.)	December 14, 2010
110	001792	TSA webpage on tsa.gov titled "Hidden Disabilities." (This version of the web page was posted from December 14, 2010 through at least June 26, 2012.)	December 14, 2010
111	001797	Privacy Impact Assessment for Advanced Imaging Technology with ATR.	January 25, 2011
112	001808	Declaration of Lee R. Kair.	January 28, 2011
113	001820	Pistole Written Statement, House Homeland Security Committee, Transportation Security Subcommittee.	February 10, 2011
114	001828	White Paper discussing Not Using the Advanced Imaging Technology (AIT) to Resolve Walk Through Metal Detector (WTMD) Alarms.	February 15, 2011
115	001829	Kane & Kair Written Statement, House Committee on Oversight & Government Reform, National Security Subcommittee	March 16, 2011
116	001834	TSA Press Release titled "TSA Takes Next Steps to Further Enhance Passenger Privacy."	July 20, 2011
117	001836	TSA Management Directive 100.4 -- Transportation Security Searches	January 25, 2012
118	001847	Written Statement of Christopher McLaughlin, Assistant Administrator for TSA's Office of Security Operations, to House Committee on Oversight & Government Reform & Transportation Infrastructure Comm.	March 26, 2012
119	001856	Graph Tracking AIT Opt-out Rates, June 2, 2009 to May 2, 2012	June 5, 2012

Item	AR Page #	Description	Date
120	001857	Declaration of Gale Rossides	June 17, 2012
121	001864	TSA webpage on tsa.gov titled "Travelers with Disabilities and Medical Conditions," available at http://www.tsa.gov/traveler-information/travelers-disabilities-and-medical-conditions. (This version of the web page was posted from October 22, 2012 to the present.)	October 22, 2012
122	001867	TSA webpage on tsa.gov titled "Notification Card," available at http://www.tsa.gov/traveler-information/notification-card. (This version of the web page was posted from October 23, 2012 to the present.)	October 23, 2012
123	001868	TSA webpage on tsa.gov titled "Pat-Downs," available at http://www.tsa.gov/traveler-information/pat-downs. (This version of the web page was posted from November 27, 2012 to the present.)	November 27, 2012
124	001870	TSA webpage on tsa.gov titled "Advanced Imaging Technology (AIT)," available at http://www.tsa.gov/traveler-information/advanced-imaging-technology-ait. (This version of the web page was posted from November 27, 2012 to the present.)	November 27, 2012
125	001872	TSA webpage on tsa.gov titled "Metal Implants," available at http://www.tsa.gov/traveler-information/metal-implants. (This version of the web page was posted from November 28, 2012 to the present.)	November 28, 2012
126	001874	TSA web-page on tsa.gov titled "Religious and Cultural Needs," available at http://www.tsa.gov/traveler-information/religious-and-cultural-needs. (This version of the web page was posted from December 6, 2012 to the present.)	December 6, 2012

Item	AR Page #	Description	Date
127	001876	TSA webpage on tsa.gov title "Security Effectiveness and Efficiency" available at http://www.tsa.gov/press/news/2013/01/17/security-effectiveness-and-efficiency	January 17, 2013
128	001877	TSA Blog entry titled "Rapiscan Backscatter Contract Terminated – Units to be Removed"	January 18, 2013
129	001878	Statement of John S. Pistole, Administrator, Transportation Security Administration, before the U.S. House of Representatives Committee on Appropriations, Subcommittee on Homeland Security	February 27, 2013

ACC Technology Day

Passenger Screening Program

Presented by:

[redacted], Passenger Screening Program

[redacted], Passenger Screening Program

[redacted], Passenger Screening Program

[redacted], Passenger Screening Program

July 17, 2009

Transportation Security Administration

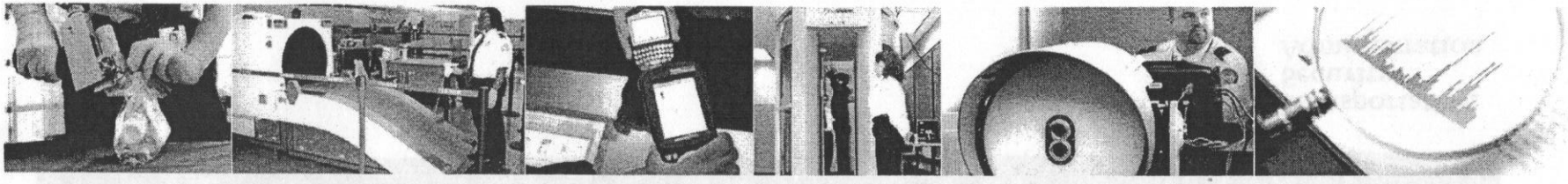
AR 000685

Outline

- Program Overview
- FY09 Spend Plan Highlights
- Testing Strategy
- Deployment Strategy
- Requirements Management Advisory Group
- SI Contract Update
- Upcoming Milestones

AR 000686

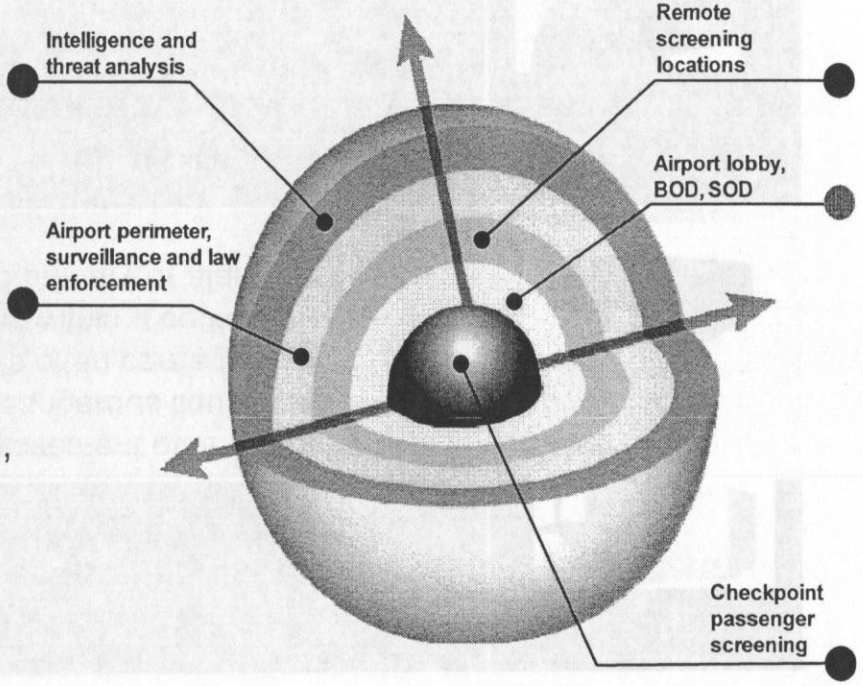
Transportation Security Administration



What is PSP?

TSA's Passen_er Screenin_ Pro_ram PSP **identifies, tests, procures, deploys, and sustains** equipment that detects threats concealed on **people** and in their **carry-on** items as they enter the airport terminal sterile area through the passenger screening checkpoint.

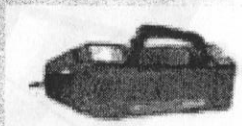
PSP is working to create a transportation security system that is an optimized, integrated, **layered mix** of networked systems that addresses known and emerging threats and vulnerabilities. PSP's vision is to use technology to change the fundamental experience for the passenger. PSP wants to move away from an environment that requires extensive passenger preparation for screening to an environment that is simple and stable for the passenger.



AR 000687

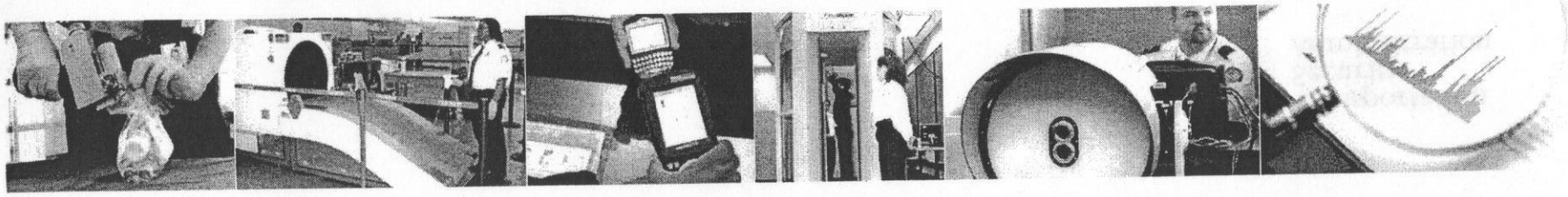
Transportation Security Administration

PSP Technology Fleet

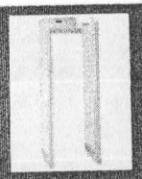
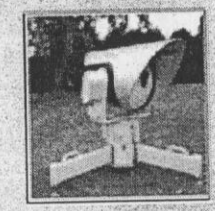
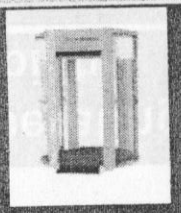
AT	Advanced Technology (AT) refers to the next generation of X-Ray which will replace legacy equipment (TRX) and provides a high resolution, multi-dimension view of carry-on baggage giving the operator an enhanced ability to examine the dimensions and density of objects.	
BLS	The Bottled Liquids Scanner (BLS) is an improvement over currently deployed technologies that can discriminate dangerous liquids and compounds from common, benign substances often carried by passengers. The devices analyze substances within a container in a matter of seconds and can be operated in the primary or alarm resolution position.	
CAT/ BPSS	Credential Authentication Technology (CAT) is an automated system that verifies identification presented by passengers and airport employees. CAT will be able to identify many types of security features (watermarks, Smartchips, micro printing, micro threading). Boarding Pass Security Scanners (BPSS) verifies the authenticity of a boarding pass at the checkpoint and enables the use of paperless boarding passes by the airlines. This technology will increase efficiency, since TSOs will no longer need to manually analyze a diverse set of documentation.	

AR 000688

Transportation Security Administration

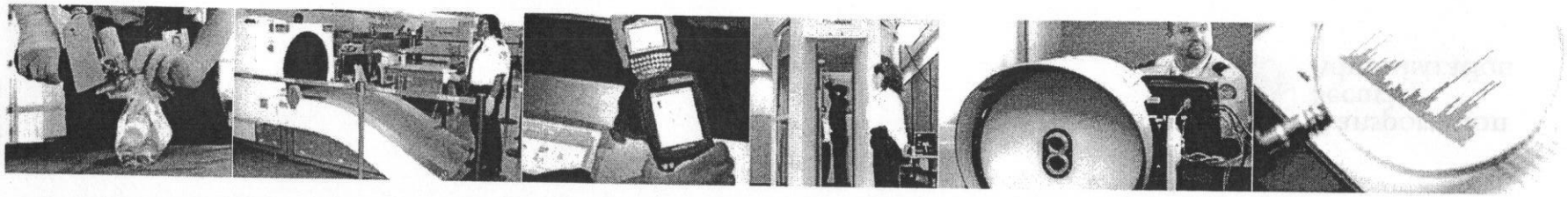


PSP Technology Fleet (cont.)

EMD2	Enhanced Metal Detectors (EMD) 2 refers to the second generation of Enhanced Metal Detectors. EMD 2 builds on the capabilities of the legacy EMD, with a new procurement and the opportunity to integrate additional capabilities.	
SOD	In the Proof of Concept, Standoff Detectors (SOD) used passive millimeter wave (MMW) technology to detect anomalies on the body to help Transportation Security Officers (TSOs) focus on and evaluate passengers exhibiting anomalous behavior. This technology falls in line with the layered security approach.	
AIT	Advanced Imaging Technology is a new capability that will be used to improve detection of concealed weapons (metal and non-metal), explosives and other prohibited items concealed on a passenger. In addition, imaging technology offers a TSO the opportunity to review anomalies on an individual to determine if a hand wand and/or physical pat-down inspection is required.	

AR 000689

Transportation Security Administration



FY09 Spend Plan Highlights

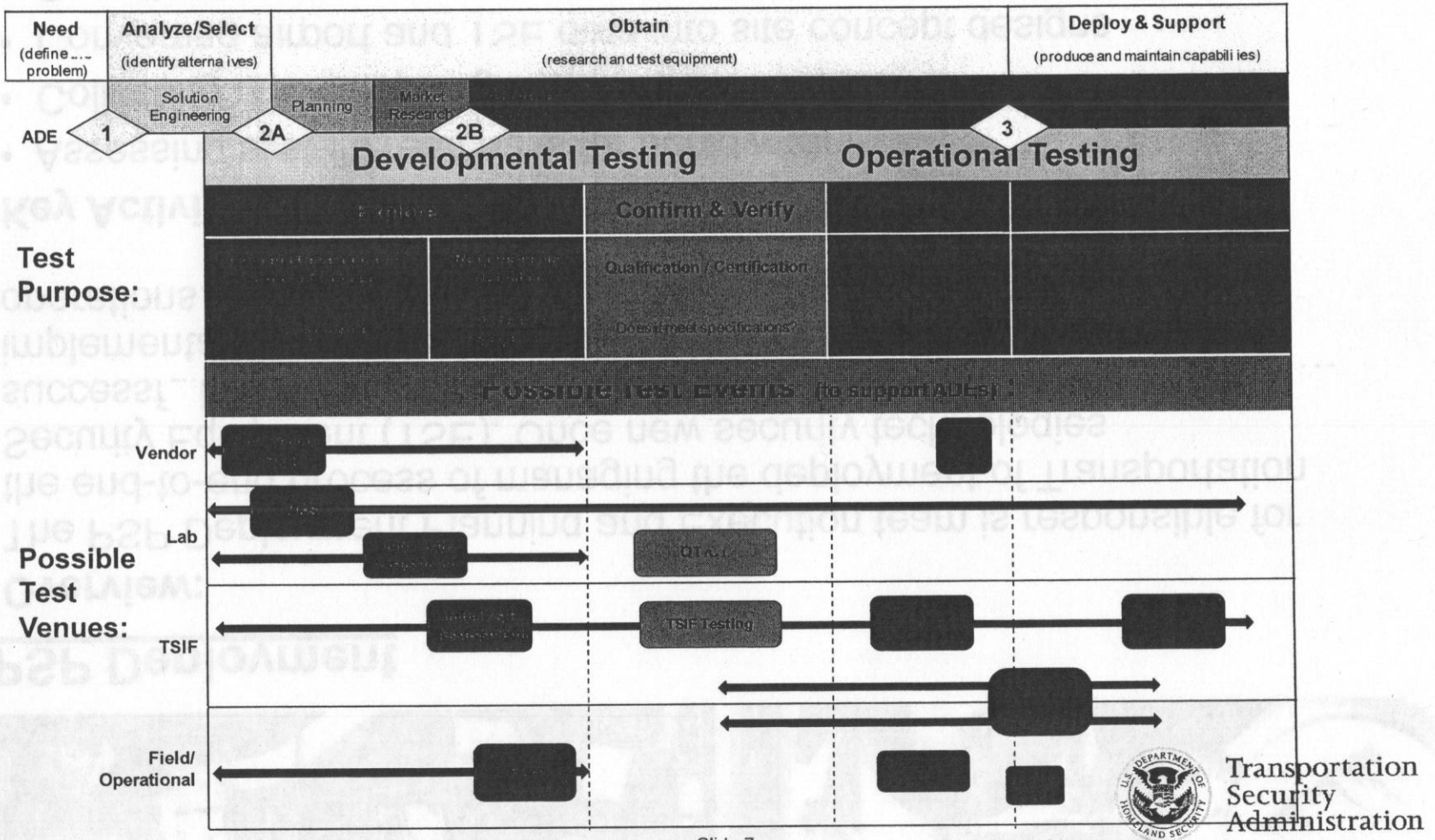
Technology	Total Deployment*	Initial Operating Capability
Advanced Technology	2325 Units	Q1 FY08
Advanced Imaging Technology	878 Units	Q1 FY08
Credential Authentication Technology	2325 Units	Q1 FY10
Bottled Liquids Scanners	1300 Units	Q1 FY10
ETD	1600 Units**	Q1 FY10

**Total units deployed is based on final CONOPS, footprint, and throughput*
***Primarily in support of lifecycle replacements and checkpoint lane expansions*

AR 000690

Transportation Security Administration

Test and Evaluation Process Map



Transportation Security Administration

AR 000691

PSP Deployment

Overview:

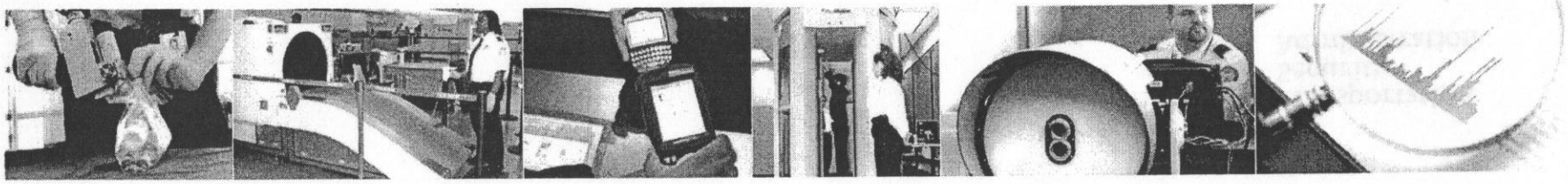
The PSP Deployment Planning and Execution team is responsible for the end-to-end process of managing the deployment of Transportation Security Equipment (TSE). Once new security technologies successfully complete required testing and evaluations, the deployment implementation process is used to transition the new capability to operations.

Key Activities include:

- Assessing system readiness for deployment
- Collecting and compiling airport and TSE data
- Converting airport and TSE data into site concept designs
- Coordinating site preparations and TSE delivery
- Performing on-site TSE installations and performing site hand-off activities (e.g. site acceptance test (SAT), operator training complete, system maintenance support in-place, etc)

AR 000692

Transportation Security Administration



PSP Deployment Strategy

PSP Objectives

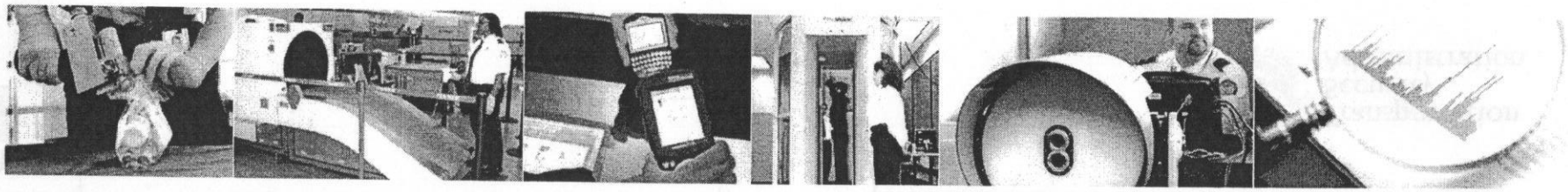
1. Increase threat detection capabilities.
2. Increase checkpoint automation.
3. Minimize securit_ screenin_ footprint to minimize construction investments.
4. Maintain or increase throughput per lane.
5. Minimize disruptions to airport operations.
4. Preserve passenger privacy while enhancing security effectiveness.
5. Ensure screening technology does not introduce health risks to TSOs or passengers.

Deployment Driving Factors

- **Threat-Based** — Prioritize deployment schedule based on the airport threat list provided by DHS.
- **Hub & Spoke Based** — Optimize deployment resources based on the location of major Hubs & Spokes.
- **Common Technology Brand** — Deploy the same brand across hub airports and their regional spoke sites.
- **Create Unified CAD Drawings** — Create full CAD drawings in order to handle permitting in one shot and decrease A&E costs.

Transportation Security Administration

AR 000693

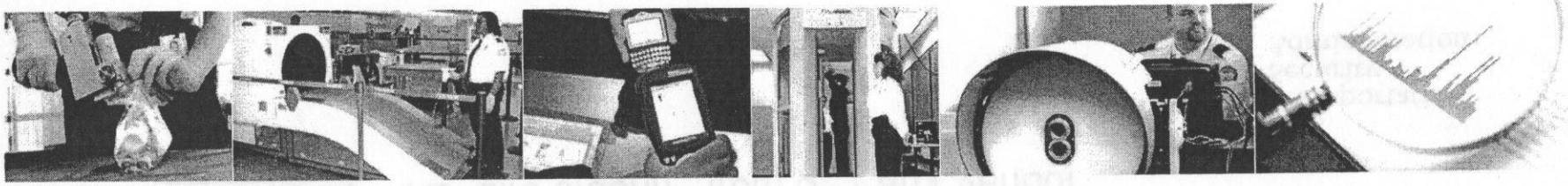


PSP Deployment Activities

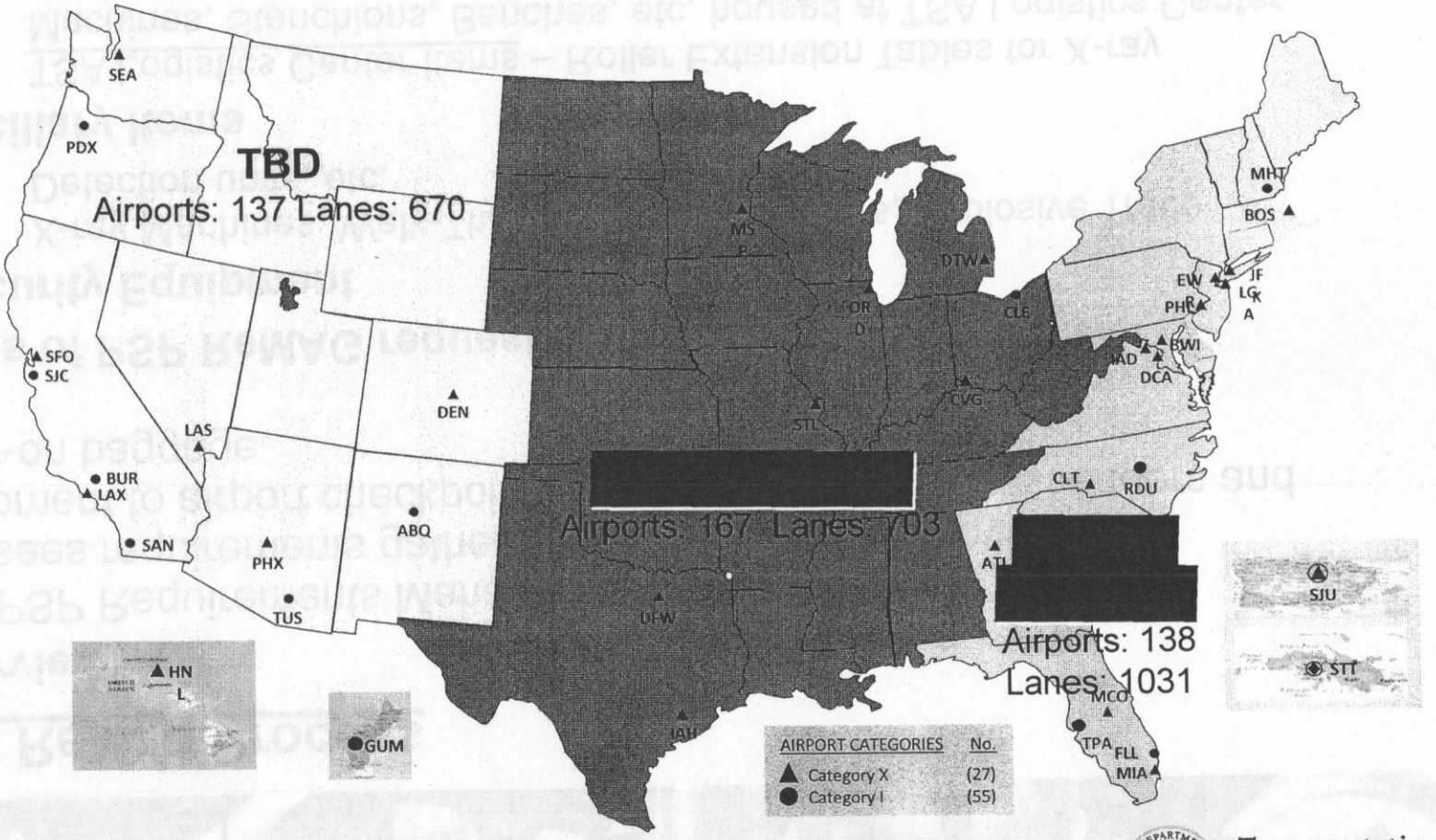
	Design Package	Site Preparation	Equipment Install
Key Activities	• Conduct Site Surveys • Identify Site Issues (electrical, permitting, physical dimensions) • CAD drawings detailing equipment locations and checkpoint configuration • Collect OSO and other stakeholders feedback to ensure buy-in	• Design Validation • Site-_ ermittin_ and subcontracting • Coordination with Airport and OEMs • Site Construction • Electrical, HVAC, rigging	• System Shipping • Final System hook-up, calibration and system test • Legacy System R_m_v_l • Site System • Acceptance Testing • Final Site Acceptance
Duration	▪ 3 to 5 weeks	▪ 4 to 6 weeks	▪ 1 to 3 weeks

AR 000694

Transportation Security Administration



PSP Deployment Regions



Transportation Security Administration

AR 000695

PSP ReMag Process

Overview:

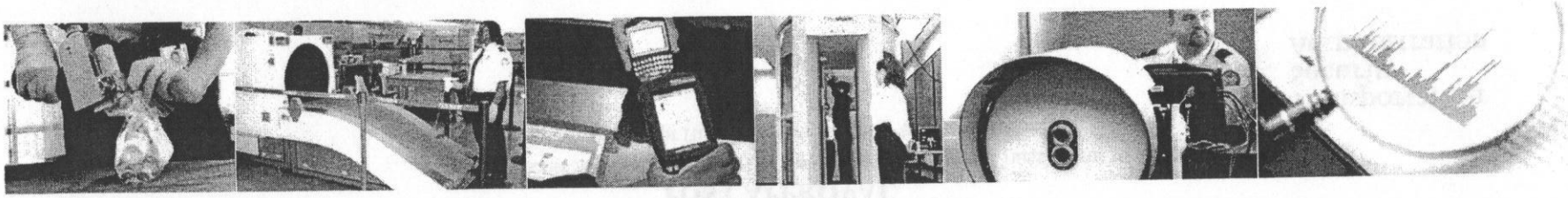
The PSP Requirements Management Advisory Group (ReMAG) oversees requirements gathering, analysis, and deployment of equipment to airport checkpoints for the screening of passengers and carry-on baggage.

Types of PSP ReMAG requests:

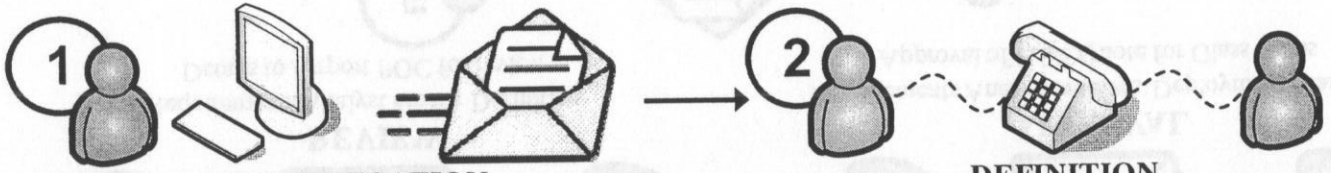
- **Security Equipment**
  - X-ray Machines, Walk-Through Metal Detectors, Explosive Trace Detection units, etc.
- **Ancillary Items**
  - TSA Logistics Center Items – Roller Extension Tables for X-ray Machines, Stanchions, Benches, etc. housed at TSA Logistics Center (TLC)
  - Glass Items – Re uire orderin from 3rd Party Vendor

AR 000696

Transportation Security Administration



ReMag: Security Equipment Process



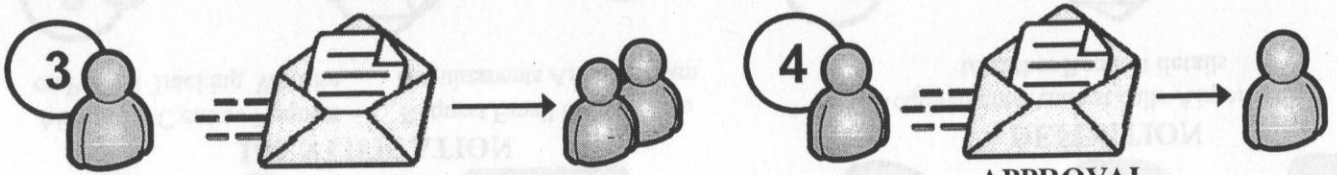
IDENTIFICATION

Airport POC enters Request on Project Tracking Website

Request Email delivered to Requirements Analyst Team

DEFINITION

Requirements Analyst calls Airport POC to gather Request details

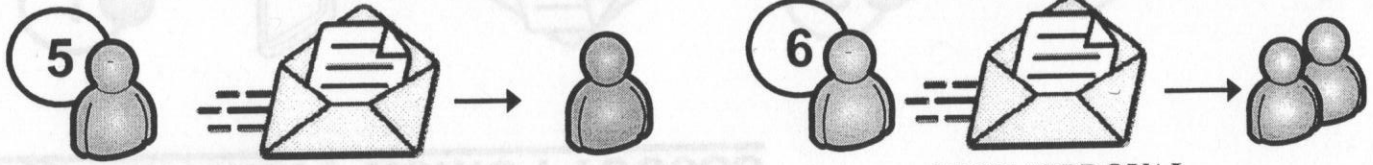


EVALUATION

Requirements Analyst emails Request details to TSA Stakeholders for Evaluation

APPROVAL

Deployment Manager emails Requirements Analyst Validation decision



CONFIRMATION

Requirements Analyst emails Deployment Manager decision to Airport POC for review

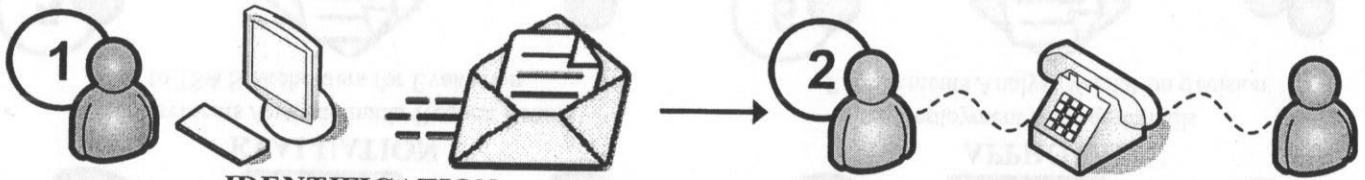
POST APPROVAL

Requirements Analyst emails Approved Request to TSA Property Management for fulfillment and delivery of equipment

Transportation Security Administration

AR 000697

ReMag: Ancillary Items Process



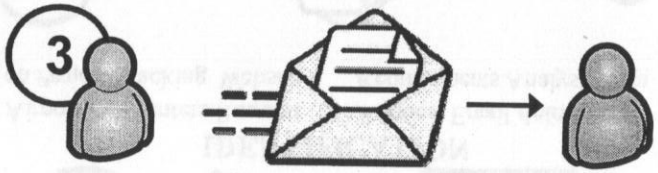
IDENTIFICATION

Airport POC enters Request on Project Tracking Website

Request Email delivered to Requirements Analyst Team

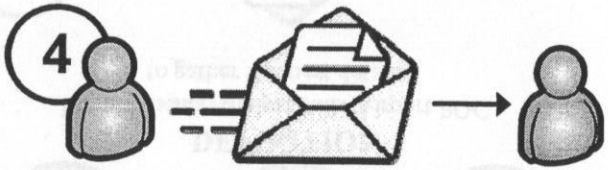
DEFINITION

Requirements Analyst calls Airport POC to gather Request details



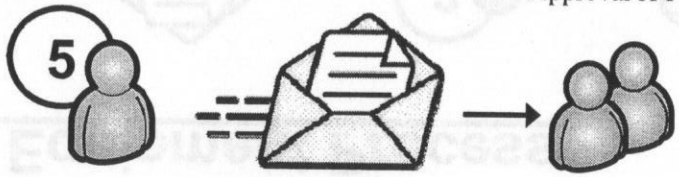
REVIEW

Requirements Analyst emails Definition Details to Airport POC for review



APPROVAL

Requirements Analyst receives Deployment Manager Approval of Price Quote for Glass Items

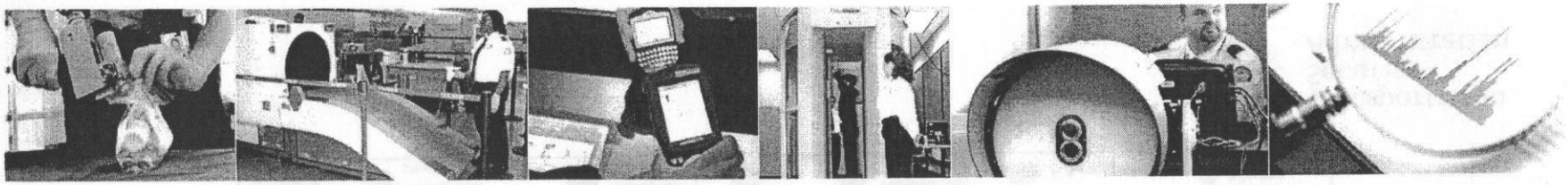


POST APPROVAL

Requirements Analyst emails Ancillary Items to TLC and Glass Items to 3rd Party Vendor for fulfillment & delivery of requested items

Transportation Security Administration

AR 000698

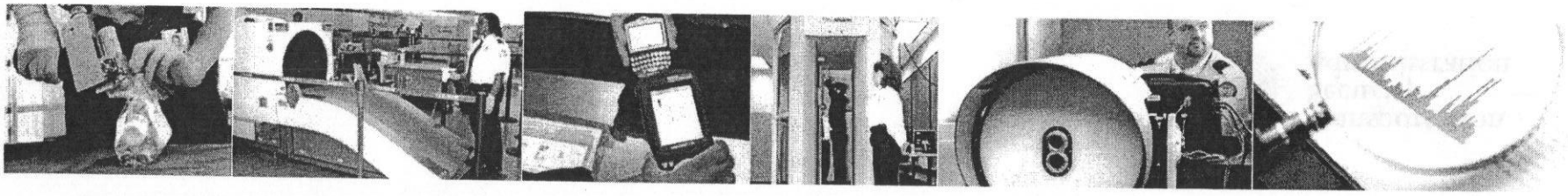


Engineering and Integration Services

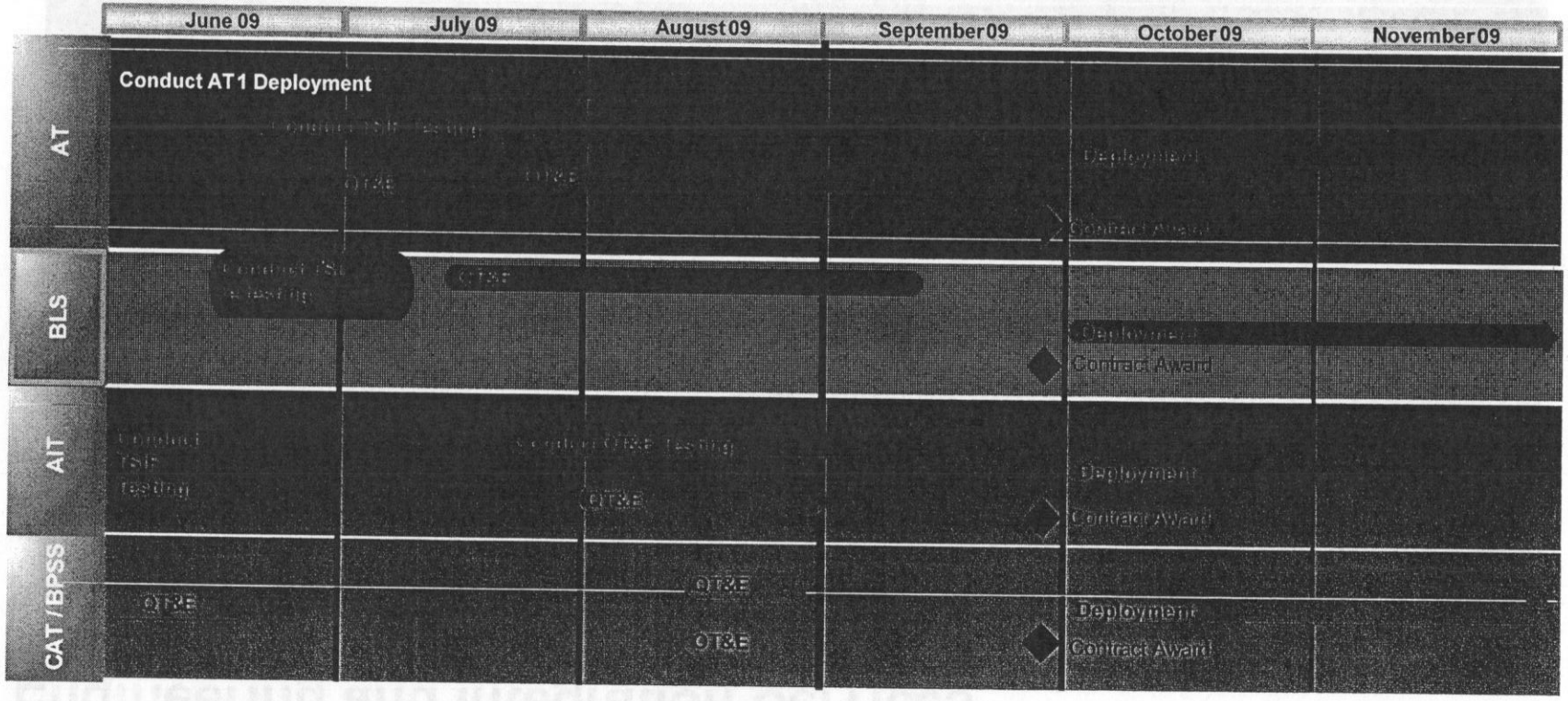
Key Activities	
System Installation	Manage installation and integration of all security equipment, including permitting.
Checkpoint Redesign	Create a more efficient layout which will increase throughput, improve the effectiveness of hostile intent programs, and reduce safety issues and potential breaches in checkpoint operations.
Shipping and Rigging	Coordinating the shipping and rigging of all TSE and ancillary equipment for new equipment installation projects as well as general routine requirements for local TSA operations at airports around the country for items such as ADA gates, barriers, ETD cabinets, anti-fatigue mats, etc.
Equipment Moves	Certified to move any passenger screening technology equipment

AR 000699

Transportation Security Administration



Upcoming Milestones



AR 000700

Transportation Security Administration

Privacy Impact Assessment Update
for
TSA Whole Body Imaging

July 23, 2009

Contact Point
Robin Kane
Assistant Administrator
Operational Process & Technology
robin.kane@dhs.gov

Reviewing Official
Peter Pietra
Director, Privacy Policy & Compliance
Transportation Security Administration
TSAprivacy@dhs.gov

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) will conduct pilot operations to evaluate the use of various Whole Body Imaging (WBI) technologies, including backscatter x-ray and millimeter wave devices, to detect threat objects carried on persons entering airport sterile areas[1]. WBI creates an image of the full body, showing the surface of the skin and revealing objects that are on the body, not in the body. To mitigate the privacy risk associated with creating an image of the individual's body, TSA isolated the Transportation Security Officer (TSO) viewing the image from the TSO interacting with the individual. During the initial phase of the pilot, individuals who must undergo secondary screening will be given the option of undergoing the normal secondary screening technique involving a physical pat down by a TSO or a screening by a WBI device. A subsequent phase will evaluate WBI technology for individuals undergoing primary screening. Individuals will be able to choose to undergo WBI screening in primary.

In the interest of transparency to the public, this Privacy Impact Assessment (PIA) conducted pursuant to Section 222 of the Homeland Security Act ensures that technologies sustain and do not erode privacy protections. TSA has developed operating processes for the WBI, used for pilot operations, that do not collect, store, or distribute any personally identifiable information.

Reason for this Update

TSA continues to evaluate improved backscatter and millimeter wave technologies that may better assist TSOs in identifying anomalies than currently deployed technologies. As the technologies evolve, the image may change allowing for better resolution of anomalies. Given the anonymity afforded by existing operational protocols, the change to the image discussed in this PIA update does not pose any new privacy risk to individuals. No changes have been made to any of the operating protocols with this PIA update; there are minor updates to the previously approved and published PIA dated October 17, 2008. The backscatter image has been updated to reflect the technical improvements, overall scanning time for the backscatter technology has been reduced, and the type of notice to travelers (signs) has been updated.

[1] "Sterile area" is defined in 49 CFR 1540.5 and generally means an area of an airport with access limited to persons who have undergone security screening by TSA.

Introduction

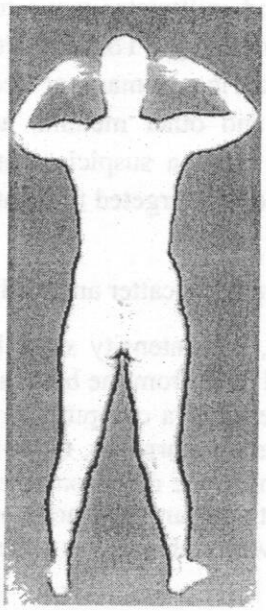
The Aviation and Transportation Security Act (ATSA), PL 107-71, directs TSA to conduct "research, development, testing and evaluation of threats carried on persons boarding aircraft or entering secure areas, including detection of weapons, explosives, and components of weapons of mass destruction." Pursuant to that authority, as well as its general authorities to conduct research and development to enhance transportation security, TSA proposes to evaluate the effectiveness of WBI technologies in operational settings. TSA tested WBI technologies in a controlled laboratory setting and determined the technologies to be technically functional. In the operational setting, TSA will determine whether sufficient passenger throughput can be achieved while maintaining threat detection levels, and will compare operational detection levels between technologies.[2] TSA will use x-ray backscatter and millimeter wave technology in a limited number of airports. By using passenger imaging technology, TSA expects to be able to quickly, and without physical contact, screen passengers during primary or secondary inspection for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing. In the event a suspicious item cannot be cleared visually, the individual will undergo a physical pat down targeted to locations identified through the WBI visual inspection.

TSA will test two types of WBI technologies: backscatter and millimeter wave.

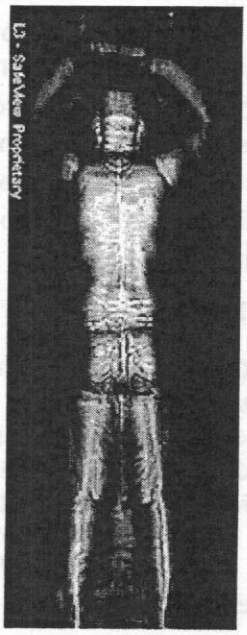
- Backscatter technology relies on a narrow, low intensity x-ray beam scanned over the body's surface at high speed that is reflected back from the body and other objects placed or carried on the body, where it is converted into a computer image of the subject and displayed on a remote monitor. For comparison purposes, the x-ray dose received from the previous backscatter system is equivalent to the radiation received in two minutes of airplane flight at altitude (.02 millirem for two scans by backscatter compared to .0276 millirem for two minutes of a flight). Newer technologies require less scanning time, further reducing individual x-ray exposure.
- Millimeter wave technology uses non-ionizing radio frequency energy in the millimeter wave spectrum to generate an image based on the energy reflected from the body. The three-dimensional image of the body is displayed on a remote monitor for analysis. The energy projected by the system is 100,000 times less than a cell phone transmission (.00000597 mW/cm^2 for millimeter wave technology compared to 37.5 mW/cm^2 for a cellphone).

[2] TSA additionally requested that the National Research Council study "technologies to protect the nation's air transportation system from attacks by terrorists and others of like mind." The study, *Assessment of Millimeter-wave and Terahertz Technology for Detection and Identification of Concealed Explosive and Weapons*, published in 2007, provides further discussion of the systems, their technologies, and a proposed implementation strategy for their deployment.

The images created by the WBI technologies are not equivalent to photography and do not present sufficient details that the image could be used for personal identification. Below are examples of the current level of image detail created by the WBI technology, which may change. Sample images will be made available to individuals at the location of the WBI equipment to show the image to individuals deciding whether or not to choose the WBI visual inspection instead of the physical pat down inspection. It should be noted that the millimeter wave image rotates and both technologies place a blur over the face as the front appears in view.



Backscatter image

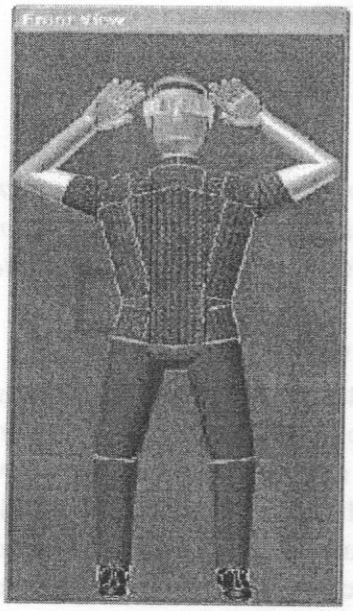


Millimeter wave image

While the equipment has the capability of collecting and storing an image, the image storage functions will be disabled by the manufacturer before the devices are placed in an airport and will not have the capability to be activated by operators. Images will be maintained on the screen only for as long as it takes to resolve any anomalies; if a TSO sees a suspicious area or prohibited item, the image will remain on the screen until the item is cleared either by the TSO recognizing the item on the screen, or by a physical screening by the TSO with the individual. The image is deleted in order to permit the next individual to be screened. The equipment does not retain the image. In addition, TSOs will be prohibited from bringing any device into the viewing area that has any photographic capability, including cell phone cameras. Rules

governing the operating procedures of TSOs using this WBI equipment are documented in standard operating procedures (SOP), and compliance with these procedures is reviewed on a routine basis. Due the sensitivity of the technical and operational details, the SOP will not be publicized, however, TSOs receive extensive training prior to operating WBI technology.

The TSO who views the image will be located remotely from the individual being screened so the TSO will not be able to see the actual individual. The TSO viewing the image will communicate with the TSO at the checkpoint through a red/green light system, or through a monitor located at the checkpoint on which there will be an indication either that there is no anomaly to be resolved such that the individual can proceed or that an anomaly exists that must be resolved. If there is an anomaly to be resolved, the TSO will communicate via radio to direct the TSO at the checkpoint to the location on the individual's body where a threat item is suspected, or will highlight the anomaly location on a generic figure that is displayed on a monitor that the checkpoint TSO can read. A sample generic figure with a sample highlighting appears below. The TSO at the checkpoint will then conduct a physical pat-down that is focused on the particular area and not necessarily of the individual's entire body which would normally occur absent the added information from the WBI technology.



Generic Figure Highlighting Area for Resolution

The WBI pilot program recognizes and seeks to accomplish the twin goals of minimizing privacy intrusions, while ensuring that prohibited items, such as weapons and explosives, do not enter the airport's sterile area. The WBI system present images of potential threats while minimizing individually identifying features. Further, the operational documentation cites with approval NRC Publication NMAB-482-1, *Airline Passenger Security Screening: New*

Technologies and Implementation Issues, (1996), and appears to have considered carefully the issues raised in that publication.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974 and shall assure that technology sustains and does not erode privacy.

In response to this obligation, the DHS Privacy Office has developed a set of Fair Information Practice Principles (FIPPs) from the underling concepts of the Privacy Act, which encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure. Given the particular technologies and the scope and nature of their use, TSA used the DHS Privacy Office FIPPS PIA template.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

TSA has published extensive information on WBI technologies on its website (www.TSA.gov) beginning in February 2007, and conducted outreach with national press and with privacy advocacy groups to explain the evaluation of WBI technologies. Informational brochures regarding the program will be made available at each WBI site that will show a WBI image that the technology will create. Most PIAs are conducted on IT systems that collect and retain PII. TSA has configured the WBI technologies it is using such that they do not retain the images once the individual has been screened. TSA is conducting this PIA in order to be transparent and provide notice to the public regarding TSA's use of WBI technologies.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and

maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Individuals undergoing primary screening will have the option to decline a WBI screening in favor of alternative screening. Individuals referred to secondary inspection are offered the option to undergo WBI screening as an alternative to the pat-down screening that would otherwise be required. Individual participation and consent is exercised by the individual's selection of the screening method and no individual is required to use WBI for screening. Consent is informed by the availability of signage that explains the technology and shows a sample image.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII, to include images, and specifically articulate the purpose or purposes for which the PII is intended to be used.

TSA is responsible for security in all modes of transportation, including commercial aviation. 49 USC §114. Congress directed TSA to conduct "research, development, testing and evaluation of threats carried on persons boarding aircraft or entering secure areas, including detection of weapons, explosives, and components of weapons of mass destruction." 49 USC §137.

Pursuant to that authority, as well as its general authorities to conduct research and development to enhance transportation security, TSA is evaluating the use of WBI as an improvement over current threat item detection by metal detector and pat-down, particularly with respect to non-metallic threat objects and liquids. An image will appear on the WBI viewer to screen for threat objects and will be deleted as soon as any anomalies are resolved. The image is not connected to an individual identity and is not sufficiently detailed to identify an individual.

4. Principle of Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

WBI technologies identify objects on the outside of the physical body and do not reveal implants beneath the surface of the skin. TSA does not save the image in connection with the use of WBI technologies. While the technology can be configured to store images, TSA considered the privacy issues of this storage feature and carefully evaluated all potential uses of the images for training, investigations, or possible prosecution of persons caught with prohibited

items. Based on this evaluation, TSA decided to have the manufacturer disable the data storage capabilities prior to delivery to TSA. Individual operators do not have the capability to reverse the capability to enable image retention. As a result, the image will only be available during the time the individual is being screened and will be deleted immediately thereafter.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

TSOs sitting in the remote viewing room are the only persons to see the WBI images that appear on the screen transiently for the purpose of identifying any potential threat items. The TSOs at the screening location and the supervisory TSO overseeing their actions are prohibited from entering the remote room and viewing the images on the screen. Once any anomaly is resolved, the image is deleted, and therefore cannot be used for any other purpose or shared with anyone. The images will not be used in any other context inside DHS and will not be shared outside of the Department.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII, including images, is accurate, relevant, timely, and complete, within the context of each use of the PII.

The WBI images are generated by direct observation by the imaging technology. Accordingly, it is accurate, timely, and complete, and is directly relevant to the identification of threat objects. Potential threat items are resolved through a directed physical pat down before the individual is cleared to enter the sterile area. The images are not retained, thereby further mitigating any data quality or integrity issues.

Viewing of WBI images occasionally requires interpretation of the images. A WBI image with a suspicious area (one in which it is unclear whether there is a prohibited item) will require additional screening of the traveler with a limited pat-down, focusing on the suspicious area alone. The traveler may be patted down in the screening area, an alternate screening area, or in a private area.

7. Principle of Security

Principle: DHS should protect PII, including images, through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

WBI data is transmitted between the checkpoint and the viewer by a landline connection and cannot be lost, modified, or disclosed. Backscatter images are encrypted. Millimeter wave data is transmitted in a proprietary format that cannot be deciphered without the proprietary technology. TSA's decision not to retain images mitigates further data storage security issues. In addition, the computers used to process and present the images will be locked with both physical and software controls to prevent the insertion of any storage media or other communication devices. Administrative controls limit access to the remote viewing rooms to TSOs and prohibit TSOs from bringing photographic devices, to include cell phone cameras, into the room in which images are viewed.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, including images, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TSOs operating WBI technology are given extensive training both in detecting threat items as revealed by the WBI technology and the operational protocols that protect the privacy of individuals undergoing WBI screening. Specifically, TSOs will undergo privacy and Privacy Act training developed by the DHS Privacy Office for the Department. Supervisors will ensure that policies and procedures regarding photography are fully enforced. In addition to administrative controls imposed by the operating protocols, technical controls also enforce accountability since WBI technology settings are locked and cannot be changed by the TSO operating the equipment.

9. Additional Issues

Discuss any issues impacting privacy not covered by the eight FIPPs.

There are none.

Conclusion

WBI technology used in the pilot program has the potential to improve threat detection capabilities for both metallic and non-metallic threat objects, while improving the passenger experience for those passengers for whom a physical pat-down is uncomfortable. The operating protocols of remote viewing and no image retention are strong privacy protections that permit security benefits to be achieved. TSA will update this PIA as needed if there is a decision to utilize one or both of these WBI technologies beyond pilot operations in several airports.

Responsible Officials

Mike Golden

Assistant Administrator

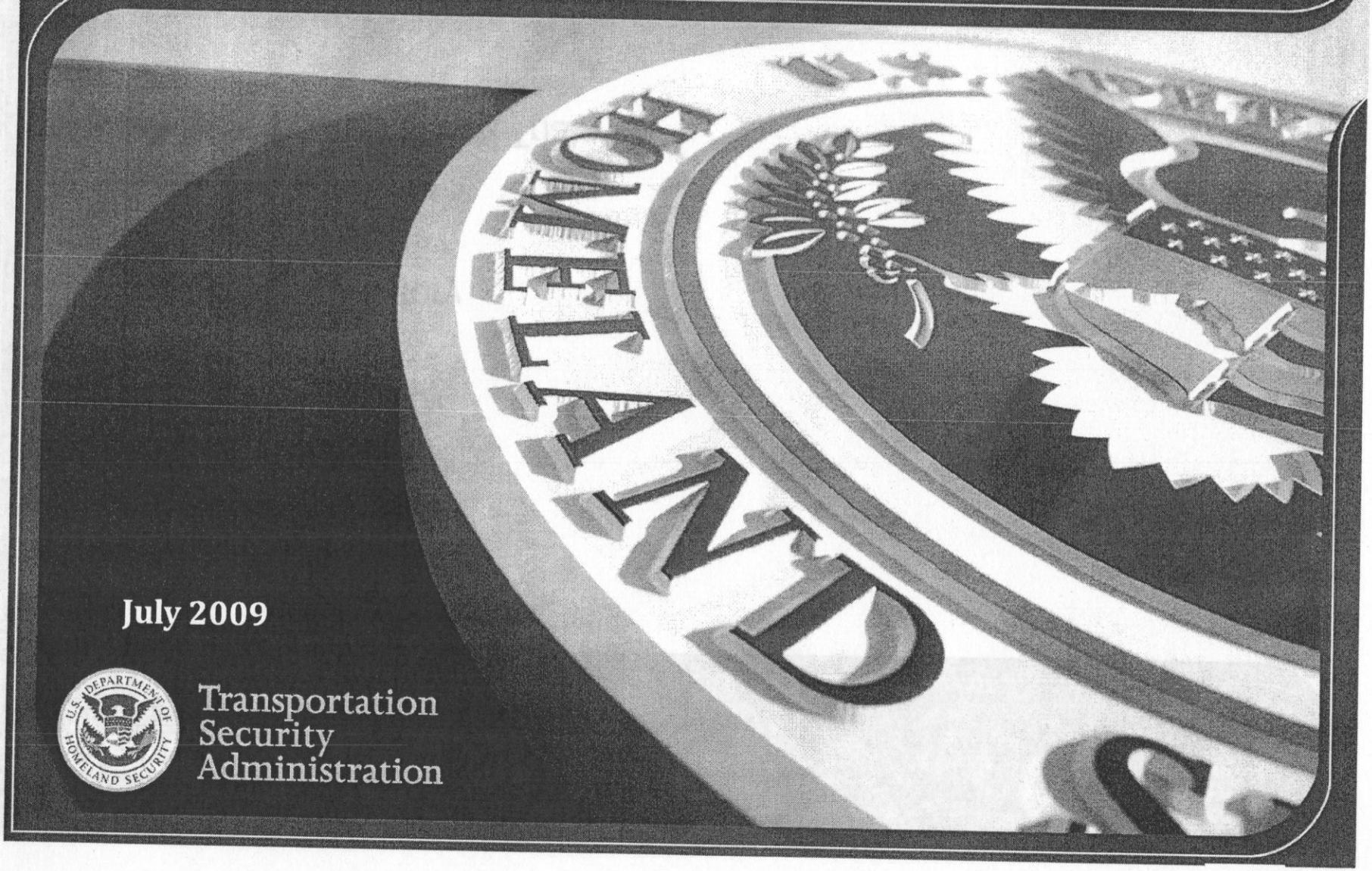
Operational Process & Technology

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Imaging Technology Airport Brief



July 2009

Transportation
Security
Administration

AR 000711

Agenda

Transportation Security Administration

- Overview
- System Description
- Benefits
- Passenger Privacy
- Safety
- Deployment History
- Current Locations
- New Procurement
- Testing Update: Field Trials

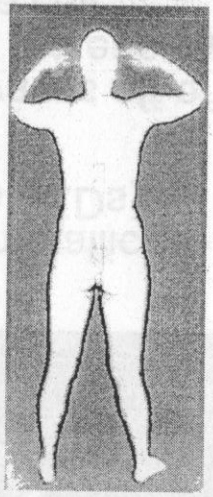
Imaging Technology: Overview

Transportation Security Administration

Overview

- **Description:** Millimeter Wave (MMW) and Backscatter Technologies are designed to display anomalies concealed on passengers
- **Value:** Improves passenger convenience and comfort and provides greater detection capability for metallic and non-metallic threats
- **Fit:** Imaging Technology provides a reliable alternative to current screening procedures in both primary and secondary screening positions

Millimeter Wave



Backscatter

AR 000713

System Description

Transportation Security Administration

- Imaging Technology is designed to identify a variety of potential metallic and non-metallic threats and other Improvised Explosive Devices (IEDs).
- Millimeter wave technology bounces harmless electromagnetic waves off of the human body to create a black and white image. It is safe and the energy emitted by millimeter wave technology is 10,000 times less than a cell phone. The image is displayed on a remote monitor for analysis to determine whether anomalies are present.
- Backscatter technology uses a narrow, low-intensity, X-ray beam scanned over the surface of the body at a high speed that is converted into a computer image of the body.
- Imaging technology greatly enhances detection capabilities at the security checkpoint to include a broader range of potential threats.

AR 000714

Imaging Technology Benefits

Transportation Security Administration

Benefits

- **Improves security effectiveness** by displaying both metallic and non-metallic anomalies.
- **Improves security effectiveness** by eliminating physical fatigue of Security Personnel and improving their effectiveness through training and image detection techniques.
- **Improves passenger experience** by reducing need for physical pat-downs.
- **Improves privacy** by removing security officers from sight, activating privacy filters, which minimizes the chance of recognition, and not having the capability to store or transfer images.

AR 000715

Passenger Privacy

Transportation Security Administration

- The use of this technology is optional. All passengers may request alternate screening procedures - walk through metal detector and pat-down.
- Imaging technology is equipped with a privacy filter that blurs the features of individuals.
- The generated image of the individual cannot be stored, transmitted, or printed.
- Image reviewing operator is seated remotely and cannot physically view passengers in the screening device.
- No cameras or cell phones with photographic capabilities or data storage/transfer devices are permitted in the Image Operator remote viewing room.
- All communications are transmitted on closed microphone radios.

AR 000716

Safety

Transportation Security Administration

- The energy emitted by millimeter wave technology is 10,000 times less than a cell phone.
- The radiation projected from one Backscatter scan is equivalent to two minutes on an airline flight.
- Imaging technology ***does not*** pose a health risk to:
  - Pregnant women
  - Infants or Children
  - Individuals with implanted medical devices (i.e. pacemaker, implanted defibrillator, etc.)

AR 000717

Deployment History

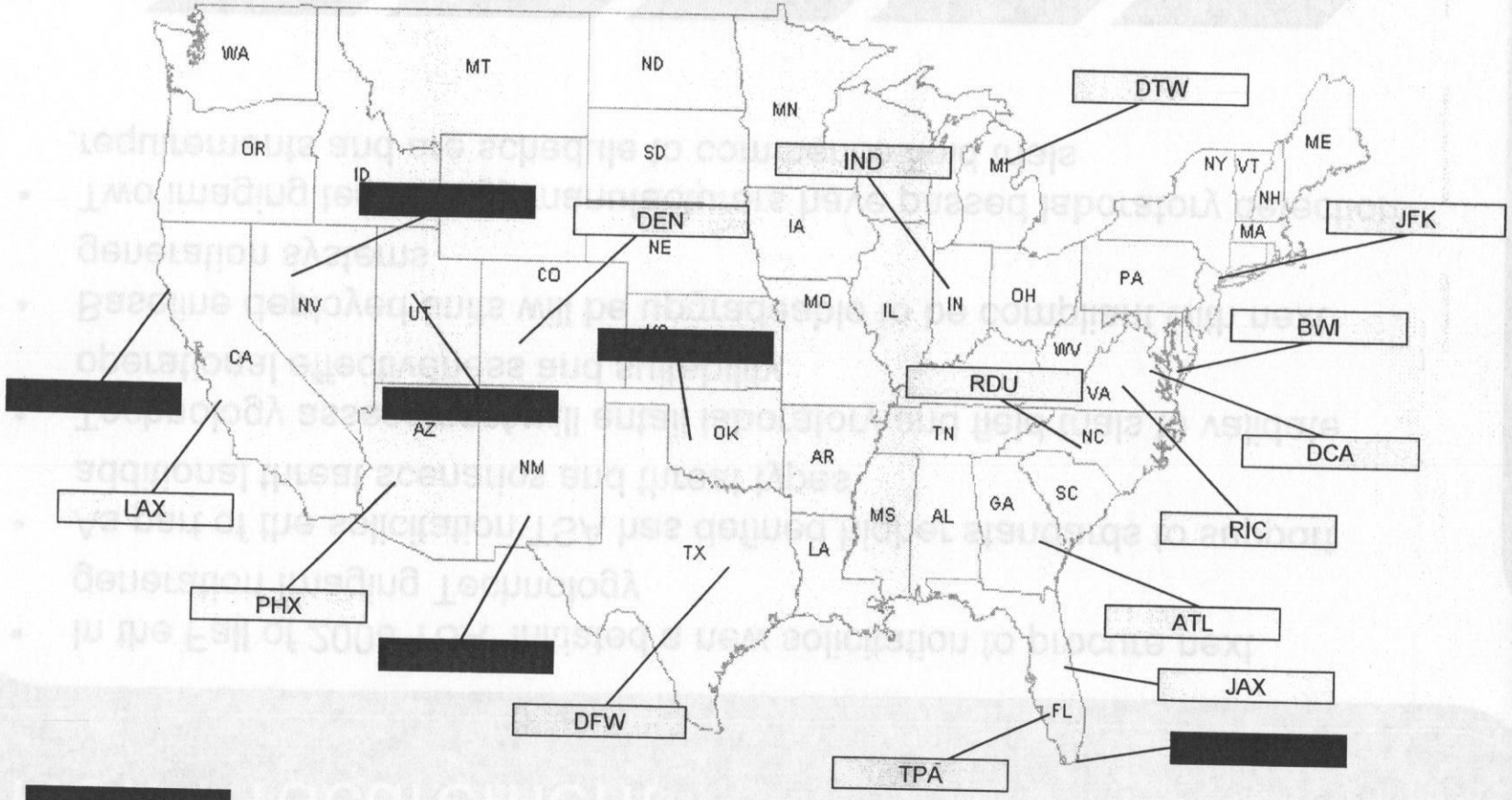
Transportation Security Administration

- ✓ Aug 2007 – Field Trials of MMW and Backscatter Passenger Imaging Technology units at JFK, LAX, & PHX in a secondary screening dual-scan configuration.
- ✓ Sept 2007 – TSA awarded contracts for a limited number of systems to MMW and Backscatter manufacturers for preliminary deployments to support extended surveillance.
- ✓ Apr 2008 – Completed deployment of 40 units in the secondary configuration.
- ✓ Spring 2009 – Re-deployment of 6 units to the primary screening configuration.

AR 000718

Current Locations

Transportation Security Administration



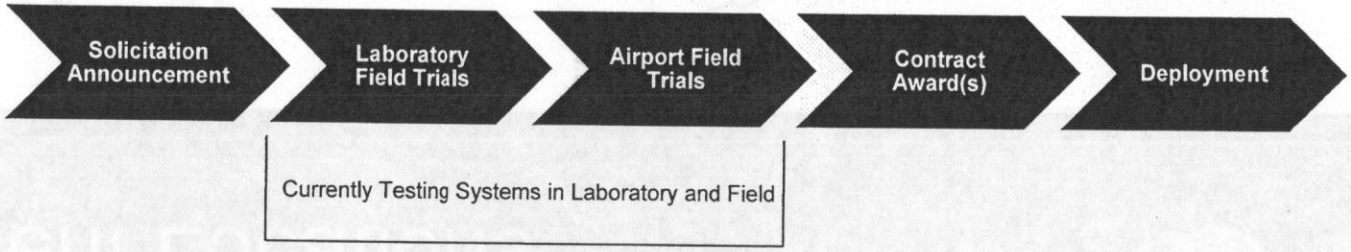
Slide 9

AR 000719

New Procurement

Transportation Security Administration

- In the Fall of 2008 TSA initiated a new solicitation to procure next generation Imaging Technology
- As part of the solicitation TSA has defined higher standards to support additional threat scenarios and threat types
- Technology assessment will entail laboratory and field trials to validate operational effectiveness and suitability
- Baseline deployed units will be upgradeable to be compliant with next generation systems
- Two imaging technology manufacturers have passed laboratory detection requirements and are schedule to commence field trials



AR 000720

Testing Update: Field Trials

Transportation Security Administration

- Summer 2009 – Field Trials of six Imaging Technology units (3 MMW & 3 Backscatter).
  - MMW technology includes enhanced software upgrades improving detection capabilities
  - Backscatter technology includes enhanced hardware upgrades improving detection and processing capabilities

- TSA is planning to go-live at the following locations:
  - BUR: 7/30 (L-3)
  - CLE: 7/31 (L-3 - MMW & Rapiscan- Backscatter)
  - IAH: 7/31 (L-3 & Rapiscan)
  - ROC: 8/1 (Rapiscan)

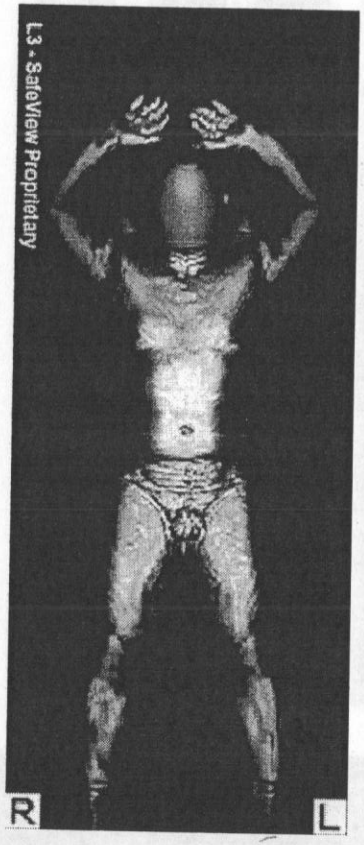
AR 000721

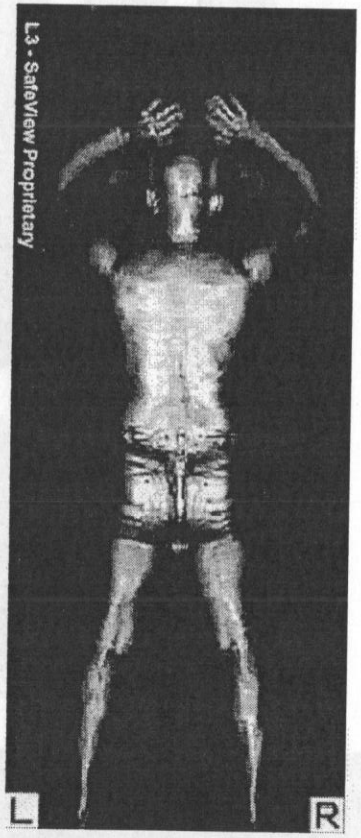
Transportation Security Administration

Appendix

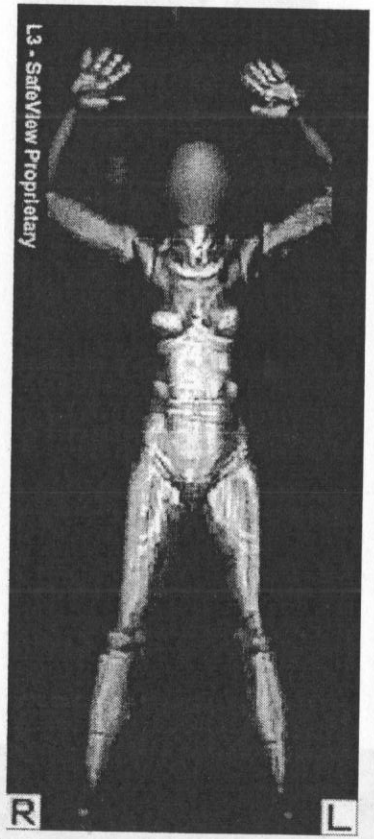
Millimeter Wave Image

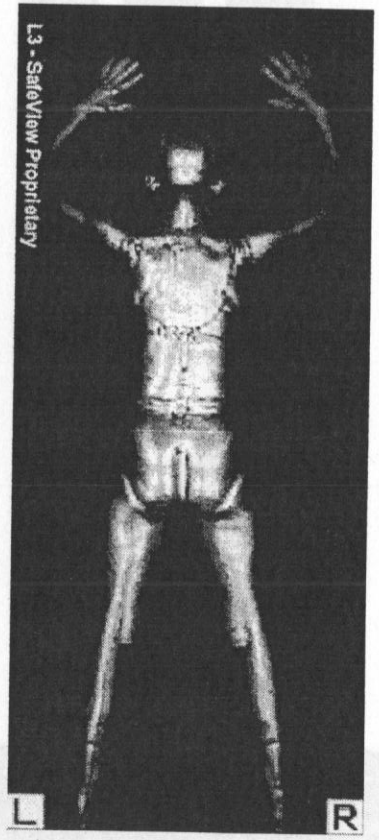
Transportation Security Administration





Male Front and Back





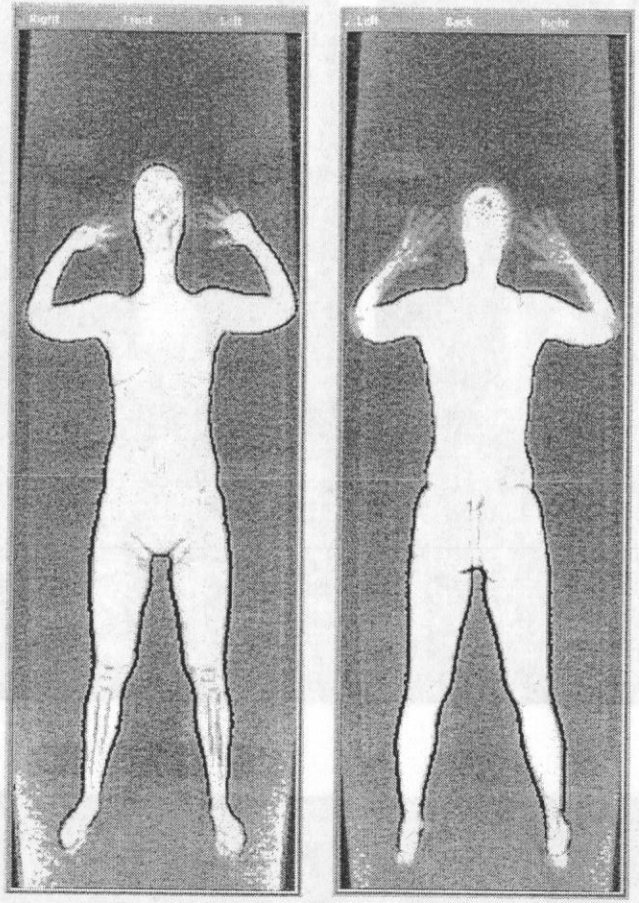
Female Front and Back

Slide 13

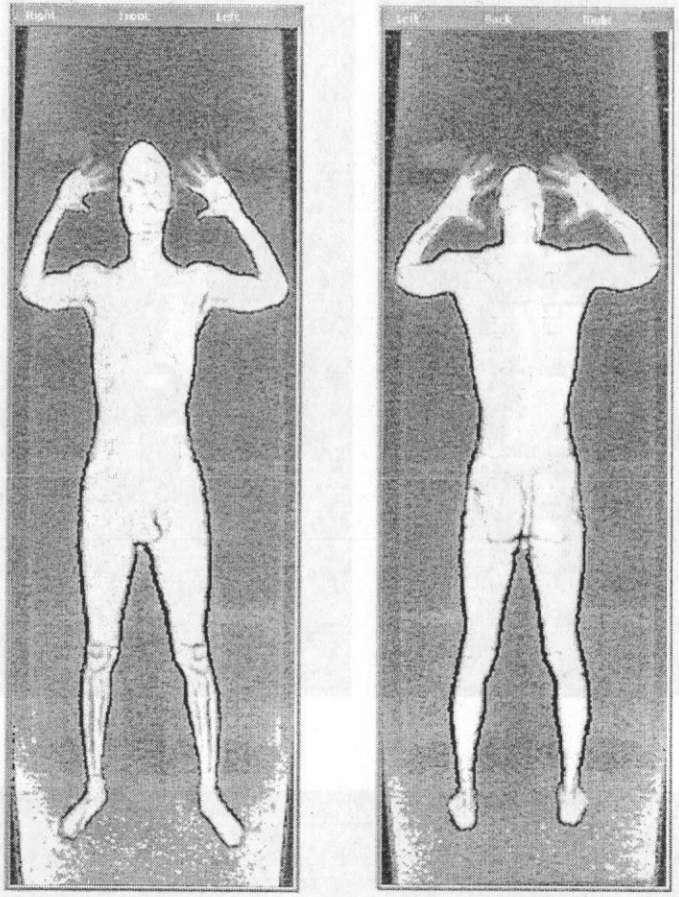
AR 000723

Backscatter Image

Transportation Security Administration



Female Front and Back



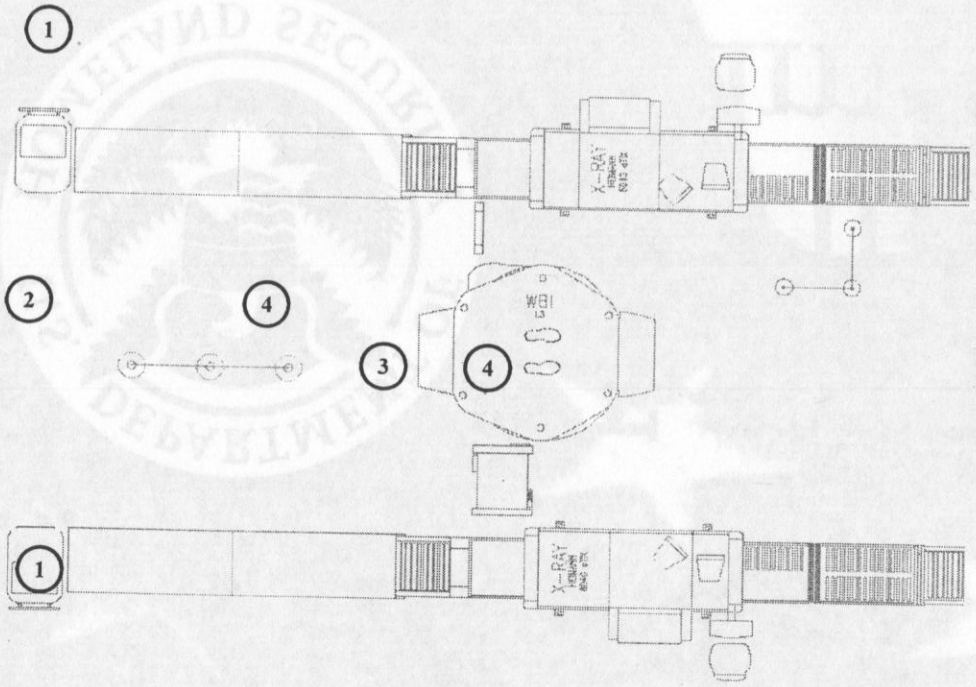
Male Front and Back

Slide 14

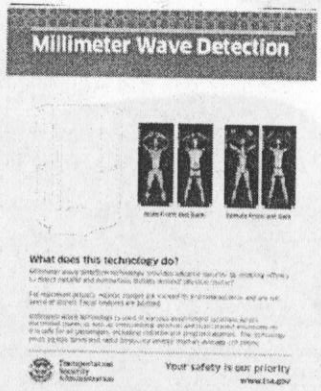
AR 000724

Signage

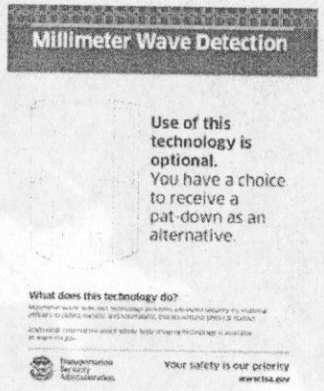
Transportation Security Administration



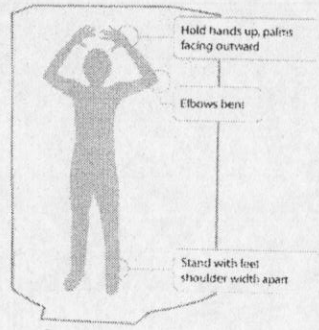
1



2



3



4

Slide 15

AR 000725

U.S. DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

TSA to Begin Testing Imaging Technology at George Bush Intercontinental Airport

Press Release

July 31, 2009

Contact: TSA Public Affairs
(571) 227-2829

HOUSTON – The Transportation Security Administration (TSA) announced today that it will begin testing two types of advanced imaging technology at George Bush Intercontinental Airport. Imaging technologies quickly and unobtrusively screen passengers for metallic and nonmetallic threats without physical contact.

Millimeter wave and backscatter imaging technologies provide enhanced detection capabilities and are 100 percent optional for all passengers. Both technologies have privacy protections in place for the traveler. The security officer who assists the passenger through the screening process never sees the image the technology produces. The image is viewed by a remotely located security officer who never sees the traveler. Further, these technologies cannot save, print, or transmit images. Once the image is deleted it cannot be restored. To further protect passenger privacy, millimeter wave technology blurs all facial features and backscatter has an algorithm applied to the entire image.

"State-of-the-art technologies like these are critical tools to ensure the safety of the traveling public," said Dempsey Jones, Acting Federal Security Director, George Bush Intercontinental Airport, Transportation Security Administration. "Imaging technology screens passengers quickly and with a high level of threat detection while managing privacy protections."

Millimeter wave technology uses harmless electromagnetic waves and 10,000 times less energy than a cell phone to perform a single scan. Backscatter technology uses low-level X-ray and a single scan is the equivalent of flying on an airplane for approximately two minutes. These technologies produce an image that allows TSA to remotely screen passengers for threats without physical contact. Imaging technology not only enhances security, it reduces the need for pat-down searches for passengers with joint replacements and other medical conditions.

At George Bush Intercontinental, TSA will assess the operational efficiency and public acceptance of these technologies as the primary screening technology in lieu of the traditional metal detector. Both technologies are 100 percent optional for all passengers. Passengers that choose not to be screened by imaging technology will receive a physical pat down. It is anticipated the test will last approximately 60 days.

WHY Imaging Technology

Imaging technology is a critical layer of security that enables TSA to screen passengers for a wide range of threats while maintaining passenger privacy. Layers of security, like this one, are integrated to mitigate risk and ensure the safety of the traveling public. For more information about imaging technology and a complete list of airports where it is in use, please visit www.tsa.gov.

Homeland Security

Secretary Napolitano Announces More than $355 Million in Recovery Act Funding for Airport Security Projects

Release Date: October 1, 2009

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Department of Homeland Security (DHS) Secretary Janet Napolitano today announced more than $355 million in funding for more than a dozen airport security projects funded by the American Recovery and Reinvestment Act (ARRA).

"These state-of-the-art technologies will bolster security and increase efficiency for both travelers and employees," said Secretary Napolitano. "Investing Recovery Act funds in these critical airport projects will create jobs in local communities while strengthening our efforts to guard against terrorism."

Secretary Napolitano announced approximately $254 million in ARRA funds for inline baggage handling systems at six airports—including Washington Dulles International Airport ($154 million); Mineta San Jose International Airport ($20.9 million); San Antonio International Airport ($14.4 million); Portland (Maine) International Jetport ($9.2 million); Port Columbus International Airport ($35.2 million); and Hartsfield-Jackson Atlanta International Airport ($20 million).

Inline baggage handling systems eliminate the need for passengers to walk checked baggage to a screening location and wait before proceeding to the security checkpoint, incorporate enhanced explosive detection technology to provide on-screen viewing capabilities for TSA officers conducting baggage screenings and reduce the number of re-scans and physical bag searches

In addition, Secretary Napolitano announced approximately $38 million in ARRA funds to support new and enhanced closed circuit television (CCTV) systems, which enhance surveillance capabilities at six airports—including Chicago Midway International Airport ($2.7 million); Little Rock National Airport/Adams Field ($5.9 million); Kansas City International Airport ($9.4 million); Omaha Eppley Airfield Airport ($3.6 million); Washington Dulles International Airport ($8.1 million); and Tampa International Airport ($8.1 million).

Secretary Napolitano also announced approximately $37 million in ARRA funds for the purchase and installation of multiple additional checkpoint technologies—including $15 million for Explosive Trace Detection (ETD) units, which detect traces of explosives; and $22 million for Bottled Liquid Scanners (BLS), a technology that screens medically necessary liquids such as infant formula and liquid medications to ensure they do not contain a threat.

More than $25 million will fund the purchase and deployment of approximately 150 backscatter advanced imaging units to airports across the nation—designed to bolster security by quickly screening passengers for concealed threats of all kinds without physical contact. This deployment follows a successful pilot phase, during which 46 imaging technology units were deployed at 23 airports and passengers opted to use imaging technology for primary screening 99 percent of the time.

In awarding ARRA funds, DHS prioritizes shovel-ready projects that infuse resources into local economies quickly while meeting critical security needs. DHS has obligated more than 50 percent of its ARRA funds to date—more than $1.5 billion.

ARRA, signed into law by President Obama on Feb. 19, committed more than $3 billion for homeland security projects through DHS and the General Services Administration (GSA). Of the $1 billion allocated to TSA for aviation security projects, $700 million was dedicated to screening checked baggage and $300 million was allocated for checkpoint

explosives detection technology and closed circuit television systems.

To learn more about the DHS Recovery Act projects, visit www.dhs.gov/recovery.

###

This page was last reviewed/modified on October 1, 2009.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

GAO

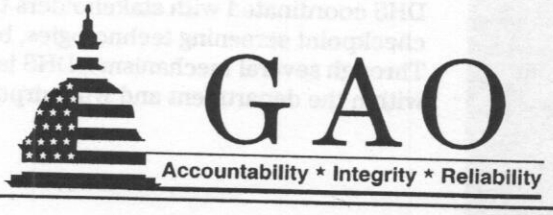
United States Government Accountability Office

Report to Congressional Requesters

October 2009

AVIATION SECURITY

DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges



GAO-10-128

October 2009

AVIATION SECURITY

DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-10-128, a report to congressional requesters

Why GAO Did This Study

Since fiscal year 2002, the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) have invested over $795 million in technologies to screen passengers at airport checkpoints. The DHS Science and Technology Directorate (S&T) is responsible, with TSA, for researching and developing technologies, and TSA deploys them. GAO was asked to evaluate the extent to which (1) TSA used a risk-based strategy to prioritize technology investments; (2) DHS researched, developed, and deployed new technologies, and why deployment of the explosives trace portal (ETP) was halted; and (3) DHS coordinated research and development efforts with key stakeholders. To address these objectives, GAO analyzed DHS and TSA plans and documents, conducted site visits to research laboratories and nine airports, and interviewed agency officials, airport operators, and technology vendors.

What GAO Recommends

GAO recommends, among other things, that TSA (1) conduct a risk assessment and develop a cost–benefit analysis and performance measures for passenger screening technologies, and (2) to the extent feasible, ensure that technologies have completed operational tests and evaluations before they are deployed. DHS concurred with the recommendations; however, its implementation plans do not fully address six of the eight recommendations in the report.

View GAO-10-128 or key components. For more information, contact Steve Lord at (202) 512-8777 or lords@gao.gov.

What GAO Found

TSA completed a strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies; however, the plan is not risk-based. According to TSA officials, the strategic plan and its underlying strategy for the Passenger Screening Program were developed using risk information, such as threat information. However, the strategic plan and its underlying strategy do not reflect some of the key risk management principles set forth in DHS's National Infrastructure Protection Plan (NIPP), such as conducting a risk assessment based on the three elements of risk—threat, vulnerability, and consequence—and developing a cost-benefit analysis and performance measures. TSA officials stated that, as of September 2009, a draft risk assessment for all of commercial aviation, the Aviation Domain Risk Assessment, was being reviewed internally. However, completion of this risk assessment has been repeatedly delayed, and TSA could not identify the extent to which it will address all three elements of risk. TSA officials also stated that they expect to develop a cost-benefit analysis and establish performance measures, but officials could not provide timeframes for their completion. Without adhering to all key risk management principles as required in the NIPP, TSA lacks assurance that its investments in screening technologies address the highest priority security needs at airport passenger checkpoints.

Since TSA's creation, 10 passenger screening technologies have been in various phases of research, development, test and evaluation, procurement, and deployment, but TSA has not deployed any of these technologies to airports nationwide. The ETP, the first new technology deployment initiated by TSA, was halted in June 2006 because of performance problems and high installation costs. Deployment has been initiated for four technologies—the ETP in January 2006, and the advanced technology systems, a cast and prosthesis scanner, and a bottled liquids scanner in 2008. TSA's acquisition guidance and leading commercial firms recommend testing the operational effectiveness and suitability of technologies or products prior to deploying them. However, in the case of the ETP, although TSA tested earlier models, the models ultimately chosen were not operationally tested before they were deployed to ensure they demonstrated effective performance in an operational environment. Without operationally testing technologies prior to deployment, TSA does not have reasonable assurance that technologies will perform as intended.

DHS coordinated with stakeholders to research, develop, and deploy checkpoint screening technologies, but coordination challenges remain. Through several mechanisms, DHS is taking steps to strengthen coordination within the department and with airport operators and technology vendors.

AR 000732

Contents

Letter		1
	Results in Brief	6
	Background	9
	TSA Has Taken Actions to Prioritize Investments in Passenger Checkpoint Screening Technologies, but Lacks a Risk-Based Strategy	18
	Ten New Checkpoint Screening Technologies Are in Various Phases of RDT&E, Procurement, and Deployment, but ETP Deployment Has Been Halted	31
	DHS Is Addressing Coordination and Collaboration Challenges with Stakeholders to Research, Develop, and Deploy Checkpoint Screening Technologies	41
	Conclusions	50
	Recommendations for Executive Action	51
	Agency Comments and Our Evaluation	52
Appendix I	**Objectives, Scope, and Methodology**	57
Appendix II	**Comments from the Department of Homeland Security**	60
Appendix III	**GAO Contact and Staff Acknowledgments**	70
Figures		
	Figure 1: TSA Passenger Checkpoint Screening Functions	11
	Figure 2: NIPP Risk Management Framework	16
	Figure 3: Status of Six Checkpoint Screening Technologies that Had Initiated Procurement and/or Deployment as of September 2008	33

Abbreviations

ADRA	Aviation Domain Risk Assessment
AMS	Acquisition Management System
ATSA	Aviation and Transportation Security Act
DHS	Department of Homeland Security
ETP	explosives trace portal
FAA	Federal Aviation Administration
IED	improvised explosive device
IPT	Integrated Product Team
MOU	memorandum of understanding
NIPP	National Infrastructure Protection Plan
PSP	Passenger Screening Program
RDT&E	research, development, test and evaluation
RMAT	Risk Management and Analysis Toolset
S&T	Science and Technology Directorate
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
TSO	Transportation Security Officer

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 7, 2009

The Honorable James L. Oberstar
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Jerry F. Costello
Chairman
Subcommittee on Aviation
Committee on Transportation and Infrastructure
House of Representatives

Commercial aircraft have long been a target of terrorism at the hands of hijackers and suicide bombers. The Transportation Security Administration (TSA), the agency with primary responsibility for securing the nation's civil aviation system after the September 11, 2001, terrorist attacks, has identified the need for improved technology to detect explosives and other threat items at airport passenger screening checkpoints to strengthen the nation's defenses against acts of terrorism. From fiscal years 2002 through 2008, over $795 million has been invested by TSA and the Department of Homeland Security (DHS) for the research, development, test and evaluation (RDT&E), procurement, and deployment of checkpoint screening technologies.

TSA has implemented a multilayered system of security to protect commercial aviation—the most publicly visible layer being the physical screening of passengers and their carry-on items at airport screening checkpoints. TSA's passenger checkpoint screening system—located at all airports regulated by TSA—is comprised of three elements: (1) the personnel, or screeners, responsible for conducting the screening of airline passengers and their carry-on items; (2) the procedures screeners are to follow to conduct screening; and (3) the technology used during the screening process. Collectively, these elements—the people, process and

technology—help to determine the effectiveness and efficiency of passenger checkpoint screening.[1] We previously reported that TSA had made efforts to enhance its passenger checkpoint screening system by strengthening screener training, measuring the performance of screeners and the screening system, and modifying screening procedures to address terrorist threats.[2]

Within DHS, 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, provides input to S&T during the research and development of new technologies, which TSA then procures and deploys.[3]

In 2004, we reviewed DHS's investments in the research and development of technologies to secure the transportation sector, including aviation, and found that DHS needed to strengthen the management of its research and development efforts.[4] In October 2007, we testified that a key challenge related to securing the homeland involves allocating resources based on

[1]TSA screeners are known as Transportation Security Officers and perform a variety of duties related to security and protection of air travelers, airports, and aircraft. TSA further oversees the operations of private sector screeners at airports participating in TSA's Screening Partnership Program.

[2]GAO, *Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains*, GAO-05-457 (Washington, D.C.: May 2, 2005); and *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved*, GAO-07-57SU (Washington, D.C.: March 7, 2007).

[3]In this report, we define basic research as including all scientific efforts and experimentation directed towards increasing knowledge and understanding; applied research as including all efforts directed toward— the solution of specific problems; advanced development as including all efforts directed toward projects that have moved into the development of hardware; and operational testing as verification that new systems are operationally effective, supportable, and suitable.

[4]GAO, *Transportation Security R&D: TSA and DHS Are Researching and Developing Technologies, but Need to Improve R&D Management*, GAO-04-890 (Washington, D.C.: September 30, 2004).

risk.[5] DHS and TSA leadership have identified that risk-informed considerations will be a cornerstone of departmental and agency policy. In particular, DHS's National Infrastructure Protection Plan (NIPP) stated that TSA should be considering risk management principles when allocating funding for the research and development of security technologies. According to the NIPP, security strategies should be informed by, among other things, a risk assessment that includes threat, vulnerability, and consequence assessments, information such as cost–benefit analyses to prioritize investments, and performance measures to assess the extent to which a strategy reduces or mitigates the risk of terrorist attacks.

In response to your request, this report provides the results of our review of DHS's efforts, through S&T and TSA, to research, develop, and deploy emerging screening technologies for use at airport passenger checkpoints by addressing the following questions: (1) To what extent has TSA developed a risk-informed strategy to prioritize investments in the research and development of passenger checkpoint screening technologies; (2) What new passenger checkpoint screening technologies has DHS researched, developed, tested and evaluated, procured, and deployed since its creation, and why did TSA halt the first technology deployment that it initiated—the explosives trace portal (ETP); and (3) To what extent has DHS coordinated the RDT&E, procurement, and deployment of passenger checkpoint screening technologies internally and with key stakeholders, such as airport operators and technology vendors?

This report is a public version of a restricted report (GAO-09-21SU) that we provided to you earlier this year. In this report in three cases we provide updates regarding the Aviation Domain Risk Assessment (ADRA),

[5]GAO, *Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security Are Under Way, but Challenges Remain*, GAO-08-140T (Washington, D.C.: October 16, 2007).

the NIPP, and the number of ETPs in airports.[6] DHS and TSA deemed some of the information in the restricted report to be sensitive security information, which must be protected from public disclosure. Although this report omits that information, such as specific details associated with the methods and results of testing during the research and development of the ETPs, it addresses the same questions as the restricted report. Also, the overall methodology used for both reports is the same.

To determine the extent to which TSA developed a risk-informed strategy to prioritize investments in the research and development of new checkpoint technologies, we analyzed program documents, including TSA's August 2008 strategic plan for checkpoint technologies, technology project plans, and budget documents. We also compared TSA's strategic plan and DHS's responses regarding their efforts to develop a risk-informed strategy for their research and development investments with DHS's guidance on using risk management principles to prioritize investments and allocate resources.

To determine what new passenger checkpoint screening technologies DHS has researched, developed, tested and evaluated, procured, and deployed, and the reasons why TSA halted the first technology for which it initiated deployment—the ETP, we analyzed TSA's strategic plan, TSA's PSP documentation, technical and operational requirements for new technologies, laboratory test reports, and testing data from operational pilots. Additionally, we interviewed TSA and S&T officials to obtain information on current technologies being researched, developed, and deployed, and conducted site visits to the Transportation Security Laboratory (TSL) and Tyndall Air Force Base to observe testing of new checkpoint technologies. We visited the TSL because that is where S&T tests and evaluates transportation technologies, including checkpoint

[6] In the April 2009 restricted version of this report, we reported that, as of September 2008, TSA officials could not provide an expected completion date or identify the extent to which the ADRA would address risks to the checkpoint. In this public report on pages 7, 18, and 22, we updated this information and stated that, as of September 2009, TSA officials expected the ADRA to be completed by the end of 2009, but could not identify the extent to which the ADRA would address risks to the checkpoint. Also, in the restricted version of this report, we reported that the NIPP was issued in 2006. In this public report on page 15, we updated this information and stated that DHS issued a new version of the plan in 2009. Furthermore, in the restricted version of this report, we reported that, as of April 2009, TSA had 90 ETPs at airports and 116 ETPs in storage. In this report on page 39, we updated this information and stated that, as of September 2009, 22 ETPs were at airports and no ETPs were in storage.

screening technologies. We visited Tyndall Air Force Base because technologies to detect bottled liquids explosives were being tested there. We also interviewed TSA headquarters officials and senior TSA officials from the airports where TSA had initially deployed or planned to deploy the ETPs, including 29 Federal Security Directors, 1 Deputy Federal Security Director, and 5 Assistant Federal Security Directors for Screening.[7] We chose these officials because they are the senior TSA officials in charge of security and managing TSA's role in deploying new technologies at the airport. We also visited nine airports and selected these locations based on the technologies that had been deployed or were being tested on site, their geography, size, and proximity to research and development laboratories. Of the nine airports we visited, the ETPs had been deployed or were to be deployed to all of them and other new checkpoint screening technologies were undergoing pilot demonstrations or testing at two of them. We visited four airports on the east coast, three airports on the west coast, and two airports located in the west and southwestern regions of the United States. We selected these locations because they represented small-, medium-, and large-sized airports and different regions in the United States.

To determine the extent to which TSA coordinated and collaborated internally and with key external stakeholders—airport operators and technology vendors—on the RDT&E, procurement, and deployment of checkpoint technologies, we analyzed program documents, including a memorandum of understanding (MOU) between S&T and TSA. Additionally, we interviewed S&T and TSA officials, seven checkpoint technology vendors, and airport operators[8] and other officials at 40 airports where ETPs had initially been or were to be deployed. Because we selected a nonprobability sample of airports to visit and officials to interview there, we cannot generalize the results of what we learned to airports nationwide. However, the information we gathered from these locations—insights based on observing airport operations and on perspectives of officials who were involved with DHS's efforts to operationally test, evaluate, and deploy checkpoint technologies—could only be obtained through direct observation or from officials stationed at

[7]A Federal Security Director is the ranking TSA authority responsible for the leadership and coordination of TSA security activities at TSA-regulated airports.

[8]TSA defines "airport operator" as any person who operates an airport serving an aircraft operator or foreign air carrier required to have a security program under 49 C.F.R. parts 1544 or 1546. See 49 C.F.R. § 1540.5.

these select sites where technologies were being deployed and tested. We also selected a nonprobability sample of 8 out of the 157 total requirements for the ETP to determine whether some of its key requirements had been tested prior to procuring and deploying the machines.[9] In addition, we reviewed S&T's and TSA's coordination and collaboration activities and compared them to TSA program guidance and leading practices for collaborating agencies regarding communication, planning, and federal coordination internally and with external stakeholders.[10] Appendix I contains additional information on the objectives, scope, and methodology of our review.

We conducted this performance audit from June 2006 through April 2009, with some updated information as of September 2009 as previously disclosed, 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 and conclusions based on our audit objectives.

Results in Brief

TSA completed a strategic plan in August 2008, which identified a strategy to invest in the RDT&E, procurement, and deployment of passenger checkpoint screening technologies; however, the plan and its underlying strategy are not risk informed. TSA's strategy does not incorporate some key risk management principles—a risk assessment, cost-benefit analysis, and performance measures—as required by the NIPP. To guide investments in checkpoint screening technologies, TSA officials stated that they consider risks to the checkpoint by analyzing threat information and other factors. However, this approach does not address all three risk elements required by the NIPP, which specifies that risk assessments are to be based on threat, vulnerability, and consequence assessments. Officials stated that they have drafted the Aviation Domain Risk Assessment (ADRA), a risk assessment of the entire aviation sector, including the passenger checkpoint, which is to include an assessment of all three risk elements. TSA officials anticipated finalizing the ADRA in

[9]We selected the eight requirements because they were related to some of the ETP's key functionality requirements, including operational effectiveness, operational suitability, and passenger throughput.

[10]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 21, 2005).

February 2008, but have postponed its completion multiple times. As of September 2009, officials expected completion of the ADRA by the end of calendar year 2009, but could not identify the extent to which the ADRA would address risks to the checkpoint. Therefore, we could not determine when the ADRA will be completed, to what extent it will incorporate all three elements of a risk assessment, and whether it will identify and assess risks to the checkpoint. In addition, TSA officials stated that they have not yet conducted a cost–benefit analysis to set priorities for the PSP, or established performance measures that assess how deployed technologies have reduced or mitigated risk, as required by the NIPP. Officials acknowledged that a cost–benefit analysis and performance measures should be completed; however, they could not provide timeframes for completing them. Without incorporating these DHS risk management principles into the PSP strategy, TSA cannot ensure that it is targeting the highest priority security needs at checkpoints; measure the extent to which deployed technologies reduce the risk of terrorist attacks; or make needed adjustments to its PSP strategy.

S&T and TSA have placed 10 new checkpoint screening technologies in various phases of RDT&E, procurement, and deployment, but halted the deployment of the ETP due to performance problems and high installation costs. TSA has initiated, but not yet completed, deployments of 4 of the 10 technologies; initiated procurements, but not yet deployed, 2 more technologies, including the Whole Body Imager; and has 4 additional technologies, including a shoe scanner, in research and development. In 2006, TSA deployed 101 ETPs to airports, the first deployment of a checkpoint technology initiated by the agency.[11] The ETP was deployed even though TSA officials were aware that tests conducted during 2004 and 2005 on earlier ETP models suggested they did not demonstrate reliable performance in an airport environment. Furthermore, the ETP models that were subsequently deployed were not first tested to prove their effective performance in an operational environment, contrary to TSA's acquisition guidance, which recommends such testing. As a result, TSA lacked assurance that the ETP would meet its functional requirements in airports. TSA officials stated that they deployed the machines without resolving these issues to respond quickly to the threat of suicide bombers. After being deployed, the ETPs broke down frequently

[11]TSA deployed the ETPs from January to June 2006. Since June 2006, TSA removed 11 ETPs from airports due to maintenance issues and placed the ETPs in a warehouse for storage.

and were more expensive to maintain than expected, according to TSA officials. TSA continued to use them at checkpoint lanes even though TSA could not identify whether ETPs were more effective than existing screening procedures. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security.

DHS S&T and TSA share responsibilities related to the RDT&E, procurement, and deployment of checkpoint screening technologies, and have coordinated and collaborated with each other and key external stakeholders; however, coordination and collaboration challenges remain that DHS is addressing. The Homeland Security Act of 2002 and the Aviation and Transportation Security Act, which established DHS and TSA, respectively, each address the need for coordination and collaboration with stakeholders. S&T and TSA coordination efforts include a 2006 memorandum of understanding for using the TSL, and the establishment of the Capstone Integrated Product Team for Explosives Prevention in 2006 to help DHS, TSA, and the U.S. Secret Service to, among other things, identify priorities for explosives prevention. However, S&T and TSA officials stated that some technology projects were delayed because TSA had not consistently communicated clear requirements to S&T to test technologies, and S&T had not consistently communicated to TSA about projects at the TSL or the time frames to complete them. According to S&T and TSA officials, coordination and collaboration between them has improved since the summer of 2007. TSA has also taken steps to build partnerships with airport operators and technology vendors, such as by hosting conferences with them; however, the agency has not established a systematic process for coordinating with these stakeholders related to passenger checkpoint technologies. For example, 11 of 33 airport operators[12] and 4 of 7 vendors we interviewed told us that TSA had not solicited or shared information with them regarding checkpoint technology needs and priorities. TSA officials acknowledged the need to improve relationships with external stakeholders. According to TSA officials, an Industry Outreach Manager was hired in 2007 and a draft communications plan to provide guidance and a more systematic process to coordinate with these stakeholders is being reviewed, but no completion date could be provided.

[12]We interviewed 46 airport operators, but 13 of them did not express an opinion about whether TSA had shared or solicited information regarding research and development needs and priorities for checkpoint technologies.

To help ensure that DHS's S&T and TSA take a comprehensive, risk-informed approach to the RDT&E, procurement, and deployment of passenger checkpoint screening technologies, and to increase the likelihood of successful procurements and deployments of such technologies, in the restricted version of this report, we recommended that TSA conduct a complete risk assessment, including threat, vulnerability and consequence assessments, that would apply to the PSP; develop cost–benefit analyses to assist in prioritizing investments in new checkpoint technologies; develop quantifiable performance measures to assess the extent to which investments in research and development have mitigated the risks of a terrorist attack; determine if changes need to be made to the PSP strategy as a result of the risk assessment, cost–benefit analyses, and performance measures; to the extent feasible, ensure that operational testing has been successfully completed before deploying checkpoint technologies to airports; and evaluate the benefits and costs of the ETPs currently being used in airports in order to determine whether it is cost effective to continue to use the machines. In written comments on our report, DHS stated that it agreed with our recommendations and identified actions planned or underway to implement them. While DHS is taking steps to address our first and second recommendations related to conducting a risk assessment and cost-benefit analysis, the actions DHS reported TSA had taken or plans to take do not fully address the intent of the remaining recommendations. DHS also provided us with technical comments, which we considered and incorporated in the report where appropriate. In particular, we clarified the wording of a recommendation which originally stated that TSA should develop quantifiable performance measures to assess the extent to which investments in checkpoint screening technologies mitigated the risks of a terrorist attack. We altered the wording to state that performance measures should be developed to assess progress towards security goals.

Background

TSA's airport passenger checkpoint screening system is comprised of three elements: the (1) personnel, or screeners, responsible for operating the checkpoint, including the screening of airline passengers and their carry-on items; (2) standard operating procedures that screeners are to follow to conduct screening; and (3) technology used during the screening process. Collectively, these elements determine the effectiveness and efficiency of passenger checkpoint screening. In strengthening one or more elements of its checkpoint screening system, TSA aims to balance its security goals with the need to efficiently process passengers. We previously reported that TSA had made progress in enhancing its passenger checkpoint screening system by strengthening screener training, measuring the performance of screeners and the screening

system, and modifying screening procedures to address terrorist threats and efficiency concerns.[13] We made recommendations to DHS designed to strengthen TSA's efforts to train screeners, modify screening standard operating procedures, and measure the performance of the checkpoint screening system. DHS generally agreed with our recommendations and TSA has taken steps to implement them.

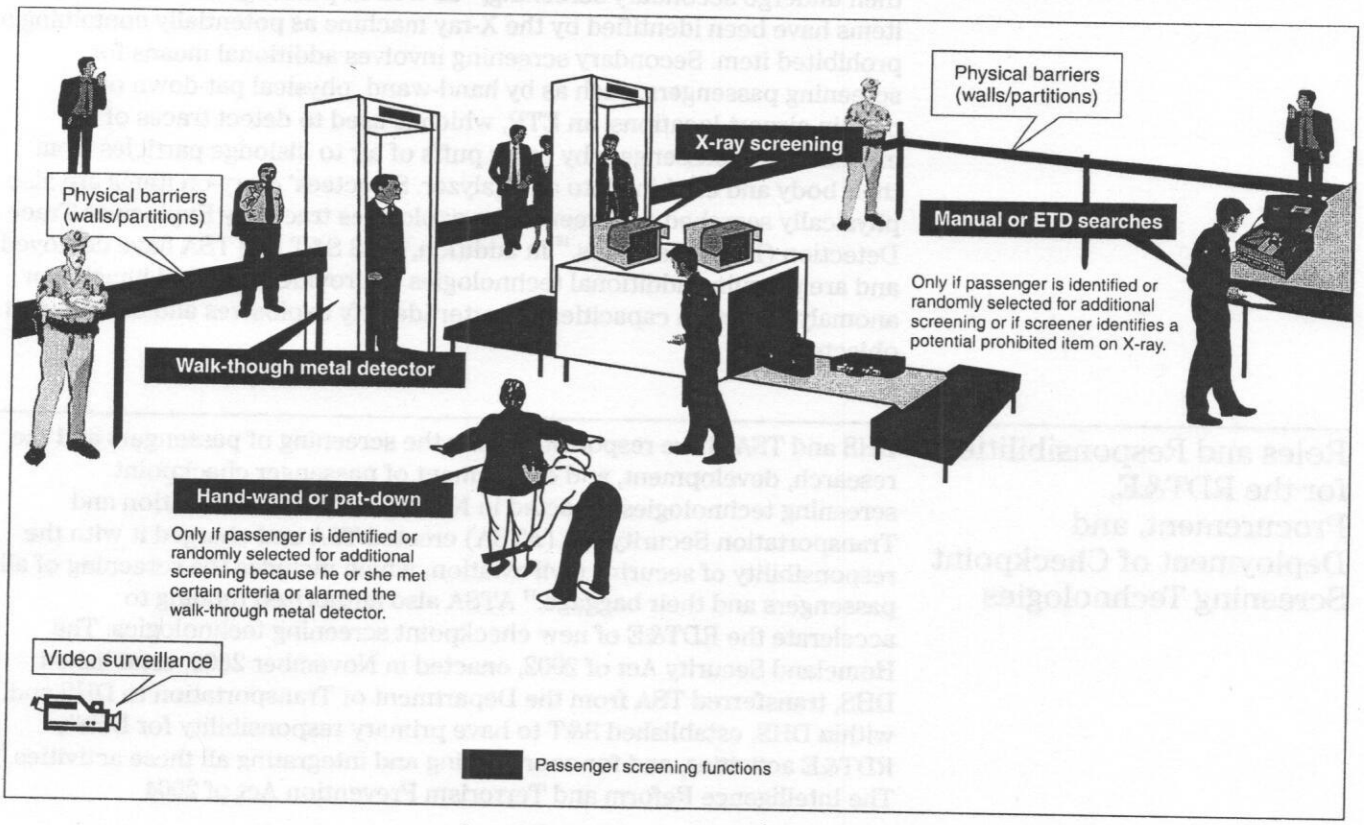
Passenger Checkpoint Screening Process

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 carriage of any unauthorized explosive, incendiary, weapon, or other prohibited item onboard an aircraft or into a sterile area.[14] Screeners inspect individuals for prohibited items at designated screening locations. TSA developed standard operating procedures and the process for screening passengers at airport checkpoints. Figure 1 illustrates the screening functions at a typical passenger checkpoint.

[13]See GAO-05-457 and GAO-07-57SU. We found that TSA had initiated actions designed to enhance screener training; however, screeners sometimes encountered difficulty accessing and completing training due to technological and staffing constraints. We also found that TSA had implemented and strengthened efforts to collect screener and checkpoint performance data through covert testing and a screener recertification program. We further reported that TSA modified standard operating procedures based on risk information, airport staff experiences, and complaints and concerns made by the traveling public, but that TSA could strengthen data collection and analysis to assist in determining whether proposed procedures would achieve their intended purpose.

[14]Sterile areas are generally located within the terminal where passengers are provided access to boarding aircraft and access is controlled in accordance with TSA requirements. Access is controlled by screeners—either Transportation Security Officers employed by TSA or nonfederal screeners at airports participating in TSA's Screening Partnership Program—at checkpoints where screening is conducted of individuals and carry-on baggage for weapons, explosives, and other prohibited items. Screeners must deny passage beyond the screening location to any individual or property that has not been screened or inspected in accordance with measures and procedures in place at that checkpoint. If an individual refuses inspection or the inspection of any item, that person or item may not be allowed to enter the sterile area or to board an aircraft.

Figure 1: TSA Passenger Checkpoint Screening Functions



Source: GAO and Nova Development Corporation.

[a]Explosives trace detection (ETD) machines detect small amounts of explosives on or in passenger's carry-on items. ETDs work by detecting vapors and residues of explosives. Human operators collect samples by rubbing bags with swabs, which are chemically analyzed to identify any traces of explosives material.

Primary screening is conducted on all airline passengers prior to entering 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,[15] as well as passengers whose carry-on items have been identified by the X-ray machine as potentially containing a prohibited item. Secondary screening involves additional means for screening passengers, such as by hand-wand, physical pat-down or, at certain airport locations, an ETP, which is used to detect traces of explosives on passengers by using puffs of air to dislodge particles from their body and clothing into an analyzer. Selectees' carry-on items are also physically searched or screened for explosives traces by Explosives Trace Detection (ETD) machines.[16] In addition, DHS S&T and TSA have deployed and are pursuing additional technologies to provide improved imaging or anomaly detection capacities to better identify explosives and other threat objects.

Roles and Responsibilities for the RDT&E, Procurement, and Deployment of Checkpoint Screening Technologies

DHS and TSA share responsibility for the screening of passengers and the research, development, and deployment of passenger checkpoint screening technologies. Enacted in November 2001, the Aviation and Transportation Security Act (ATSA) created TSA and charged it with the responsibility of securing civil aviation, which includes the screening of all passengers and their baggage.[17] ATSA also authorized funding to accelerate the RDT&E of new checkpoint screening technologies. The Homeland Security Act of 2002, enacted in November 2002, established DHS, transferred TSA from the Department of Transportation to DHS and, within DHS, established S&T to have primary responsibility for DHS's RDT&E activities, and for coordinating and integrating all these activities.[18] The Intelligence Reform and Terrorism Prevention Act of 2004

[15]A nonselectee passenger who alarms the walk-through metal detector on the first pass is offered a second pass. If the passenger declines the second pass through, the passenger must proceed to additional screening. If the nonselectee passenger accepts the second pass and the machine does not alarm, the passenger may generally proceed without further screening.

[16]Passengers are also screened by Behavior Detection Officers under the Screening of Passengers by Observation Techniques (SPOT) program and by Travel Document Checkers. SPOT is an additional layer of security using behavior observations and analysis techniques to identify potentially high-risk individuals based on deviations from environmental baselines. Behavior Detection Officers are tasked with detecting individuals exhibiting behaviors that indicate they may be a threat to aviation and/or transportation security. Travel Document Checkers are specially trained screeners who are positioned in front of the checkpoint to check passengers' boarding passes and identification in order to determine the authenticity of these documents.

[17]See Pub. L. No. 107-71, 115 Stat. 597 (2001).

[18]See Pub. L. No. 107-296, § 302, 116 Stat. 2135, 2163-64 (2002).

(Intelligence Reform Act), enacted in December 2004, directed the Secretary of Homeland Security to give high priority to developing, testing, improving, and deploying checkpoint screening equipment that detects nonmetallic, chemical, biological, and radiological weapons and explosives, in all forms, on individuals and in their personal property.[19]

Until fiscal year 2006, TSA had primary responsibility for investing in the research and development of new checkpoint screening technologies, and was responsible for developmental and operational test and evaluation of new technologies.[20] However, during fiscal year 2006, research and development functions within DHS were consolidated, for the most part, within S&T.[21] After this consolidation, S&T assumed primary responsibility for funding the research, development, and developmental test and evaluation of airport checkpoint screening technologies. S&T also assumed responsibility from TSA for the Transportation Security Laboratory (TSL) which, among other things, tests and evaluates technologies under development. TSA, through the PSP that was transferred from the Federal Aviation Administration (FAA) to TSA, continues to be responsible for identifying the requirements for new checkpoint technologies; operationally testing and evaluating technologies in airports; and procuring, deploying, and maintaining technologies. This transfer of responsibility from TSA to S&T did not limit TSA's authority to acquire commercially available technologies for use at the checkpoint.

DHS and TSA's Processes for the RDT&E, Procurement, and Deployment of Checkpoint Screening Technologies

S&T and TSA's RDT&E, procurement, and deployment efforts are made up of seven components: basic research, applied research, advanced development, operational testing, procurement, operational integration, and deployment. S&T is responsible for conducting basic and applied research, and advanced development, including developmental test and evaluation. TSA is responsible for conducting operational test and evaluation, operational integration, procurement and deployment of new

[19]See Pub. L. No. 108-458, § 4013(a), 118 Stat. 3638, 3719-20 (2004) (codified at 49 U.S.C. § 44925(a)).

[20]Developmental testing is conducted to assist in the development and maturation of a system or subsystem to verify the status of technical progress and certify readiness to enter initial operational testing. Operational testing verifies that new systems are operationally effective, supportable, and suitable before deployment.

[21]DHS undertook to coordinate and integrate most of its research, development, demonstration, testing, and evaluation activities in accordance with section 302(12) of the Homeland Security Act.

technologies, including checkpoint screening technologies. These seven components are described below.

- *Basic research* includes scientific efforts and experimentation directed toward increasing knowledge and understanding in the fields of physical, engineering, environmental, social, and life sciences related to long-term national needs.
- *Applied research* includes efforts directed toward solving specific problems with a view toward developing and evaluating the feasibility of proposed solutions.
- *Advanced development* includes efforts directed toward projects that have moved into the development of hardware and software for field experiments and tests, such as acceptance testing.[22]
- *Operational test and evaluation* verifies that new systems are operationally effective, supportable, and suitable before deployment.
- *Operational integration* is the process employed to enable successful transition of viable technologies and systems to the field environment.
- *Procurement* includes the efforts to obtain a product or service.[23]
- *Deployment* is a series of actions following the determination that the product meets its requirements and is accepted by the program manager and integrated product team; designated locations are configured for product integration into the screening operating system and the installed product passes site acceptance tests; and logistics support is in place and all users are trained to use the product.

RDT&E, Procurement, and Deployment Funding for Checkpoint Screening Technologies

Over $795 million has been invested by DHS and TSA during fiscal years 2002 through 2008 for the RDT&E, procurement, and deployment of checkpoint screening technologies. During this time, over $91 million was invested in the RDT&E of checkpoint technologies and about $704 million was invested in the procurement and deployment of these technologies. From fiscal years 2002 through 2005, TSA was responsible for the RDT&E of checkpoint technologies; however, TSA officials could not identify the

[22]Acceptance testing consists of testing conducted to determine whether a system or, in this case, technology satisfies its acceptance criteria, such as specification requirements, and to enable the customer to determine whether to accept the system or technology.

[23]According to TSA officials, depending on the requirements of the sought-after technology and how it will be used, S&T and TSA first try to identify commercial-off-the-shelf (COTS) equipment that meets identified requirements without having to modify it. If COTS equipment is identified but must be modified to meet TSA's needs, it would only be used if it could be modified within a reasonable cost and time frame. If COTS equipment cannot be identified or cannot be modified to meet TSA's requirements within a reasonable cost or time frame, S&T would try to develop a new technology for TSA.

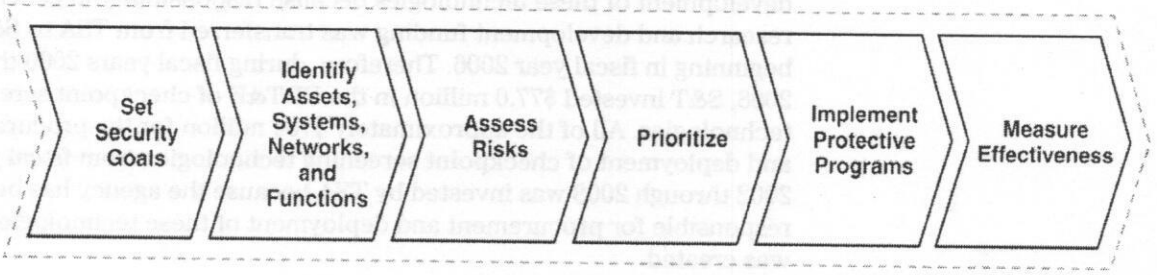
amount of funding the agency invested for these purposes during those years. After fiscal year 2005, TSA invested $14.5 million for test and evaluation of checkpoint technologies, but did not fund the research and development of these technologies because responsibility in general for research and development funding was transferred from TSA to S&T beginning in fiscal year 2006. Therefore, during fiscal years 2006 through 2008, S&T invested $77.0 million in the RDT&E of checkpoint screening technologies. All of the approximately $704 million for the procurement and deployment of checkpoint screening technologies from fiscal years 2002 through 2008 was invested by TSA because the agency has been responsible for procurement and deployment of these technologies since it was created.

Applying a Risk Management Approach to Checkpoint Technology Investments

Risk management is a tool that policy makers can use to help ensure that strategies to develop protective programs and allocate resources target the highest priority security needs. This information helps officials determine which security programs are most important to develop and fund, given that it is not possible to protect the country against all threats because of limited resources. Law and related policy, including the Intelligence Reform Act, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), and Homeland Security Presidential Directive 7, provide that federal agencies with homeland security responsibilities are to apply risk-informed principles to prioritize security needs and allocate resources. Consistent with these provisions, DHS issued the National Strategy for Transportation Security in 2005 that, among other things, describes the policies that DHS is to apply when managing risks to the security of the U.S. transportation system. Further, in June 2006, DHS issued the NIPP, which provides a risk management framework to guide strategies to develop homeland security programs and allocate resources to them.[24] According to the NIPP, its risk management framework consists of six phases that help to identify and assess risks and prioritize investments in programs, as illustrated in figure 2. The NIPP designated TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector.

[24]DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). In 2009, DHS issued an updated plan that replaced the one issued in 2006.

Figure 2: NIPP Risk Management Framework



Source: DHS.

A risk-informed strategy to develop and invest in critical infrastructure protection, according to the NIPP, begins with setting security goals. Setting security goals involves defining specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture. Once security goals are established, decisionmakers are to identify what assets or systems to protect and identify and assess the greatest risks to them, that is, the type of terrorist attack that is most likely to occur and that would result in the most severe consequences. Risk of a terrorist attack, according to the NIPP, is to be assessed by analyzing consequences of an attack; the threat—that is, the likelihood of an attack; and the extent to which an asset or a system, in this case the transportation system, is vulnerable to this type of attack.[25] The potential consequences of any incident, including terrorist attacks and natural or manmade disasters, is the first factor to be considered in a risk assessment. In the context of the NIPP, consequence is measured as the range of loss or damage that can be expected in the event a terrorist attack succeeds. A consequence assessment looks at the expected worst case or reasonable worst case impact of a successful attack. A threat assessment is the identification and evaluation of adverse events that can harm or damage an asset and takes into account certain factors, such as whether the intent and capability to carry out the attack exist. A vulnerability assessment identifies weaknesses or characteristics of an asset or system, such as its design and location, which make it susceptible to a terrorist

[25]DHS has adopted an all-hazards mission, which includes both natural disasters and terrorism. The department uses the NIPP to assess risk for both; however, in the context of this report, we are focusing on terrorism. The NIPP provides that for some critical infrastructure sectors, assessing system risk is more appropriate.

attack and that may be exploited. This analysis should also take into consideration factors such as protective measures that are in place which may reduce the risk of an attack and the system's resiliency, that is, ability to recover from an attack.

Once the three components of risk—threat, vulnerability, and consequence—have been assessed for a given asset or system, they are used to provide an estimate of the expected loss considering the likelihood of an attack or other incident. According to the NIPP, calculating a numerical risk score using comparable, credible methodologies provides a systematic and comparable estimate of risk that can help inform national and sector-level risk management decisions. To be considered credible, the NIPP states that a methodology must have a sound basis; be complete; be based on assumptions and produce results that are defensible; and specifically address the three variables of the risk calculus: threat, vulnerability, and consequence. The methodology should also be comparable with other methodologies to support a comparative sector or national risk assessment. To be comparable, a methodology must be documented, transparent, reproducible, accurate, and provide clear and sufficient documentation of the analysis process and the products that result from its use.

The next steps in the DHS risk management framework involve establishing priorities for program development based on risk assessments; implementing these protective programs; and measuring their effectiveness by developing and using performance measures. Identifying and assessing risks helps decisionmakers to identify those assets or systems that are exposed to the greatest risk of attack and, based on this information, prioritize the development and funding of protective programs that provide the greatest mitigation of risk given available resources. The NIPP notes that because resources are limited, risk analysis must be completed before sound priorities can be established. To determine which protective measures provide the greatest mitigation of risk for the resources that are available, the NIPP directs policy makers to evaluate how different options reduce or mitigate threat, vulnerability, or consequence of a terrorist attack. To do so, the NIPP states that cost estimates are combined with risk-mitigation estimates in a cost–benefit analysis to choose between the different options. The last step in the NIPP, measuring the effectiveness of security programs by developing and using performance measures, provides feedback to DHS on its efforts to attain its security goals. Performance metrics are to be developed and used to affirm that specific goals and objectives are being met or to articulate gaps in the national effort or supporting sector efforts. Performance measures

enable the identification of corrective actions and provide decisionmakers with a feedback mechanism to help them make appropriate adjustments in their strategies for protecting critical infrastructure.

TSA Has Taken Actions to Prioritize Investments in Passenger Checkpoint Screening Technologies, but Lacks a Risk-Based Strategy

While TSA completed a strategic plan for the PSP in August 2008 that identifies a strategy for researching, developing, and deploying checkpoint screening technologies, the plan and the strategy were not developed based upon all of the key risk management principles outlined in DHS's NIPP. For instance, TSA has not conducted a complete risk assessment for the PSP, conducted a cost–benefit analysis to prioritize investments, or developed performance measures to assess the extent to which the risk of attack has been reduced or mitigated by investments in technologies. While the agency is currently reviewing a draft of the Aviation Domain Risk Assessment (ADRA), as of September 2009, the ADRA had not been finalized. Officials expect it to be finalized by the end of calendar year 2009. TSA officials could not provide an expected completion date. Therefore, we could not determine when TSA will complete it or to what extent it will be consistent with DHS's risk management framework. TSA officials acknowledged the importance of a cost–benefit analysis and performance measures to guide technology investments, and stated that they intend to develop them, but could not identify when they would be completed. Until TSA completes these activities, the agency lacks assurances that the PSP strategy addresses the highest priority needs and mitigates the risk of an attack. Further, TSA lacks information to adjust its strategy, if needed.

TSA Completed a Strategic Plan for the PSP that Identifies Goals and Objectives

TSA completed a strategic plan in August 2008 that identifies a strategy and establishes goals and objectives for the PSP, and submitted the plan to congressional committees in September 2008.[26] However, TSA officials stated that the NIPP was not used as guidance in developing the plan. Instead, the officials stated that the specific requirements for a strategic plan, as outlined in the Intelligence Reform Act and 9/11 Commission Act, were used as guidance to construct the plan. The strategic plan identifies three broad trends that have been observed in the types of threats that TSA faces. First, interest in catastrophic destruction of aircraft and

[26]Passenger Checkpoint Screening Program Strategic Plan, Aviation Security, Report to Congress in Response to Conference Report 109-699 to the Fiscal Year 2007 Department of Homeland Security Appropriations Bill, August 2008.

facilities has increased, in contrast to hijacking and hostage-taking that characterized the majority of earlier attacks. Second, the range of encountered weapons has expanded, many not previously recognized as threats, nor detected by the technologies that were deployed. Third, terrorists have attacked "soft" airport targets, including airport lobbies, in other countries. To address these challenges, TSA's strategic plan identifies that the agency's strategy is to utilize intelligence; partner with law enforcement, industry partners, and the public; and implement security measures that are flexible, widely deployable, mobile, and layered to address the nation's complex open transportation network. According to the plan, TSA is in the process of implementing and evaluating a fundamental shift in strategy for the security checkpoint that encompasses the critical elements of people, process, and technology. In addition, the plan states that implementing a new security approach called Checkpoint Evolution,[27] which started in the spring 2008, will bring the most significant changes that have occurred in passenger screening since the airport security checkpoint was first established in the 1970s.

TSA's strategic plan identifies that the key component of TSA's strategy related to security checkpoints is to improve security effectiveness and resource utilization at the checkpoints. Also, the PSP manager stated that a goal of the PSP strategy is to achieve full operating capability by the dates discussed for each checkpoint screening technology listed in the strategic plan. To meet these goals, the PSP strategic plan identifies three strategic objectives: (1) improve explosive detection capability, (2) improve the behavior detection capability of Transportation Security Officers (TSO), and (3) extend the layers of security throughout the passenger journey. The first objective, improving explosive detection capability, involves combining new technology with procedures that emphasize an element of unpredictability to improve explosive detection capability and prevent would-be attackers from knowing the TSA security process. The second objective, improving the behavior detection capability of TSOs, involves shaping the checkpoint environment to better support and enhance behavior detection capabilities by enabling TSOs to engage a larger number of passengers more frequently throughout the checkpoint queue using informal interviews and SPOT; improving the observation conditions for TSOs trained in SPOT by enhancing the

[27]According to TSA, Checkpoint Evolution is a new security approach that involves many different elements to secure the checkpoint including continuously adapting security procedures to improve passenger security.

AR 000753

contrast between passengers exhibiting signs of travel stress and those intending to do harm to other passengers, aircraft, or the airport; and providing communications tools for enhanced coordination between TSOs trained in SPOT. The third objective, extending the layers of security throughout the passenger journey, involves enabling additional layers of non-intrusive security beyond the checkpoint and into public spaces; increasing the interaction between TSOs and passengers to provide more opportunities to identify irregular behaviors far ahead of the potential threat reaching the checkpoint; and partnering with airlines, airports, and the private sector to reduce vulnerabilities in soft target areas.

TSA had been directed on multiple occasions to provide strategic plans for explosives detection checkpoint technologies to congressional committees. The Intelligence Reform Act mandated that TSA provide a strategic plan that included, at a minimum, a description of the current efforts to detect explosives on individuals and in their personal property; operational applications of explosive detection equipment at airport checkpoints; quantities of equipment needed to implement the plan and a deployment schedule; funding needed to implement the plan; measures taken and anticipated to be taken to provide explosives detection screening for all passengers identified for additional screening; and recommended legislative actions, if any.[28] The Intelligence Reform Act mandated that such a strategic plan be submitted to congressional committees during the second quarter of fiscal year 2005. According to TSA officials, a strategic plan was developed and delivered to congressional committees on August 9, 2005, in satisfaction of the statutory mandate. However, the 9/11 Commission Act, enacted August 3, 2007, reiterated a requirement for a strategic plan that TSA was mandated to submit in accordance with the Intelligence Reform Act. Specifically, the 9/11 Commission Act required that the Secretary of Homeland Security issue a strategic plan addressing its checkpoint technology program not later than 30 days after enactment of the 9/11 Commission Act (that is, by September 3, 2007) and required implementation of the plan to begin within 1 year of the act's enactment.[29] In response to the 9/11 Commission Act, TSA provided to Congress the Aviation Security Report: Development

[28] See 49 U.S.C. § 44925(b).

[29] See Pub. L. No. 110-53, § 1607, 121 Stat. at 483.

of a Passenger Checkpoint Strategic Plan, September 2007.[30] Finally, Division E of the Consolidated Appropriations Act, 2008, enacted on December 26, 2007, required that the Secretary of Homeland Security submit a strategic plan for checkpoint technologies no later than 60 days after enactment of the Act (that is, by February 25, 2008), and further restricted the use of $10,000,000 appropriated to TSA for Transportation Security Support until the Secretary submitted the plan to the Committees on Appropriations of the Senate and House of Representatives.[31] As a result of the mandate for a strategic plan and the funding restriction in the 2008 Consolidated Appropriations Act, TSA officials told us that they interpreted this legislative language to mean that congressional committees considered TSA's aviation security report in September 2007 to be incomplete and insufficient. After approximately 12 months had elapsed since a strategic plan had been mandated in the 9/11 Commission Act, in August 2008 TSA completed its revised strategic plan and delivered it to the committees in September 2008, which TSA officials stated meets the mandate for a strategic plan in the 9/11 Commission Act, as well as the mandate for a strategic plan in the appropriations act.

As previously discussed, the Intelligence Reform Act included requirements for a deployment schedule, and descriptions of the quantities of equipment and funding needed to implement the plan.[32] However, our analysis of TSA's August 2008 strategic plan indicates that the strategic plan could include more complete information about these requirements. For example, although TSA provided some deployment information for each emerging checkpoint technology listed in the strategic plan—such as the total quantity to be deployed, expected full operating capability date, and types or categories of airports where the equipment is to be deployed—it does not include a year-by-year schedule showing the number of units for each emerging technology that is expected to be deployed to each specific airport. Regarding information on the funding needed to implement the strategic plan, it includes a funding profile for each fiscal year from 2007 through 2009. However, a number of the

[30] The strategic plan mandated by the Intelligence Reform and 9/11 Commission Acts was to be submitted to the Senate Commerce, Science, and Transportation Committee and the House of Representatives Transportation and Infrastructure Committee.

[31] See Pub. L. No. 110-161, Div. E, 121 Stat. at 1844, 2053 (2007) (referencing H.R. Conf. Rep. No. 109-699, at 138 (Sept. 28, 2006), which had initially directed TSA to develop and submit this plan to the committees).

[32] See 49 U.S.C. § 44925(b)(2).

emerging technologies are not expected to reach full operating capability until fiscal year 2014. TSA officials stated that they have derived notional (that is, unofficial) quantities to be deployed on an annual basis for each technology through its respective full operating capability date, but the officials stated that the funding profile in the strategic plan does not reflect the funding needed for these future quantities because the funding that will be appropriated for them after fiscal year 2009 is unknown. According to the officials, to implement the strategic plan in the years beyond fiscal year 2009, the agency intends to use a year-by-year approach whereby the quantities to be deployed in a particular year, and the funding needed for that year, would not be officially identified prior to the budget request for that year.

TSA officials stated that they used risk to inform the August 2008 strategic plan and the PSP strategy identified in it. Although TSA may have considered that risk to some degree, our analysis does not confirm that these efforts meet the risk-based framework outlined in the NIPP. Specifically, TSA has not conducted a risk assessment or cost–benefit analyses, or established quantifiable performance measures. As a result, TSA does not have assurance that its efforts are focused on the highest priority security needs, as discussed below.

TSA Has Not Conducted a Risk Assessment to Inform Its PSP Strategy, but Is Finalizing an Assessment and Developing Information that May Help Guide PSP Efforts

TSA has not conducted a risk assessment that includes an assessment of threat, vulnerability, and consequence, which would address passenger checkpoint screening; consequently, the PSP strategy has not been informed by such a risk assessment as required by the NIPP. Agency officials stated that they prepared and are currently reviewing a draft of a risk assessment of the aviation domain, known as the ADRA, which is expected to address checkpoint security and officials expect it to be finalized by the end of calendar year 2009; however, its completion has been delayed multiple times since February 2008. Therefore, it is not clear when this assessment will be completed. The ADRA, when completed, is to provide a scenario-based risk assessment for the aviation system that may augment the information TSA uses to prioritize investments in security measures, including the PSP. However, officials could not provide details regarding the extent to which the ADRA would assess threat, vulnerability, and consequence related to the passenger checkpoint. In 2004, we recommended that the Secretary of Homeland Security and the Assistant Secretary for TSA complete risk assessments—including a

consideration of threat, vulnerability, and consequence—for all modes of transportation, and use the results of these assessments to help select and prioritize research and development projects.[33] TSA and DHS concurred with the recommendation, but have not completed these risk assessments. Because TSA has not issued the ADRA or provided details regarding what it will entail, and because it is uncertain when the ADRA will be completed, it is not clear whether the ADRA will provide the risk information needed to support the PSP and TSA's checkpoint technology strategy. In the meantime, TSA has continued to invest in checkpoint technologies without the benefit of the risk assessment information outlined in the NIPP. Consequently, TSA increases the possibility that its investments will not address the highest priority security needs.

Although TSA has not completed a risk assessment to guide its PSP, officials stated that they identify and assess risks associated with the passenger screening checkpoint by relying on threat information, vulnerability information from Threat Image Projection (TIP) scores, limitations of screening equipment identified during laboratory testing, covert tests, and expert judgment to guide its investment strategy in the PSP.[34] Specifically, TSA's Office of Intelligence produces civil aviation threat assessments on an annual basis, among other intelligence products. These assessments provide information on individuals who could carry out attacks, tactics they might use, and potential targets. TSA's most recent aviation threat assessment, dated December 2008, identifies that terrorists worldwide continue to view civil aviation as a viable target for attack and as a weapon that can be used to inflict mass casualties and economic damage. It also concluded that improvised explosive devices (IED) and hijackings pose the most dangerous terrorist threat to commercial airliners in the United States. The assessment identifies that these devices may be concealed on persons, disguised as liquids, or hidden within everyday, familiar objects such as footwear, clothing, toys, and

[33]GAO-04-890.

[34]The Threat Image Projection (TIP) system places images of threat objects on the X-ray screen during actual operations and records whether screeners identify the threat object. TIP is designed to test screeners' detection capabilities by projecting threat images, including guns and explosives, into bags as they are screened. Screeners are responsible for positively identifying the threat image and calling for the bag to be searched. Once prompted, TIP identifies to the screener whether the threat is real and then records the screener's performance in a database that could be analyzed for performance trends. Low performance makes the screening process vulnerable to terrorist attempts to smuggle such materials onto aircraft.

electronics. The threat assessment further identifies that terrorists have various techniques for concealing explosives on their persons. In addition to the annual civil aviation threat assessment, the Office of Intelligence prepares for TSA's senior leadership team and other officials a (1) daily intelligence briefing, (2) tactical intelligence report that is produced one to four times per week, (3) weekly field intelligence summary, (4) weekly suspicious incident report, and, when necessary, (5) special events update, for example, during major political events. However, according to the NIPP, relying on threat information is not sufficient to identify and assess risks. Rather, threat information, which indicates whether a terrorist is capable of carrying out a particular attack and intends to do so, is to be analyzed along side information on vulnerabilities—weakness in a system that would allow such an attack to occur—and on the consequences of the attack, that is, the results of a specific type of terrorist attack, according to the NIPP.

TSA officials stated that, to guide the PSP, they also rely on programs in place that are designed to assess vulnerabilities at airport checkpoints. To identify vulnerabilities at airport checkpoints, TSA officials stated that TSA analyzes TIP scores, known limitations of screening equipment based on laboratory testing, and information from its covert testing program. TSA conducts national and local covert tests, whereby individuals attempt to enter the secure area of an airport through the passenger checkpoint with a prohibited item in their carry-on bags or hidden on their person. Officials stated they use these sources of information to identify needed changes to standard screening procedures, new technology requirements, and deployment strategies for the PSP. When a checkpoint vulnerability is identified, officials stated that TSA's Office of Security Technology engages other TSA stakeholders through the PSP's Integrated Project Team process[35] to identify and develop necessary technology requirements which may lead to new technology initiatives. Officials credited this process with helping TSA identify needed changes to standard screening procedures and deployment strategies for new technologies. For example, according to a TSA official, a technology was developed as a result of tests conducted by GAO that found that prohibited items and components of an

[35] TSA manages the PSP, in part, through an Integrated Product Team (IPT), which is led by the PSP, but draws its members from across TSA, including the Office of Security Operations and the Office of Acquisitions.

IED might be more readily identified if TSA were to develop new screening technologies to screen these items.[36]

Although TSA has obtained information on vulnerabilities at the screening checkpoint, the agency has not assessed vulnerabilities (that is, weaknesses in the system that terrorists could exploit in order to carry out an attack) related to passenger screening technologies that are currently deployed. The NIPP requires a risk assessment to include assessments of threat, vulnerability, and consequence. TSA has not assessed whether there are tactics that terrorists could use, such as the placement of explosives or weapons on specific places on their bodies, to increase the likelihood that the screening equipment would fail to detect the hidden weapons or explosives. Although TIP scores measure how effectively screeners identify prohibited items, they do not indicate whether screening technologies currently deployed may be vulnerable to tactics used by terrorists to disguise prohibited items, such as explosives or weapons, thereby defeating the screening technologies and evading detection. Similarly, TSA's covert testing programs do not systematically test passenger and baggage screening technologies nationwide to ensure that they identify the threat objects and materials the technologies are designed to detect, nor do the covert testing programs identify vulnerabilities related to these technologies. We reported in August 2008 that, while TSA's local covert testing program attempts to identify test failures that may be caused by screening equipment not working properly or caused by screeners and the screening procedures they follow, the agency's national testing program does not attribute a specific cause of the test failure.[37] We recommended, among other things, that TSA require the documentation of specific causes of all national covert testing failures, including documenting failures related to equipment, in the covert testing database to help TSA better identify areas for improvement. TSA concurred with this recommendation and stated that the agency will expand the covert testing database to document test failures related to screening equipment. Moreover, TSA officials stated that it is difficult to attribute a test failure to equipment, because there is a possibility that the threat item used for the test was not designed properly and, therefore,

[36]The work related to the tests conducted by GAO contains classified material and the results of these tests are not publicly available.

[37]GAO, *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests*, GAO-08-958 (Washington, D.C.: August 8, 2008).

should not have set off the equipment's alarm. TSA officials also stated that it is difficult to identify a single cause for a test failure because covert testing failures can be caused by multiple factors. As a result, TSA lacks a method to systematically test and identify vulnerabilities in its passenger and baggage screening equipment in an operational airport setting. Consequently, TSA officials do not have complete information to identify the extent to which existing screening technologies mitigate vulnerabilities at the passenger checkpoints, so that they can incorporate this information into the agency's security strategy, as required by DHS guidance.

TSA's ADRA, once completed, is to cover the entire aviation domain and include three parts—assessments of over 130 terrorist attack scenarios to determine whether they pose a threat to the aviation system; an assessment of known vulnerabilities or pathways within the aviation system through which these terrorist attacks could be carried out; and an assessment of consequences of these various types of terrorist attacks, such as death, injury, and property loss. TSA officials stated that, through the use of expert panels, the ADRA will evaluate these threat scenarios to assess the likelihood that terrorists might successfully carry out each type of attack on the aviation system, and the likelihood and consequences of these various scenarios will be prioritized to identify the most pressing risks that need to be addressed. In the case of the passenger screening checkpoint, according to officials, TSA will be examining all security measures that a terrorist must breach in order to carry out a specific type of an attack, such as carrying an IED on board an aircraft and detonating it midflight. However, officials could not explain or provide documentation identifying the extent to which the ADRA will provide threat, vulnerability, and consequence assessments in support of the PSP. In addition, the completion date for the ADRA has been delayed multiple times. Because the ADRA has not been finalized and TSA has not described how the ADRA will address the passenger checkpoint, we could not determine the extent to which it will incorporate information on checkpoint

vulnerabilities, including vulnerabilities associated with screening technologies and standard operating procedures.[38]

In addition to the ADRA, TSA and DHS S&T are developing other information that could inform their identification and assessments of risks to the aviation transportation system. 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. However, according to these officials, TSA's understanding of 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, FAA, 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

[38]The ADRA is part of TSA's efforts to meet the requirements of Homeland Security Presidential Directive 16 (HSPD-16), which requires the DHS Secretary, in coordination with the Secretaries of State, Defense, Commerce, and Transportation, the Attorney General, and the Director of National Intelligence, to prepare a National Strategy for Aviation Security that provides an overarching national strategy to optimize and integrate governmentwide aviation security efforts. The national strategy and its supporting plans are to use a risk-based approach to ensure that national resources are allocated to security efforts with the greatest potential to prevent, detect, defeat, or minimize the consequence of an attack, taking into consideration threat, vulnerabilities, and probable consequences of an attack. The Secretaries of Homeland Security and Transportation are also to lead, in conjunction with the Secretaries of State, Defense, and Energy, and the Attorney General, an interagency effort, in consultation with appropriate industry representatives, to develop and execute a risk-based implementation plan for the continued reduction of vulnerabilities within the Aviation Transportation System.

placed in different locations within various aircraft models. Officials estimated this work will be completed in 3- to 4-month increments through 2008 and 2009. Officials further stated that the prototype version of the model was validated in the late summer of 2008, and that the model is currently being used. TSA and S&T officials stated that they expect 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.

TSA Has Not Completed a Cost–Benefit Analysis to Help Establish Risk-Based Priorities and Guide Its Investment Strategy

TSA has not completed a cost–benefit analysis to prioritize and fund the PSP's priorities for investing in checkpoint technologies, as required by the NIPP's risk management framework. According to the NIPP, policy makers who are designing programs and formulating budgets are to evaluate how different options reduce or mitigate threat, vulnerability, or consequence of a terrorist attack through a cost–benefit analysis that combines cost estimates with risk-mitigation estimates.[39] However, in addition to lacking information on risks to the screening checkpoint, TSA has not conducted a cost–benefit analysis of checkpoint technologies being researched and developed, procured, and deployed. Such a cost–benefit analysis is important because it would help decisionmakers 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.

One reason that TSA may have difficulty developing a cost–benefit analysis for the PSP is that it has not developed life-cycle cost estimates of each screening technology the PSP is developing, procuring, or deploying. This information is important because it helps decisionmakers determine, given the cost of various technologies, which technology provides the greatest mitigation of risk for the resources that are available. TSA officials prepared a PSP lifecycle cost estimate in September 2005, but this estimate does not include cost estimates for all technologies currently being researched, developed, tested and evaluated, procured and/or deployed, such as the Advanced Technology Systems, a technology to

[39]According to the NIPP, investments in protective programs should be prioritized based on a cost benefit analysis that weighs the cost, time, and other characteristics of potential solutions, along with the potential that these various investments in countermeasures will reduce or mitigate threat, vulnerability, or consequence of an attack.

screen carry-on items that TSA is currently procuring. TSA was subsequently instructed by DHS Joint Requirements Council[40] to complete lifecycle cost estimates for the PSP; in December 2005, the council reviewed the PSP and approved it to proceed to the Investment Review Board for an annual review and potential approval of the PSP's fiscal year 2006 procurement strategy. However, the council expressed concern about several issues that should be resolved prior to the Investment Review Board's review, including the need for complete lifecycle cost estimates for the checkpoint screening technologies that were to be developed and procured. TSA officials acknowledged that completing lifecycle cost estimates are important and stated that they have not prepared a lifecycle cost estimate since the council recommended that such an estimate be developed due to lack of staff. These officials further stated that TSA hired four full-time equivalent staff in fiscal year 2008, and two additional full-time equivalent staff are expected to be hired in the fall of 2008. The officials anticipate that these staff will help prepare lifecycle cost estimates. However, the officials did not provide a timeframe for the completion of the estimates.

Although TSA officials identified the technologies they are procuring and deploying, TSA officials could not provide us with information on their priorities for the research and development of checkpoint screening technologies or the processes they followed to develop these priorities. According to S&T officials, TSA provided priorities for near-term applied research and development projects to the S&T Capstone Integrated Product Team (IPT) for Explosives Prevention.[41] This IPT establishes priorities for research projects to be funded by S&T during the fiscal year. S&T officials stated that they rely on TSA and other members of the IPT to use a risk-based approach to identify and prioritize their agencies' or offices' individual research and development needs prior to submitting them for consideration to the IPT. However, TSA officials stated they did not submit priorities for research and development to S&T. Without cost–benefit or other analysis to compare the cost and effectiveness of various solutions, the agency cannot determine whether investments in the

[40] The role of the DHS Joint Requirements Council is, among other things, to manage investment portfolios and review projects to identify cross-functional requirements and applications.

[41] In April 2008, S&T dissolved the IPT for explosives detection and replaced it with two separate IPTs, a transportation security IPT, chaired by TSA and a counter-IED IPT, chaired by the Office for Bombing Prevention within the National Protection and Programs Directorate and the United States Secret Service.

AR 000763

research and development of new checkpoint technologies or procedures most appropriately mitigate risks with the most cost-effective use of resources. In addition, without knowing the full cost of the technologies that the PSP is developing, procuring, or deploying, TSA could potentially invest in a technology in which the cost outweighs expected benefits.

TSA Lacks Measures to Evaluate the Extent to Which the PSP Reduces the Risk of Terrorist Attacks

TSA's strategy for the PSP does not have a mechanism—such as performance measures or other evaluation methods—to monitor, assess, or test the extent to which investments in new checkpoint technologies reduce or mitigate the risk of terrorist attacks. The NIPP requires that protective programs be designed to allow measurement, evaluation, and feedback based on risk mitigation so that agencies may re-evaluate risk after programs have been implemented and take corrective action if needed, such as modifying existing programs to counter new risks or implementing alternative programs. The NIPP identifies three types of performance measures—descriptive, process/output, and outcome measures—that can help gauge the effectiveness of protective programs.[42] Although the NIPP requires that protective programs be designed to allow measurement, evaluation, and feedback based on risk mitigation, TSA has not identified quantifiable measures of progress which would allow the agency to assess the PSP's overall effectiveness. TSA officials stated that they do not have overall performance measures but are currently developing performance goals and measures for the overall program. However, the officials could not provide a time frame for their completion. In September 2004, we recommended that TSA complete strategic plans for its research and development programs which contain measurable

[42]Descriptive measures are used to understand sector resources and activities, such as the number of facilities in a jurisdiction. Process/output measures are used to measure whether specific activities were performed as planned, tracking the progression of a task, or reporting on the output of a process, such as inventorying assets. Outcome measures track progress towards a strategic goal by beneficial results rather than level of activity. In addition to the NIPP, the Government Performance and Results Act of 1993 provides, among other things, that federal agencies establish program performance measures, including the assessment of relevant outputs and outcomes of each program activity. According to the Office of Management and Budget (OMB), performance goals are target levels of performance expressed as a measurable objective, against which actual achievement can be compared. Performance goals should incorporate measures (indicators used to gauge performance); targets (characteristics that tell how well a program must accomplish the measure), and time frames.

objectives.[43] Without measures to monitor the degree to which the TSA's investments in the research, development, and deployment of new screening technologies reduce or mitigate terrorist threats, the agency is limited in its ability to assess the effectiveness of the PSP or the extent to which it complements other layers of security at the checkpoint.

Ten New Checkpoint Screening Technologies Are in Various Phases of RDT&E, Procurement, and Deployment, but ETP Deployment Has Been Halted

Since TSA's creation in 2001, 10 new checkpoint screening technologies, including the ETP, have been in various phases of RDT&E, procurement, and deployment, but TSA halted deployment of the ETP due to performance problems and high installation costs. Of the 10 technologies, TSA has initiated deployments for 4 of them, including the ETP and a Bottled Liquids Scanner, but TSA has not deployed any of the 4 technologies to airports nationwide. TSA also initiated procurements of two technologies, including the Whole Body Imager; however, deployment of these two technologies has not begun yet. Four checkpoint technologies are in research and development, such as a shoe scanning device. In June 2006, 6 to 11 months after TSA began to deploy the ETPs to airports, the agency halted their deployment due to performance problems—the machines broke down more frequently than specified by the functional requirements and the machines were more expensive to install and maintain in airports than expected. Because TSA did not follow its acquisition guidance that recommends technologies be tested and evaluated in an operational setting prior to procurement and deployment, the agency lacked assurance that the ETPs performed as required by the system's requirements. Although TSA officials were aware that tests conducted on earlier ETP models during 2004 and 2005 suggested that they did not operate reliably in an airport environment and that the ETP models that were subsequently deployed to airports had not been tested in an operational environment to prove their effectiveness, TSA deployed the

[43]In GAO-04-890, we recommended that the Secretary of Homeland Security and the Assistant Secretary for TSA complete strategic plans containing measurable objectives for DHS's and TSA's transportation security research and development programs. DHS stated that it had completed a strategic plan and that TSA was developing a strategic plan that outlined measurable objectives. However, TSA has not yet completed a risk-based plan that outlines measureable objectives. TSA's August 2008 strategic plan for the PSP states that each technology is assessed in the laboratory and in the field using key performance measures, which are reported to senior management, so a decision about whether to acquire the technology can be made. However, these measures apply to the performance of individual, specific technologies against their functional requirements before they are deployed, whereas the NIPP guidance refers to performance measures that assess the effectiveness of a program as a whole to mitigate risk and improve security.

ETPs to airports beginning in July 2005 for the Smiths Detection ETP and beginning in January 2006 for the General Electric ETP without resolving these issues. TSA officials stated that they deployed the ETPs to respond quickly to the threat posed by a potential suicide bomber after suicide bombings had been carried out onboard Russian airliners in 2004. TSA officials stated that they plan to continue to use the 90 ETPs currently deployed to airports. Because the ETPs were deployed without resolving their performance problems and validating all of the functional requirements, the ETPs have not been demonstrated to increase security at the checkpoint. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security.

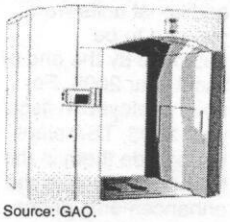
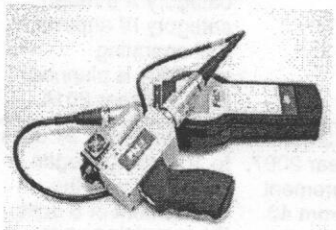
S&T and TSA Investments in RDT&E Resulted in the Procurement or Deployment of Six New Checkpoint Technologies

As a result of S&T and TSA investments in the RDT&E of checkpoint screening technologies since TSA's creation in 2001, six new screening technologies are being procured and/or deployed, while four checkpoint screening technologies are currently in the research and development phase.[44] Based on S&T and TSA RDT&E efforts, the agency has initiated deployments of four technologies—the ETP, Fido PaxPoint Bottled Liquids Scanner, Advanced Technology Systems, and Cast and Prosthesis Scanner—three of which originated as commercial-off-the-shelf technologies or commercial-off-the-shelf technologies that TSA modified for use as checkpoint screening devices.[45] However, TSA has not completed the deployment for all of these four technologies to airports nationwide. TSA officials stated that they did not deploy additional checkpoint screening technologies because they were primarily focused on deploying explosives detection systems to screen checked baggage, as mandated by ATSA. TSA has also initiated procurements of two additional technologies—Automated Explosives Detection System for Carry-on Baggage and Whole Body Imager—but has not deployed either of them yet. Figure 3 describes the status of the six checkpoint screening technologies for which TSA has initiated procurement and/or deployment.

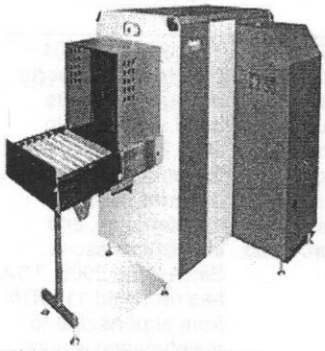
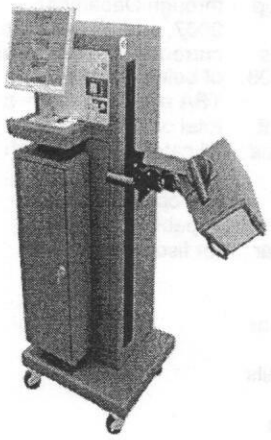
[44]Some of the technologies that have initiated deployments or procurements are continuing in research and development to do follow-on work. For example, the Bottled Liquids Scanner and Advanced Technology Systems continue to be enhanced.

[45]Commercial-off-the-shelf technology is a product or service that has been developed for sale, lease, or license to the general public and is currently available at a fair market value. The product or service can sometimes be modified, which can save time and money compared to researching, developing, and producing a product from scratch.

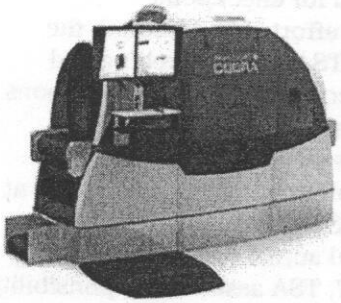
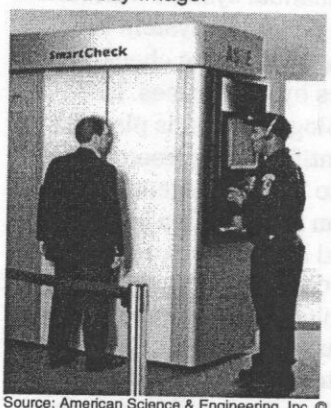
Figure 3: Status of Six Checkpoint Screening Technologies that Had Initiated Procurement and/or Deployment as of September 2008

Technology	Description	Status of		
		Operational Testing	Procurement	Deployment to Airports
Explosives Trace Portal (ETP)  Source: GAO.	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. Used for secondary screening.	Completed for earlier models, but not for models ultimately deployed. We discuss this in more detail later in the report.	TSA procured 207 ETPs. In June 2006, TSA halted further procurement due to high installation and maintenance costs and performance issues. One hundred and sixteen of the procured units remain in storage.	TSA deployed 101 portals to 36 airports during fiscal years 2005 and 2006. In June 2006, TSA halted further deployment due to performance, maintenance, and installation issues. Since June 2006, TSA has removed 11 ETPs from airports due to maintenance issues and placed them in a warehouse for storage.
Bottled Liquids Scanner  Source: ICx Technologies, Inc.	Hand-held or table-top units that screen for liquid explosives by detecting vapors of certain chemicals. Used for secondary screening.	Completed for ICx Nomadics Fido PaxPoint model, which is a type of hand-held device. Laboratory and operational tests are ongoing for hand-held and/or table-top Bottled Liquids Scanner devices.	TSA procured 215 Fido PaxPoint units during fiscal year 2007 and 79 Smiths Detection Sabre 4000 units during fiscal years 2007 and 2008. TSA planned to procure up to 750 hand-held and/or table-top units in late fiscal year 2008. TSA increased its planned procurement for fiscal year 2008 as a result of supplemental appropriations received in fiscal year 2007 and appropriations available in fiscal year 2008. Forty-one Smiths Detection units are at TSA headquarters or in a warehouse in case they are needed for rapid deployment.	TSA deployed 200 Fido PaxPoint units from July 2007 to January 2008. TSA deployed 38 Smiths Detection Sabre 4000 units from July 2007 through December 2007, and 30 units are currently in the process of being deployed. TSA plans to deploy a total of 1,300 units at all category X through category IV airports.[a] Full operating capability is planned for fiscal year 2011.

AR 000767

Technology	Description	Status of Operational Testing	Status of Procurement	Status of Deployment to Airports
Advanced Technology Systems  Source: Rapiscan Systems, Inc. © 2009.	Intended to improve capability to detect threat items, such as explosives. The units will replace the Threat Image Projection Ready X-ray machines used at airports for primary screening of carry-on items.	Completed	TSA procured 250 units during fiscal year 2007. Due to the availability of supplemental funding, appropriations available in fiscal year 2008, and the need to expedite procurement of these systems, the fiscal year 2008 planned procurement was 582 units, of which 250 units have been procured. In fiscal year 2009, TSA plans to award a contract to enhance current units.	From April 2008 to June 2008, 204 units were deployed to 12 airports, and about 287 additional units were planned to be deployed by the end of fiscal year 2008. For units deployed in fiscal year 2008, TSA plans to upgrade them in the field to incorporate the enhancements under the contract to be awarded in fiscal year 2009. TSA plans to deploy up to a total of 2,325 units at every checkpoint lane in all category X through category IV airports. Full operating capability is planned for fiscal year 2014.
Cast and Prosthesis Scanner  Source: CastScopeTM.	Provides a two-dimensional image of the area beneath a cast or inside a prosthetic device. The device operates similarly to the whole body imager, but for localized regions of a passenger's body. Intended for use as a secondary screening device.	Completed	TSA procured 34 units during fiscal year 2007. Planned procurement was reduced from 40 to 34 units due to a system maintenance cost increase. Due to a change in priorities, planned procurement of 75 units in fiscal year 2008 was cancelled because funds were redirected to procure additional units of Advanced Technology Systems and Whole Body Imagers. TSA has no plans to procure additional units in the future.	Deployment of 34 units to 10 airports began in July 2008 with the deployment of 5 units; the remaining units were expected to be deployed by the end of September 2008.

AR 000768

Technology	Description	Status of Operational Testing	Status of Procurement	Status of Deployment to Airports
Automated Explosives Detection System for Carry-on Baggage[b]  Source: Analogic Corporation.	Creates a three-dimensional image of carry-on items to detect explosives and non-metallic weapons. Being considered as a secondary screening device.[c]	Expected to be completed in September 2009.	TSA procured 20 units during fiscal year 2007 for operational testing. TSA had no plans to procure any units in fiscal year 2008.	Deployment to checkpoints at category III and IV airports is expected to begin after operational testing has been completed in September 2009.
Whole Body Imager  Source: American Science & Engineering, Inc. © 2006.	Scans passengers by producing a two-dimensional, full-body computer-generated image that reveals object anomalies underneath clothing, including plastic explosives and concealed metallic, non-metallic, ceramic and plastic objects. TSA is evaluating the feasibility of using this system as a primary and secondary screening device.[d]	Expected to be completed in fiscal year 2009.	TSA leased 15 units in fiscal year 2007 for operational testing. Due to the availability of fiscal year 2008 appropriations, 135 units were planned for procurement in fiscal year 2008, of which 47 have been procured. In fiscal year 2009, TSA plans to award a contract for enhanced units.	Deployment of 150 units is expected to begin in fiscal year 2010. For units deployed in fiscal year 2008 for testing, TSA plans to upgrade them in the field to incorporate the enhancements under the contract to be awarded in fiscal year 2009. TSA plans to deploy a total of 878 units at all category X through category IV airports. Full operating capability is expected in fiscal year 2014.

Source: TSA and S&T.

[a]TSA classifies the commercial airports in the United States into one of five security risk categories (X, I, II, III, and IV). In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest. Categories X, I, II, and III airports account for more than 90 percent of the nation's air traffic.

[b]Although this technology has an automated detection capability, TSA is not testing the automated detection function in an operational environment.

[c]Research and development of this technology is continuing, specifically, to develop a computed tomography (CT) X-ray for carry-on baggage. This technology will permit fully-automated inspection of passenger baggage as opposed to the TSA screeners having to interpret the results of the baggage screening process. Operational testing of the CT X-ray technology is to be completed in fiscal year 2009.

[d]Research and development of this technology is continuing, specifically, to develop passive terahertz (THz) and active gigahertz (GHz) technologies to improve detection performance and reduce operational costs of commercially available systems. Operational testing of the THz and GHz technologies is to be completed in fiscal years 2009 and 2010, respectively.

According to TSA's August 2008 strategic plan for checkpoint technologies, there are several other ongoing efforts in addition to the technologies discussed in figure 3.[46] S&T and TSA are researching and developing a shoe scanning device that is to conduct automated weapons and explosive detection without requiring passengers to remove their footwear. TSA plans to award a contract in fiscal year 2010, with full operating capability in fiscal year 2015. TSA plans to deploy 1,300 units at all category X through category IV airports. TSA also has two ongoing efforts related to boarding pass and credential authentication, according to the agency's strategic plan. Starting in 2007, TSA assumed responsibility from airline contractors for travel document checking, which is currently conducted manually. TSA plans to replace the manual system with an automated one. Specifically, the Boarding Pass Scanning System is expected to verify the authenticity of a boarding pass at the checkpoint and enable the use of paperless boarding passes by the airlines. In addition, the Credential Authentication Technology System is planned to be an automated system that authenticates identification presented by passengers and airport employees. According to TSA, the agency plans to eventually combine both of these authentication systems in a single travel document checking system. TSA plans to award a contract for these two systems in fiscal year 2009, with full operating capability expected in fiscal year 2014. TSA plans to deploy a total of 878 units to replace the existing document verification tools at all category X through category IV airports. Another ongoing effort identified in TSA's strategic plan is the Next Generation ETD. This system is planned to replace legacy ETD systems and to be able to identify a larger range of explosives. Specifically, this system is expected to have enhanced explosive detection capability in terms of sensitivity and the ability to detect new threats, as well as other improvements over legacy systems, which are expected to produce lower lifecycle costs. TSA plans to deploy 1,500 units at all category X through category IV airports.

[46]TSA submitted a strategic plan for the PSP to congressional committees in September 2008. In the plan TSA identified several new technologies that the agency had not previously identified to us. Because we did not receive this strategic plan until toward the end of our review in September 2008, we did not conduct detailed assessments of these particular technologies.

TSA also has two additional efforts to assess possible technologies. One effort is called Standoff Detection, which is intended to display images to detect anomalies concealed under passengers' clothing. TSA plans to conduct an operational utility evaluation of test article units during fiscal year 2009 to evaluate the technology's feasibility within checkpoint screening operations. According to TSA, this technology would assist the agency in applying layered security prior to the checkpoint in soft target areas, such as airport lobbies, to improve early awareness of a potential explosive threat. If the technology proves effective in the checkpoint operation, TSA plans to award a contract in fiscal year 2010, with full operational capability expected by fiscal year 2014, and to deploy 351 units to every checkpoint at category X and category I airports. The other effort is called Explosives Characterization for Trace (Chemical-based) Detection. This effort includes the research and development of trace signatures, detection, and physical properties of explosives to improve the detection and performance of deployed explosives trace detection technologies.

TSA Procured and Deployed ETPs without Assurance that They Would Perform as Intended in an Operational Setting

During 2004 and 2005, prior to deployment of the ETPs, TSA conducted a series of acceptance tests (that is, laboratory tests) of the General Electric and Smiths Detection ETPs that suggested they had not demonstrated reliable performance. Specifically, in 2004, TSA conducted acceptance tests on early models of the General Electric and Smiths Detection ETPs to determine whether the ETPs met key functional requirements. Subsequently, in 2004 a General Electric ETP model was field tested at five airports to determine how well the ETP performed in an operational environment. A Smiths Detection ETP model was also field tested at an airport in 2004. Based on initial test results, both vendors of the ETPs modified the machines, and TSA conducted further laboratory testing. The modified General Electric ETP was tested from December 2004 through February 2005. During the January 2005 to May 2005 time frame, both the General Electric and Smiths Detection ETP models were tested. Even though tests conducted during 2004 and 2005 of the General Electric and Smiths Detection ETPs suggested they had not demonstrated reliable performance, TSA deployed the Smiths Detection ETP and General

Electric ETP to airports starting in July 2005 and January 2006, respectively, without resolving identified performance issues.[47]

Further, TSA did not test all 157 of the ETP's functional requirements prior to procuring and deploying the General Electric and Smiths Detection ETP models. Instead, TSA tested the ETP models against a subset of the functional requirements. According to TSA's System Development Life Cycle Guidance, testing of a system is to be conducted to prove that the developed system satisfies its requirements in the functional requirements document. TSA officials could not identify the specific requirements that were tested or the reason(s) that all of the requirements were not tested.

A TSA official stated that TSA had intended to resolve problems regarding the ETPs' performance after they had been deployed, but TSA officials could not explain how these problems were to be resolved. Officials further stated that they worked for over 1 year during 2006 and 2007 with the ETP vendors to correct reliability and maintenance issues after the ETPs were initially deployed, but could not resolve them. Furthermore, according to S&T officials, when TSA conducted limited field tests, the ETP manufacturers provided different configurations from those used during the laboratory tests. According to officials, once this was discovered, it took more than 6 months for the ETP manufacturers to recreate the configurations that had passed the laboratory tests. TSA officials stated that, during this 6-month period, the agency decided to award a sole source contract to General Electric to procure its ETP.

Regarding the reliability of the ETPs, of the 101 ETPs (71 from General Electric and 30 from Smiths Detection) that were originally deployed to 36 airports, the General Electric ETP did not meet the system requirement for operational availability due to frequent breakdowns. Both vendors' ETPs were also more expensive to maintain than expected, according to the TSA Chief Technology Officer serving during this period. The functional requirements document requires the ETP to be operationally available 98.38 percent of the time. However, the General Electric ETPs were not always able to meet this requirement. TSA officials could not provide information on the operational availability of the Smiths Detection ETPs. For the General Electric ETPs, from January through May 2006, they were

[47]According to TSA, the specific methods and results of testing of the ETPs during the research and development phase are sensitive security information protected from disclosure pursuant to 49 C.F.R. § 1520.5(b). As a result, the relevant sections are described in the restricted version of this report.

operationally available an average of 98.05 percent of the time, although the ETPs met the operational availability requirement for 2 months during that period. Furthermore, TSA's operational requirements specify that the ETP should function for a minimum of 1,460 hours between critical failures. A critical failure means that an ETP fails to operate and must be repaired as soon as possible. However, the TSA Chief Technology Officer at the time stated that the ETPs operated at a much lower average number of hours before a critical failure occurred because, for example, the dirt and humidity of some airport environments adversely affected the equipment. Specifically, from January 2006 through May 2006, the General Electric ETPs operated for an average of 559 hours before a critical failure, which means that these ETPs operated on average 38 percent of the time that they were required to operate before a critical failure occurred. TSA officials could not provide information on the mean time between critical failures for the Smiths Detection ETPs. TSA officials stated that they tested the ETPs in several airports for several months prior to deployment, but data from these tests did not identify a problem with mean time between critical failures. One reason for this, a TSA official stated, was that not enough data were collected during the field tests. As usage of the ETPs increased, officials stated that they discovered the ETP was not meeting operational availability requirements. The ETPs also required replacement filters and other consumables more often than expected, according to officials, which drove up maintenance costs.

According to TSA officials, because of a variance in operational availability hours among the deployed ETPs, maintenance problems, and the high cost of ETP installation at airports, in June 2006, the agency halted the deployment of the ETP to additional airports and stopped the planned purchase of additional ETPs. TSA officials plan to continue to use the 90 ETPs currently deployed to airports. However, without validating that the ETPs meet their functional requirements, TSA officials do not have assurance that it is worthwhile to continue to use the ETPs in light of the cost to maintain and operate them. In addition, TSA officials are considering what to do with the ETPs that were procured and are currently in storage. As of April 2009, 116 ETPs were in storage.[48]

[48]TSA originally deployed 101 ETPs to airport checkpoints, and had 90 ETPs at airports and 116 ETPs in storage at the time we issued our restricted April 2009 report. After issuance of our restricted report, TSA stated that 22 ETPs were at airports and no ETPs were in storage as of September 2009.

TSA did not follow the Acquisition Management System (AMS) guidance or a knowledge-based acquisition approach before procuring the ETPs, which contributed to the ETPs not performing as required after they were deployed to airports. Specifically, AMS guidance provides that testing should be conducted in an operational environment to validate that the system meets all functional requirements before deployment. 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.[49] 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. As discussed earlier in this report, TSA officials told us that they deployed the ETP despite performance problems because officials wanted to quickly respond to emergent threats. However, TSA did not provide written documentation to us that described the process used at the time to make the decision to deploy the ETP or the process that is currently used to make deployment decisions.

Using Validated Technologies Would Enhance TSA's Efforts to Improve Checkpoint Security

TSA has relied on technologies in day-to-day airport operations that have not been demonstrated to meet their functional requirements in an operational environment. For example, TSA has substituted existing screening procedures with screening by the Whole Body Imager even though its performance has not yet been validated by testing in an operational environment. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security. Furthermore, without retaining existing screening procedures until the effectiveness of future technologies has been validated, TSA officials cannot be sure that checkpoint security will be improved.[50]

[49]GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition*, GAO-04-386SP (Washington, D.C.: January 2004).

[50]According to TSA, our evaluation of TSA's use and validation of airport screening technologies is sensitive security information protected from disclosure pursuant to 49 C.F.R. § 1520.5(b)(9)(v). As a result, the relevant sections are described in the restricted version of this report.

DHS Is Addressing Coordination and Collaboration Challenges with Stakeholders to Research, Develop, and Deploy Checkpoint Screening Technologies

DHS S&T and TSA coordinated and collaborated with each other and key stakeholders on their research, development, and deployment activities for airport checkpoint screening technologies, and DHS is taking actions to address challenges and strengthen these efforts.[51] Because S&T and TSA share responsibilities related to the 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. For example, in accordance with provisions of the Homeland Security Act and ATSA, S&T and TSA are to coordinate and collaborate with internal and external stakeholders on matters related to technologies and countermeasures for homeland security missions. S&T and TSA signed an MOU in August 2006 that establishes a framework to coordinate their work at the TSL, which tests and evaluates technologies under development. S&T also established a Capstone IPT for Explosives Prevention in 2006 to bring S&T, TSA, and U.S. Secret Service leadership together to identify gaps in explosives detection capability; prioritize identified gaps; review relevant, ongoing S&T programs; and develop capabilities to meet identified needs. However, inconsistent communication and the lack of an overarching test and evaluation strategy have limited S&T's and TSA's ability to coordinate effectively with one another. To coordinate with the aviation community, S&T and TSA have hosted industry days and conference calls to discuss new technologies with airport operators and technology vendors. Although TSA has taken actions to build partnerships with airport operators and vendors, it has not established a systematic process to coordinate with them related to checkpoint screening technologies. However, TSA officials stated that they are in the beginning stages of establishing a systematic process.

[51]S&T is responsible for conducting basic and applied research, and advanced development, including developmental test and evaluation. TSA is responsible for conducting operational test and evaluation, operational integration, procurement and deployment of new technologies, including checkpoint screening technologies.

S&T and TSA Are Addressing Coordination and Collaboration Challenges with Each Other on New Checkpoint Screening Technologies, but Challenges Remain

S&T and TSA have taken actions to coordinate and collaborate with each other related to the RDT&E of checkpoint screening technologies, such as by communicating priorities and requirements for technologies and working with each other on the Capstone IPT for Explosives Prevention. However, S&T and TSA coordination and collaboration were not always effective due to inconsistent communication and the lack of an overarching test and evaluation strategy. The Homeland Security Act assigned responsibilities within the department for coordinating and integrating the research, development, demonstration, testing, and evaluation activities of the department, as well as for working with federal and private sector stakeholders to develop innovative approaches to produce and deploy the best available technologies for homeland security missions. The act further assigned S&T with responsibility for coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the department to reduce duplication and identify unmet needs. ATSA had also assigned TSA with coordination responsibilities, including the coordination of countermeasures with appropriate departments, agencies, and instrumentalities of the U.S. government.[52]

S&T and TSA have taken several actions to coordinate and collaborate on their research and development activities related to checkpoint screening technologies. First, to coordinate the transition of the TSL from TSA to S&T, minimize disruption of work, and prevent duplication of effort, S&T and TSA signed an MOU that defines the roles and responsibilities for the research and development of homeland security technologies, including checkpoint screening, and establishes a framework for how to coordinate their work. Additionally, S&T created the Capstone IPT for Explosives Prevention, which is co-chaired by the Assistant Secretary for TSA and the Director of the U.S. Secret Service, to identify and prioritize capabilities needed to detect explosives; review relevant, ongoing S&T programs; and develop capabilities to meet the identified needs. The IPT was first convened in December 2006 to identify research and development priorities for explosives detection technologies at airport checkpoints as

[52]In accordance with provisions of the Homeland Security Act and ATSA, the S&T's Explosives Division and TSA should coordinate with one another and other stakeholders, including the commercial aviation community and DHS components, to facilitate the research, development, and deployment of checkpoint screening technologies. TSA should also coordinate countermeasures to protect civil aviation with appropriate federal departments and agencies. See 49 U.S.C. § 114(f)(4). The S&T Explosives Division develops technical capabilities to detect, interdict, and lessen impacts of nonnuclear explosives used in terrorist attacks against mass transit, civil aviation, and critical infrastructure.

well as for other transportation modes, and has met periodically since then. According to TSA officials, the Capstone IPT has enabled TSA to establish a clear understanding with S&T of TSA's needs for technology solutions that meet stringent detection thresholds and throughput requirements to support the aviation sector. Additionally, the officials stated that the Capstone IPT has given TSA a better collective understanding of the technology needs of other DHS components, which will help DHS identify technology solutions that can be combined to benefit multiple users. Finally, to follow through on the priorities established by the Capstone IPT for Explosives Prevention, S&T officials stated that they established project-level IPTs, including one for airport checkpoints and one for homemade explosives. S&T officials stated that they are working with TSA on these project-level IPTs to try to meet the needs identified by the Capstone IPT. TSA officials further stated that they have PSP IPTs or working groups to coordinate on technology projects, establish program goals and objectives, and develop requirements and time lines. These groups meet on a weekly basis, according to TSA officials. In April 2008, S&T dissolved the IPT for explosives detection and replaced it with two separate IPTs, a transportation security IPT, chaired by TSA and a counter-IED IPT, chaired by the Office of Bombing Prevention within the National Protection and Programs Directorate and the United States Secret Service.

Coordination and collaboration efforts between S&T and TSA have helped in identifying checkpoint screening solutions. For example, S&T and TSA officials collaborated on a hand-held vapor detection unit called the Fido PaxPoint. After the August 2006, discovery of the alleged plot to detonate liquid explosives on board commercial air carriers bound for the United States from the United Kingdom, S&T and TSA worked together to identify, develop, and test screening technologies to address this threat. According to TSA officials, S&T learned that the Department of Defense had developed a handheld unit that could detect vapors from explosives. S&T modified the Department of Defense handheld unit, resulting in the Fido PaxPoint unit to screen liquids and gels at airport checkpoints for explosives, and S&T helped TSA test and evaluate the device.[53]

[53]Even though TSA officials stated that the Fido PaxPoint was determined to be effective, the data collection process for it has been extended to ascertain its operational suitability, specifically, how sustainable and maintainable it is. TSA could not provide information to us on the status of this data collection process.

Although S&T and TSA have taken steps to coordinate and collaborate with one another, inconsistent communication and a lack of an overarching test and evaluation strategy have contributed to coordination and collaboration challenges. Specifically, communication between S&T and TSA related to S&T's basic and applied research efforts and TSA's efforts to modify commercially available technologies has been lacking at times. For example, TSA officials stated that early in the TSL's transition to S&T (that is, during fiscal year 2006), TSA did not receive information from S&T regarding which of TSA's research and development needs S&T would fund, which projects related to airport checkpoint technologies were underway at the TSL, or the time frames to complete those projects. TSA officials stated that, without this information, TSA was unable to determine whether its work on modifying commercially available technologies for screening passengers and carry-on items unnecessarily duplicated S&T's research and development efforts, although TSA officials were not aware of any duplication that occurred. An S&T official further stated that TSA had not consistently fulfilled its responsibility to provide clearly defined functional requirements for the equipment to be developed by S&T and tested by the TSL, nor has TSA consistently given sufficient notice to the TSL of TSA testing requests. Under the S&T and TSA MOU, TSA has retained responsibility to establish requirements for equipment certification and qualification and acceptance testing. Specifically, an S&T official at the TSL stated that TSA had inadequately defined the functional requirements and allowed too little time for testing several checkpoint screening technologies, including the Advanced Technology Systems, Enhanced Metal Detector II, and Bottled Liquids Scanner. A TSL official acknowledged that when the TSA was responsible for the TSL, the agency had not consistently developed requirements prior to testing or certification of equipment as required by the DHS guidance.[54]

In another example, as previously mentioned in this report, TSA is developing new certification standards and functional requirements for screening technologies, and is working with national laboratories to validate data on aircraft vulnerabilities and generate new computer models to help TSA develop requirements for explosives detection. According to the TSA Chief Technology Officer in 2007, the TSL has custody of the aircraft vulnerability data, but TSL officials had refused to release the data to the national laboratories as requested by TSA. Although

[54]DHS Investment Review Process Management Directive 1400. This directive was replaced in November 2008 by an Interim Acquisition Directive (102-01).

the TSL later provided 32 of the 46 requested reports, TSA officials estimated that the TSL's refusal to release all of the reports had delayed the effort to develop new certification standards and technology requirements by about 1 month. The officials added that most of TSA's requests to S&T and the TSL had involved similar problems and that, although the MOU provides a framework for coordination, these types of problems are related to day-to-day operations and will have to be resolved as situations arise.

According to S&T and TSA officials, senior-level management turnover at S&T and TSA contributed to these communication difficulties, as well as an S&T reorganization which began in August 2006 with the arrival of a new Under Secretary for Science and Technology. S&T officials further stated that, prior to the establishment of the PSP working groups, there was no mechanism for S&T and TSA to communicate information about priorities, funding, or project timelines. However, through the working groups, S&T officials stated that S&T and TSA are beginning to achieve regular communication and interaction at the working level, which allows for information to be shared in a mutually beneficial way. S&T and TSA officials also stated that communication with each other has improved since the MOU was signed in August 2006 and, in particular since the summer of 2007, although officials from both organizations stated that further improvement is needed. According to S&T officials, the TSL's independent test and evaluation division and TSA have developed an effective working relationship for several programs, including the Whole Body Imager and Advanced Technology Systems. In addition, S&T officials stated that TSA has come to better understand the processes involving the Capstone IPT and identifying capability needs. According to TSA officials, the agency is in the process of determining whether a position within its Office of Security Technology should be established as a liaison with S&T to improve coordination between S&T and TSA. If the position is created, the TSA liaison would coordinate and collaborate with S&T officials on technology projects by assessing the science that supports the technologies.

The MOU specifies that S&T and TSA will coordinate activities, including developing an integrated, overarching test and evaluation strategy for projects to ensure that test and evaluation functions are not duplicative, adequate resources are outlined and secured for these functions, and activities are scheduled to support the overall project master schedule. However, an overarching test and evaluation strategy for checkpoint technologies has not been developed. The lack of this strategy has presented coordination and collaboration challenges between S&T and

TSA, and has resulted in the delay of some technologies. For example, a TSL official stated that the TSL could not accommodate TSA's request to test the Advanced Technology Systems, in part, because TSA officials had not provided sufficient advance notice of their testing needs. TSA officials said they were working with S&T to develop a project master schedule for the Advanced Technology Systems. S&T and TSA officials stated that they plan to develop a test and evaluation strategy to define a coordinated technology transition process from S&T to TSA by outlining key responsibilities and criteria to initiate field evaluations of technologies, but officials could not tell us when the test and evaluation strategy would be completed.

DHS Is Using Several Approaches to Strengthen Coordination and Collaboration with Airport Operators, Technology Vendors, and Other Federal Agencies

DHS, through S&T and TSA, coordinates with airport operators, private sector partners, such as technology vendors, and other federal agencies on matters related to research and development efforts. This coordination and collaboration between TSA and airport operators and technology vendors is important because the agency relies on airport operators to facilitate the deployment of equipment for testing and day-to-day operations, and on vendors to develop and manufacture new screening equipment.[55] However, TSA does not have a systematic process to coordinate with external stakeholders related to checkpoint screening technologies, but TSA officials stated that the agency has developed a draft communications plan, which is being reviewed.

Although TSA does not have a systematic process to coordinate with technology vendors, airport operators, and other stakeholders related to the RDT&E, procurement, and deployment of checkpoint screening technologies, agency officials stated that they plan to develop and implement such a process. Specifically, TSA officials stated that they have developed a draft communications plan, which is being reviewed, that will document the communications process. However, TSA could not provide an expected completion date for the plan. Although such a plan should help in providing consistency to the agency's coordination efforts, without knowing the specific activities the plan will include or when it will be implemented, we cannot determine the extent to which the plan may

[55]We focused our work on TSA's coordination and collaboration with airport operators and technology vendors, and not on S&T's coordination and collaboration with these external stakeholders, because TSA is responsible for procuring and deploying checkpoint technologies.

strengthen coordination. In addition, in September 2007, TSA hired an Industry Outreach Manager within its Office of Security Technology to improve relationships with airport operators and communication with internal TSA stakeholders related to screening technologies, including checkpoint technologies. In general, the Industry Outreach Manager is the communications liaison for the Office of Security Technology stakeholders and customers to exchange ideas, information, and operational expertise in support of the office's mission and goals, and to provide cutting-edge technologies in the most efficient and cost-effective means possible. In addition to these steps, in January 2007, S&T created a Corporate Communications Division to coordinate on a wide variety of science and technology efforts with public and private sector stakeholders. This office is in the process of developing a tool to assess the effectiveness of its outreach efforts to industry stakeholders.

The AMS guidance recommends that TSA coordinate with airport operators to work out all equipment installation issues prior to deployment. According to TSA officials, the role of the airport operator is essential in ensuring that solutions under development are suitable for use in an airport environment, taking into consideration all logistical and operational constraints and possibilities. As described earlier, provisions of the Homeland Security Act address the need to coordinate research and development efforts to further homeland security missions, and reinforce the importance of coordinating and collaborating with airport operators. TSA sponsors monthly conference calls with airport operators to discuss issues of general interest and, according to S&T officials, S&T has conducted pilot studies with airport operators. However, according to many of the 33 airport operators we interviewed,[56] TSA's coordination on the priorities for and deployment of checkpoint screening technologies has been inconsistent. Specifically, of the 33 airport operators we interviewed, 8 had only positive comments about TSA's coordination and 16 expressed only concerns regarding TSA's coordination efforts, while 9 expressed both positive comments and concerns. Eleven of the 33 airport operators told us that TSA had not shared information with them regarding checkpoint technology needs and priorities. For example, an airport operator stated that TSA provided specifications for new screening technologies with sufficient lead time for the airport, which was building a

[56]We selected a nonprobability sample of 40 airports and obtained the views of 46 operators at these airports regarding coordination with TSA. Thirteen of the 46 airport operators did not express an opinion about coordination for and deployment of checkpoint screening technologies. See appendix I for more information on how we selected these airports.

new checkpoint at the time, and that TSA had numerous coordination meetings with airport officials to determine space constraints, power requirements, and other factors. However, this same airport operator expressed a desire for more coordination by TSA in the agency's selection of the technologies to be pilot tested at this airport. Another airport operator stated that, when TSA asks for volunteers to participate in checkpoint screening technology pilot programs, it is difficult to agree to participate because TSA does not clearly communicate the program's goals or the capabilities of the technology in the pilot program.

According to airport operators at another airport, TSA officials told them that they would have the latitude to select the ETP from either of two vendors on the TSA contract for purchase. According to the airport officials, after they selected equipment from one of the vendors because it would fit into the physical layout of the airport's checkpoint, TSA told the airport officials that particular ETP vendor was no longer under contract with TSA. As a result, airport officials stated that they had to redesign the checkpoint, including raising the ceiling, to accommodate the other vendor's ETP. Senior officials in TSA's Office of Operational Process and Technology, the office responsible for the development and implementation of security technologies across several modes of transportation, subsequently agreed that coordination with airport managers and other stakeholders could be improved.

According to TSA officials, coordinating with technology vendors is essential in order to determine what technology platform would be appropriate and capable of providing the required detection and throughput capabilities. S&T and TSA have conducted outreach efforts to coordinate with technology vendors. For example, S&T officials stated that they have hosted forums known as industry days and attended conferences to discuss types of technologies needed to be developed and the department's priorities for research and development. S&T officials also stated that they make presentations at technology-related conferences, symposia, and exhibits, highlighting the work conducted by S&T. At every industry day and conference, officials said, airport security and checkpoint screening technologies have been discussed. In addition, TSA has coordinated with technology vendors through industry days, individual meetings, and conferences. For example, TSA officials stated that TSA held industry days with technology vendors to provide a forum to communicate information to potential vendors on specific technology testing and procurement efforts, and to allow vendors to ask questions regarding technology projects and TSA expectations.

Despite these outreach efforts, of the seven vendors we interviewed who had contracted with TSA to provide checkpoint screening technologies, officials from five vendors expressed concerns about the agency's ability to coordinate with them on current or future needs for checkpoint technologies. Officials from four of the seven vendors stated that TSA had not communicated a strategic vision for screening technologies that will be needed at the checkpoint in the future, and that TSA did not effectively and clearly communicate standards and requirements for technologies to vendors. For example, just as TSL officials commented that TSA did not always provide clear and quantifiable requirements to conduct tests of screening technologies, vendors stated that TSA had not communicated effectively about its future needs, such as the operational requirements for an advanced, integrated checkpoint screening system.[57] Therefore, a vendor official stated that some of them had taken the initiative to develop integrated screening technologies in the hope that TSA will eventually request this type of integrated system. TSA did not express an opinion regarding the specific concerns raised by the technology vendors, but a senior TSL official stated that TSA should sponsor better briefings for vendors after the agency announces its intentions to develop new technologies. The official stated that these briefings could provide vendors with an opportunity for open dialogue with TSA and clarification of TSA's needs for new technologies. According to a vendor, without adequate coordination and communication from TSA, the vendors' ability is limited in deciding how best to invest their resources to develop new checkpoint screening technologies.

In addition to coordinating and collaborating with airport operators and technology vendors, S&T and TSA coordinate and collaborate on the department's RDT&E efforts with other federal agencies through participation in the Technical Support Working Group, which is co-chaired by the Departments of Defense and State. The Technical Support Working Group is the U.S. national forum that identifies, prioritizes, and coordinates interagency research and development of technologies to

[57]Section 4014 of the Intelligence Reform Act required TSA to "develop and initiate a pilot program to deploy and test advanced airport checkpoint screening devices and technology as an integrated system at not less than 5 airports in the United States" by March 31, 2005. See Pub. L. No. 108-458, § 4014, 118 Stat. at 3720. According to TSA, the only advanced checkpoint screening technology available to TSA at that time was the ETP, and TSA initially conducted pilot tests at five airports and later expanded the tests to 16 airports. TSA officials stated that the agency submitted a strategic report to Congress on August 9, 2005, *Detection Equipment at Airport Screening Checkpoints*, in satisfaction of this requirement in the Act.

combat terrorist acts, including explosives detection technologies. S&T also coordinates with the national laboratories on homeland security research.[58] Specifically, S&T's Office of National Laboratories coordinates homeland security-related activities and laboratory-directed research conducted within the Department of Energy's national laboratories. According to an S&T senior official, S&T has worked with the national laboratories to supplement S&T's research and development of explosives detection technologies by tasking the national laboratories to conduct basic research on the characteristics of homemade explosives.

Conclusions

Researching, developing, testing and evaluating, procuring, and deploying checkpoint technologies capable of detecting ever-changing threats to the commercial aviation system is a daunting task. Although TSA has recently produced a strategic plan that identified a strategy for the PSP, neither the plan nor the agency's strategy for researching, developing, and deploying checkpoint technologies was informed by some key risk management principles, including a risk assessment, cost–benefit analysis, and performance measures. Without conducting a risk assessment that includes all three elements of risk—threat, vulnerability, and consequence—and completing a cost–benefit analysis to guide the PSP strategy, TSA has limited assurance that its strategy targets the most critical risks and that it invests in the most cost-effective new technologies or other protective measures. Further, without developing performance measures that assess the extent to which checkpoint screening technologies achieve the PSP's security goals and thereby reduce or mitigate the risk of terrorist attacks, TSA is limited in its ability to determine the success of its strategy and make needed adjustments. Even though TSA has not implemented a risk-informed strategy to ensure that its investments target the most pressing security needs, the agency has moved forward in investing in new checkpoint screening technologies.

Despite limited progress in the RDT&E, procurement, and deployment of new checkpoint screening technologies during the first few years that S&T and TSA had responsibilities related to these technologies, more recently, the organizations have made progress as reflected by the number of technologies for which procurement and deployment has been initiated.

[58]The Homeland Security Act addresses the need for DHS to work with federal laboratories and the private sector, among others, to develop innovative approaches to produce and deploy the best available technologies for homeland security missions. See Pub. L. No. 107-296, § 102(f)(5), 116 Stat. at 2143-44.

TSA faced challenges with the first new technology that it procured and deployed—the ETP. In the interest of protecting the homeland, it is understandable that TSA may, at times, not follow all established guidance in an effort to deploy technologies quickly to address urgent threats and vulnerabilities. However, deploying the ETP despite unresolved performance concerns identified during testing of earlier ETP models, as well as failing to ensure that ETP models that were ultimately deployed had passed operational testing, increased the risk that the machines would not perform as intended, resulting in a questionable security benefit. TSA did not follow AMS guidance that recommended operational testing of a new technology prior to deployment because it is more cost effective to resolve performance issues then. While TSA deployed the ETPs to provide a much-needed capability to automatically screen higher risk passengers at airport checkpoints, relying on the ETPs could have resulted in airport checkpoints being more vulnerable given the ETPs' performance problems and lack of operational testing. Also, relying on the ETPs to screen these particular passengers instead of existing screening procedures may not enhance airport checkpoint security because TSA does not know if ETP screening provides an improved detection capability compared to existing screening procedures. Moreover, it is risky to substitute any new technology for existing screening procedures before the technology has been proven to be effective through operational testing. Although TSA is trying to deploy new technologies to address immediate threats, the problems associated with the development and deployment of the ETPs may be repeated with other technologies unless TSA adheres to testing guidance and makes decisions using a knowledge-based acquisition approach. Finally, it is not clear whether it is worthwhile to continue to use the ETPs currently deployed to airports due to the costs associated with maintaining the machines in good, operational condition.

Recommendations for Executive Action

To help ensure that DHS's Science and Technology Directorate (S&T) and Transportation Security Administration (TSA) take a comprehensive, risk-informed approach to the RDT&E, procurement, and deployment of airport passenger checkpoint screening technologies, and to increase the likelihood of successful procurements and deployments of such technologies, in the restricted version of this report, we recommended that the Assistant Secretary for TSA take the following eight actions:

- Conduct a complete risk assessment, including threat, vulnerability, and consequence assessments, which would apply to the PSP.
- Develop cost–benefit analyses to assist in prioritizing investments in new checkpoint screening technologies.

- Develop quantifiable performance measures to assess the extent to which investments in research, development, and deployment of checkpoint screening technologies achieve performance goals for enhancing security at airport passenger checkpoints.
- After conducting a complete risk assessment and completing cost-benefit analyses and quantifiable performance measures for the PSP, incorporate the results of these efforts into the PSP strategy as determined appropriate.
- To the extent feasible, ensure that operational tests and evaluations have been successfully completed before deploying checkpoint screening technologies to airport checkpoints.
- Evaluate whether TSA's current passenger screening procedures should be revised to require the use of appropriate screening procedures until it is determined that existing emerging technologies meet their functional requirements in an operational environment.
- In the future, prior to testing or using all checkpoint screening technologies at airports, determine whether TSA's passenger screening procedures should be revised to require the use of appropriate screening procedures until the performance of the technologies has been validated through successful testing and evaluation.
- Evaluate the benefits of the Explosives Trace Portals that are being used in airports, and compare the benefits to the costs to operate and maintain this technology to determine whether it is cost-effective to continue to use the machines in airports.

Agency Comments and Our Evaluation

We provided a draft of our restricted report to DHS for review and comment. On April 7, 2009, DHS provided written comments, which are presented in Appendix II. In commenting on our report, DHS stated that it agreed with our recommendations and identified actions planned or underway to implement them. While DHS is taking steps to address our first and second recommendations related to conducting a risk assessment, the actions DHS reported TSA had taken or plans to take do not fully address the intent of the remaining six recommendations.

In its comments, DHS stated that it concurred with our first recommendation that a risk assessment should be developed for the PSP and that TSA has two efforts currently underway to do so. Completion of TSA's first effort—the Air Domain Risk Analysis (ADRA)—is expected in the winter of 2009. DHS commented that TSA's second effort is the Risk Management and Analysis Toolset (RMAT), a model to simulate the potential of some technologies to reduce the risk of certain threat scenarios which will apply specifically to the passenger screening process. DHS reported that it expects initial results from RMAT to be available during the second quarter of 2009. DHS further stated that TSA has made

resource allocation and technology decisions that were informed by consideration of risk (including threat, vulnerability, and consequence), although not by comparative assessments of these three elements. However, as we reported, TSA has not conducted a risk assessment for the PSP, and it is unclear to what extent the ADRA would provide risk information needed to support the PSP. Until such a risk assessment is developed and integrated into TSA's strategy for the PSP, TSA continues to invest in checkpoint technologies without the benefit of a risk-informed strategy and increases the possibility that its investments will not address the highest-priority security needs.

DHS also concurred with our second recommendation that it develop cost-benefit analyses. DHS commented that TSA is developing an approach for selecting cost-effective technologies by developing life-cycle cost estimates and using the RMAT tool to determine how technologies balance risk (based on current threats) with cost. TSA's decision to collect cost and benefit information is a positive first step. Irrespective of how TSA collects data on the costs and benefits of technologies, it is important, as we reported, that TSA conduct cost-benefit analysis of each checkpoint technology that it invests in that weighs the costs and benefits of technologies relative to the costs and benefits of other solutions. Such analysis is important because it helps decision-makers determine whether investments in technologies or in other security programs will provide the greatest mitigation of risk for the resources that are available.

DHS concurred with our third recommendation that TSA develop quantifiable performance measures to assess the extent to which TSA's investments in checkpoint screening technologies make the checkpoint more secure, the key mission of the program. DHS commented that it currently collects quantifiable performance attributes for all potential acquisitions with regards to metrics, such as detection, false alarm rate, and operational availability and plans to use information on machines' attributes as measures of the PSP's overall effectiveness as a program. However, these actions will not fully address our third recommendation. First, information collected on potential acquisitions prior to their deployment may not reflect their performance in an operational environment; consequently, relying on information about technologies' attributes rather than measuring the effectiveness of deployed technologies to secure the checkpoint will likely have limited value in terms of measuring the effectiveness of the PSP as a program. Second, as we reported, the ETP example illustrates that TSA did not collect information on the ETP's performance attributes such as operational availability during laboratory testing prior to procurement and did not collect data on the ETP's detection capabilities during tests in an

operational environment. This raises questions about the completeness of data TSA collects on technologies prior to acquisition and deployment. We could not verify that TSA collects such information on other technologies because TSA did not provide documentation to support this comment. As TSA moves forward in developing performance measures, it is important that these measures reflect not only efficiency of the technologies to process passengers but the effectiveness of technologies and other countermeasures to make the checkpoint more secure and thereby reduce the risks posed by those most pressing threat scenarios that will be identified once TSA completes its risk assessment.

In addition, DHS concurred with our fourth recommendation that it develop a PSP strategic plan that reflects the risk assessment, cost benefit analysis, and performance measures. DHS commented that TSA plans to combine results from the RMAT tool and lifecycle cost estimates for possible technology solutions that strike a balance between risk and efficient use of funding. DHS also stated it will use RMAT to develop proxy measures and general "what-if" analysis and risk insights. However, these actions alone will not satisfy the intent of this recommendation. While it is possible that proxy measures could be developed to assess the extent to which TSA's investments in the research and development of technologies have achieved program goals of making the checkpoint more secure, to fully address this recommendation, TSA must also conduct a risk assessment that addresses the PSP, develop quantifiable measures that clearly assess the PSP's progress towards its security goals, and revise its strategic plan accordingly.

DHS concurred with our fifth recommendation that before deploying technologies to airport checkpoints, the technologies should successfully complete testing and evaluation and stated that TSA is taking action to implement a formal testing process. DHS commented that TSA has prepared a Test and Evaluation Master Plan (TEMP) that describes a new formal testing process that is consistent with DHS's new acquisition directive. However, the TEMP does not address the intent of this recommendation. We deleted from this public report our evaluation of why the TEMP does not address the intent of this recommendation, because TSA determined our evaluation to be sensitive security information.

Further, DHS agreed with our sixth and seventh recommendations that TSA evaluate whether its screening procedures should be revised to require the use of appropriate procedures until it can be determined that emerging technologies or future technologies that may be developed meet all of their requirements in an operational environment. However, DHS's

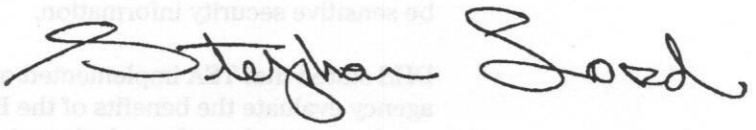
comments suggest that it does not intend to implement these recommendations. DHS commented that the performance of machines is always measured and confirmed in the laboratory setting prior to operational field testing. However, we disagree that laboratory testing is sufficient to address this recommendation. We deleted from this public report our evaluation of why laboratory testing alone does not address the intent of this recommendation, because TSA determined our evaluation to be sensitive security information.

DHS stated that TSA implemented our eighth recommendation that the agency evaluate the benefits of the ETP, such as its effectiveness, and conduct a cost-benefit analysis to determine whether the technologies should remain in use at airports. However, we disagree that TSA has implemented this recommendation. DHS commented that two actions fulfilled this recommendation: TSA's current program management reviews in which costs are periodically discussed with vendors and the laboratory testing of the ETP's detection capabilities. To fully address this recommendation, a cost-benefit analysis and tests of the ETP's effectiveness to detect explosives in an operational environment are required. As we reported, TSA has not conducted cost-benefit analyses, which, as noted earlier, should compare costs and benefits of alternative solutions. Discussions of maintenance costs with vendors on a periodic basis do not constitute a cost-benefit analysis.

Based on DHS's written comments, we deleted a reference to the 2004 OMB PART review in a footnote because of updated information from OMB's 2008 PART review. DHS also provided us with technical comments, which we considered and incorporated in the report where appropriate. In particular, we clarified the wording of a recommendation which originally stated that TSA should develop quantifiable performance measures to assess the extent to which investments in research, development, and deployment of checkpoint screening technologies have mitigated the risks of a terrorist attack. We altered the wording to state that performance measures should be developed to assess progress towards security goals.

As agreed with your offices, unless you publicly announce the contents of this report, we plan no further distribution for 45 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Assistant Secretary of the Transportation Security Administration, and appropriate congressional committees.

If you or your staffs have any questions about this report, please contact me at (202) 512-8777 or LordS@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Stephen M. Lord
Director
Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

This report addresses the following questions: (1) To what extent has the Transportation Security Administration (TSA) developed a risk-informed strategy to prioritize investments in the research and development of passenger checkpoint screening technologies? (2) What new passenger checkpoint screening technologies has the Department of Homeland Security (DHS) researched, developed, tested and evaluated, procured, and deployed since its creation, and why did TSA halt the first technology deployment that it initiated—the Explosives Trace Portal (ETP)? (3) To what extent has DHS coordinated the research, development, test and evaluation (RDT&E), procurement, and deployment of passenger checkpoint screening technologies internally and with key stakeholders, such as airport operators and technology vendors?

To determine the extent to which TSA has developed a risk-informed strategy to prioritize investments in the research and development of passenger checkpoint screening technologies, we analyzed program documents, TSA's August 2008 strategic plan for checkpoint technologies, TSA's September 2007 report on the development of a strategic plan, technology project plans, and funding. We also compared TSA's strategic plan and DHS's responses regarding their efforts to manage their research and development investments, with DHS's guidance from the National Infrastructure Protection Plan on how to utilize risk management principles to target funding.

To determine the extent to which DHS researched, developed, tested and evaluated, procured, and deployed new checkpoint screening technologies since its creation, and to identify why TSA halted deployment of the ETP, we analyzed TSA's strategic plan for checkpoint technologies, TSA's Passenger Screening Program (PSP) documentation, including information on the status of technologies being researched, developed, tested and evaluated, procured, and deployed. Regarding the ETPs, we analyzed the functional requirements for the system, contracts with General Electric and Smiths Detection, and test reports for acceptance tests, regression tests, and operational tests. We also reviewed ETP deployment schedules and documentation on operational availability and mean time between critical failure, and interviewed TSA officials about the reasons that the ETP deployment was halted. We also compared the ETP test approach used by S&T and TSA to the Acquisition Management System (AMS) guidance and knowledge-based acquisition best practices.[1] We also

[1]See GAO-06-257T.

interviewed TSA and S&T officials to obtain information on current investments in the research, development, and deployment of checkpoint technologies, and conducted site visits to the Transportation Security Laboratory in Atlantic City, New Jersey, and Tyndall Air Force Base, Florida, to observe testing of new checkpoint technologies. We visited the TSL because that is where S&T tests and evaluates technologies, including checkpoint screening technologies. We visited Tyndall Air Force Base because technologies to detect bottled liquids explosives were being tested there. Additionally, we analyzed TSA's passenger screening standard operating procedures and interviewed various TSA headquarters officials, 29 Federal Security Directors, 1 Deputy Federal Security Director, and 5 Assistant Federal Security Directors for Screening, and visited nine airports where the ETPs had been or were to be deployed or new checkpoint screening technologies were undergoing pilot testing. We chose these officials because they are the senior official at the airport in charge of security and manage TSA's role in deploying new technologies at the airport. We selected these nine locations based on the technologies that had been deployed or were being tested, their geography, size, and proximity to research and development laboratories. Of the nine airports we visited, the ETPs had been or were to be deployed to seven of them, and other new checkpoint screening technologies were undergoing pilot demonstrations or testing at two of them. We visited four airports on the east coast, and three airports on the west coast, and two airports located in the west and southwestern regions of the United States. To determine whether the ETP's requirements had been tested prior to procuring and deploying them, we selected a non-probability sample of 8 out of the 157 total requirements. We selected the 8 requirements because they were related to some of the ETP's key functionality requirements, including operational effectiveness, operational suitability, and passenger throughput.

To determine the extent to which DHS has coordinated and collaborated on the RDT&E, procurement, and deployment of passenger screening technologies internally and with key stakeholders, we analyzed program documents, including an August 2006 memorandum of understanding between TSA and S&T for the management of the Transportation Security Laboratory (TSL). Additionally, we interviewed Department of State officials, TSA and S&T officials, seven checkpoint technology vendors, and

airport operators[2] and other officials at airports where ETPs were initially deployed. Because we selected nonprobability samples of airports to visit and officials to interview, we cannot generalize the results of what we learned to airports nationwide. However, the information we gathered from these locations and officials provided us with insights and perspectives on DHS's efforts to operationally test and evaluate, and deploy checkpoint technologies that could only be obtained from officials stationed at locations where the technologies had been tested or deployed. We reviewed the Acquisition Management System, the Aviation and Transportation Security Act, the Homeland Security Act of 2002, and the Intelligence Reform and Terrorism Prevention Act and identified requirements and guidance for coordination and collaboration among S&T, TSA, and other stakeholders. We also reviewed S&T's and TSA's coordination activities and compared them to TSA program guidance and GAO's recommended coordination practices regarding agency coordination with external stakeholders.[3]

We conducted this performance audit from June 2006 through April 2009 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 and conclusions based on our audit objectives.

[2]TSA defines an "airport operator" as any persons, who operates an airport serving an aircraft operator or foreign air carrier required to have a security program under 49 C.F.R. parts 1544 or 1546. See 49 C.F.R. § 1540.5.

[3]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 21, 2005).

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 6, 2009

Ms. Cathleen A. Berrick
Managing Director, Homeland Security and Justice Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Berrick:

Thank you for the opportunity to comment on the draft report: *DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges* (GAO-09-21). The Transportation Security Administration (TSA) appreciates the U.S. Government Accountability Office's (GAO) work in planning, conducting, and issuing this report.

In its report, GAO recommends that TSA improve its analysis of technologies prior to deployment through increased use of risk-management principles and cost-benefit analyses. TSA agrees that there are opportunities for improvement in the deployment of passenger checkpoint technologies and will continue to take steps to advance the testing, deployment, ongoing performance measurement, and stakeholder outreach as each relates to these technologies.

The Passenger Screening Program has embraced the challenge to design and engineer passenger screening as an integrated network of technologies, human factors, and processes to minimize the risk of terrorist attack, using an approach that accounts for the strategic, tactical, and operational realities of the airport environment. As a strategy, the proactive approach builds upon lessons learned from hard intelligence, airport security operations, and TSA organizational experience.

The goals of TSA's security initiatives are to improve explosives detection capability by combining new technology with advanced procedures, establish a cadre of trained behavior detection officers, and incorporate unpredictability into screening measures to thwart terrorist plans. In each operational environment, be it at the checkpoint, in the queues, or in conversations with passengers, TSA created approaches designed to detect and contain risks to minimize catastrophic loss of life or property.

Today, TSA implements passenger checkpoint screening through a risk-informed approach that integrates a variety of sensors, devices, and techniques into a threat detection and response network. This integrated, network-centric approach considers operational requirements to maximize passenger throughput, minimize the number of operating personnel, and protect privacy, all within the constrained footprint of the checkpoint. This

proactive approach relies on an optimized, integrated, mix of networked systems to deter known threats through the passenger screening checkpoint.

TSA's Risk-Informed Strategy

While TSA recognizes that additional risk-informed management initiatives should and will be undertaken, current security technology initiatives have been developed based on an assessment of what TSA believes to be the most cost-effective way of reducing risk across the entire aviation system.

TSA has made resource allocation and technology decisions that were informed by considerations of risk (including threat, vulnerability, and consequence), although not by explicit formal comparative assessment of risk, including threat, vulnerability, and consequence (TVC). This approach was appropriate at TSA's previous level of maturity, and through this process, the Agency gained important insights that have become guiding principles for risk management decisions.

These principles include a deep appreciation for uncertainty and for the limits of what can be known. TSA cannot predict every attack vector in the aviation domain; therefore, our strategy reflects a bias against rigid prioritization and narrow, inflexible solutions that can be overcome by dynamic, adaptive adversaries. TSA continues to focus on developing capabilities that are flexible and adaptable, that cut across risks and threats, and that contain elements of randomness or unpredictability to inject uncertainty into adversaries' planning process. These principles have informed many of TSA's operational and technology decisions in the last few years.

As this work has progressed, TSA has also pursued a formal TVC risk analysis as important decision inputs into future strategy development. TSA has nearly completed a range of formal, comparative, scenario-based TVC risk analyses. The results will be used—along with other factors, such as cost, feasibility, statutory requirements, and privacy—to inform decisions about strategy, operations, and technology development across TSA's aviation security responsibilities, including the Passenger Screening Program (PSP).

At the strategic level, TSA is updating the initial Air Domain Risk Analysis (ADRA), an action item stemming from Homeland Security Presidential Directive 16, with final completion expected in November 2009 and approval expected in the fourth quarter of calendar year 2009. The initial ADRA will compare high-level risks to and through the checkpoint with other high-level risks (*e.g.,* risks involving aviation infrastructure and general aviation) across the domestic U.S. air domain. High-level countermeasures are also evaluated to identify their aggregate, cross-cutting risk-reduction potential across the portfolio of risks. The ADRA will also include a view of risks that originate internationally.

At a more granular level, TSA has been developing the Risk Management and Analysis Toolset (RMAT). RMAT is an agent-based, high-detail simulation model of the commercial aviation security regime, and can be used to model specific risk scenarios (for example, specific types and sizes of explosives) and the risk-reduction potential (across the portfolio of risks) of specific technologies or other countermeasures. The model accounts for dynamic, adaptive adversaries by incorporating intelligence analysis to model the adversary's decision

processes and using that as the threat input, rather than using a direct, static estimation of a threat vector.

This initial set of scenarios is keyed to the actionable decision-support needs of TSA leadership in the near term. The initial RMAT outputs are expected to be available to offer insights to TSA leaders in the second quarter of calendar year 2009. As RMAT data sets and capabilities grow, a larger range of high-detail risks can be modeled; and the effectiveness of a greater range of potential countermeasures can be evaluated.

These improved formal tools for understanding risk in a comprehensive and comparative way—explicitly considering comparative TVC—will offer additional insights and support to TSA leaders making decisions in aviation security, including in the PSP. These tools, and formal risk analysis generally, offer the additional effect of challenging accepted assumptions and surfacing hidden assumptions, providing another benefit to the decision process. Finally, formal comparative TVC risk analyses do not replace, but rather complement and enhance, TSA's principles of risk management described previously. Together they will enable TSA leaders to make decisions on aviation security that are more effective, more flexible, more traceable, and more defendable.

Measuring Performance

TSA conducts a range of threat and vulnerability assessments relative to the checkpoint to select, prioritize, and determine the effectiveness of operational and technology investments. At the field level, Federal Security Directors (FSDs) conduct various types of testing and assessment of operations of their checkpoints. TSA also conducts Joint Vulnerability Assessments (JVAs) in collaboration with the Federal Bureau of Investigation (FBI) at airports on a regular basis. The results of JVAs help provide understanding of common vulnerabilities and trends. On a national level, TSA's Office of Inspection conducts covert testing of checkpoint operations (Red Team testing). This method of measuring the checkpoint's effectiveness, both operationally and technologically, against a simulated attack can identify vulnerabilities that may be specific to one airport or common across the system. Covert tests serve both as a measure of vulnerability that can help inform investment decisions and a reality-based measure of effectiveness of existing operational and technology investments. TSA collaborates with GAO to review Red Team results based on threat injects conducted at checkpoints. In addition, TSA continually monitors field equipment performance data such as Mean Down Time (MDT), Operational Availability (OA), Mean Time to Repair (MTTR), and throughput.

TSA recognized that it needed a more systematic, nationwide framework to assess the effectiveness of the screening process and to identify areas to focus our resources in training and technology. To this end, TSA instituted a comprehensive program to measure screening performance called the Aviation Screening Assessment Program (ASAP). ASAP is aggressively focused on improving recognition of Improvised Explosive Devices (IEDs), and TSA has performed thousands of covert assessments at airports across the country. Through ASAP, we are assessing our performance every day in every aspect of the screening process. Findings from ASAP are reported directly to TSA leadership, who use these performance metrics to make strategic decisions within the screening environment. These decisions include the type of equipment TSA purchases to the type of training TSA delivers to our Transportation Security Officers (TSOs).

In addition, TSA recognizes the value of measuring program progress by developing core program metrics. Through TSA's participation in the Office of Management and Budget (OMB) Program Assessment Rating Tool (PART), the Agency measures both long-term and annual performance metrics. Along with the Reliability, Maintainability, Availability (RMA) metrics, PSP calculates the Operational Availability of Passenger Screening Equipment, the Cost per Bag Screened, and the Ratio of Bags Screened to Passenger Screener Full-Time Equivalent (FTE) Expended. In addition, TSA includes key performance parameters in all technology specifications and tests the technology against those measures. These measures reflect different facets of the purpose of PSP. Contrary to footnote 43 of the draft GAO report, the most recent review (2008) of PSP by OMB through the PART ranked the program as "Effective."

Testing and Evaluation Strategy for New Technologies

TSA is in the process of improving the already robust Testing and Evaluation (T&E) paradigm to ensure that operational effectiveness and suitability of candidate security technology systems are evaluated prior to deployment. Employing the concept of independent and integrated T&E in support of acquisition decisions and other program reviews, this process leverages data from multiple developmental and operational testing sources, accredited vendor data, modeling and simulation, and other special analyses (as required), in accordance with T&E and systems engineering principles and best practices, to streamline T&E requirements while still providing a credible and comprehensive evaluation product. The system-specific integrated T&E strategy addresses technical and operational requirements, considering the contributions of people, processes, and technologies, to provide a single portrait of anticipated mission capabilities for decision makers. TSA is also active in the U.S. Department of Homeland Security (DHS) T&E Council, which will lead to implementation of best practices for T&E across DHS.

TSA has prepared a Test and Evaluation Master Plan (TEMP) for the PSP program and is implementing a formal testing process specified in the TEMP, consistent with DHS's new Acquisition Directive 102. The TEMP establishes a framework that provides an overview of the testing processes followed for all PSP technologies to ensure products meet our specifications, are safe, and operationally effective. The test and evaluation strategy is consistent with the program acquisition strategy. All PSP technology projects follow this testing process, which includes, at a minimum, qualification test and evaluation (QT&E) conducted by the DHS Directorate for Science & Technology (S&T) and operational test and evaluation (OT&E) conducted by TSA. While QT&E tests equipment in a lab setting to validate its operational effectiveness, OT&E tests the product in an airport setting to validate its operational suitability.

Recognizing that Initial Operational Testing and Evaluation (IOT&E) principles mandate examining system detection performance in the field environment, TSA's Office of Security Technology (OST) recently implemented a process to better coordinate realistic threat portrayal with our developmental/technical testing partners. Starting with a common threat baseline, we have developed a process to evaluate system performance (considering operators, systems under test, and concepts of operations) against both active threat agents in a laboratory environment, as well as threat surrogates covertly inserted in the stream of commerce, to better understand the system detection performance envelope. Threat surrogates employed for OT&E purposes have undergone a rigorous verification, validation,

and accreditation (VV&A) process to ensure that stimulants not only generate appropriate threat signatures (and equivalent responses) relative to the technologies of interest, but also can be strongly correlated back to the active threat and appropriate segment of the threat space for the system of interest.

As much of our operational testing is conducted in active environments, in situations where security decisions are being made with systems under test (to most realistically demonstrate operational performance), test design and execution is structured to ensure that test conduct does not degrade the current security posture within the venue. Depending on the specific test, TSA may employ redundant processes and technologies to minimize potential security risks prior to operational test execution. It should also be noted that detection effectiveness, as per TSA testing strategy, is always measured and confirmed in the laboratory setting prior to operational testing in the field.

Transportation Security Integration Facility Testing (TSIF)

TSA has completed the construction of a state-of-the-art facility permitting emerging technologies to be tested for extended periods of time while simulating a variety of operational conditions. This facility will allow TSA to evaluate future maintenance needs and the most efficient operational configurations of new equipment while avoiding disruption to the flow of passengers at checkpoints. The TSIF began operations in January 2009.

Explosives Trace Portal (ETP) Testing and Deployment

In response to a growing concern that terrorists may try to destroy an airplane by packing explosives on their person, TSA tested, procured, and deployed ETP technology from 2004 to 2006. TSA followed its standard technology development process for the ETP, which includes requirements development, testing, procurement, and deployment.

TSA and the DHS S&T followed a formalized testing process, including laboratory and field testing, from April 2004 to January 2006, to validate the effectiveness and suitability of ETPs prior to full-scale deployment. QT&E testing of two vendors' submissions was completed by the Transportation Security Laboratory (TSL) in 2004, confirming the ETP technology was effective in detecting explosives in accordance with TSA's technical detection standards. TSA proceeded with airport operational assessments by fielding five General Electric (GE) ETP systems in 2004. During the field evaluations, TSA assessed the suitability of the system and the Portal Quality Control (PQC) patches, to evaluate the quality of the patches and the application process in a checkpoint environment. As the GAO report noted, the PQC patch performed unfavorably in the February 2005 tests. The test report also indicated that a combination of factors, including the method of testing, environmental conditions, the undetermined shelf life of PQC patches, and the possible variance between levels of explosive materials in the PQC patch, which could have affected detection performance. It is important to note that detection effectiveness was established at the TSL in 2004 and that the PQC assessment demonstrated that the airport assessments did not accurately represent the ETP detection performance, since the reliability of the quality control items was unconfirmed in the field.

The ETPs were further tested by S&T at Idaho National Engineering and Environmental Laboratory (INEEL) in 2005 using methods that were not available to the TSL at that time

(live explosives). The testing at INEEL was presented to TSA by S&T as part of developmental data collection effort for research and development purposes. The INEEL test administrator who conducted the test was not authorized to perform qualification testing on the ETPs, nor was it considered as part of the detection effectiveness assessment. The performance of the ETPs during this testing was not assessed against the established standards.

S&T and TSA proceeded to further assess modified ETP systems from December 2004 to February 2005, reviewing software modifications performed by the vendor. The February 2005 review concluded that the requirements for detection were met by the modified ETP systems. TSA proceeded with another round of airport operational assessments from April to May 2005 to further validate operational suitability. Field test results demonstrated satisfactory performance, indicating the equipment was ready for full-scale deployment. In April 2006, TSA began deploying ETPs to airports.

Additional Testing

In 2006, TSA initiated another round of laboratory testing of the ETP to evaluate its operational effectiveness. During April and May of 2006, INEEL conducted testing on both vendor submissions that revealed deficiencies in reliable performance. Once these test results were received, along with exhibited performance issues with the fielded units, TSA's Office of Acquisitions formally notified the ETP vendor in June 2006 that TSA would not deploy any additional ETPs until the performance issues were addressed. Remaining delivery units were diverted to the TSA warehouse until improvements could be completed and verified. TSA received a reasonable level of assurance from the vendor that these issues could be successfully addressed.

After working with vendors for several months, it was determined that the ETP technology could not be enhanced, and vendors chose not to make additional upgrades. Consequently, TSA did not purchase any further units. TSA determined it was beneficial to keep the existing fielded units in place, since they were effective at detecting explosives when the performance reliability issues did not interfere.

Reliance on New Technologies

As has been described, TSA follows a strict testing process for all technologies before they are fully deployed. It should also be noted that detection ability, as per TSA testing strategy, is always measured and confirmed in the laboratory setting prior to operational testing in the field. For example, in the case of Whole Body Imagers (WBIs), the TSL Independent Test and Evaluation Division (IT&E) has conducted a series of laboratory tests evaluating their performance. The WBI is currently being evaluated against established criteria of threat detection, passenger throughput, and operational availability. In contrast to the ETP, the WBI provides the capability to detect a wider range of threats, including metallic and nonmetallic explosives threats. IT&E has performed five lab assessment-quality test series of WBIs with various devices and/or operational procedures starting in February 2007 and continuing to the present. These tests compare TSO performance while using WBI devices to that of a manual pat-down process. In the event of a WBI alarm, current Standard Operating Procedures (SOPs) require a minimum of a pat-down. All test results indicate the WBI technology is an effective alternative to the pat-down process.

Stakeholder Coordination and Collaboration

TSA appreciates GAO's conclusion that collaboration with S&T; our external stakeholders, including technology vendors; and our airport staff is an essential element to the successful testing, evaluation, and deployment of checkpoint technologies. TSA also values the relationships that have been fostered with industry stakeholders throughout the aviation and security technology communities. While TSA has taken measures to increase coordination with S&T through the development of a Memorandum of Understanding (MOU), the Capstone Integrated Product Team (IPT), and the associated PSP working group, the findings in GAO's report further highlight the need to increase the level of formal coordination with S&T.

TSA has participated in several American Association of Airport Executives conferences. TSA also hosted an airport symposium in the fall of 2007, in which it shared its vision for the future with airport operators and the public. TSA's OST regularly participates in outreach conferences to discuss the technologies available for passenger and baggage screening. To better focus its efforts in this regard, TSA has established a new position on checkpoint stakeholder outreach. In addition, TSA partners with DHS to host technical interchange meetings and industry days where Original Equipment Manufacturers are invited to discuss future requirements for various technologies. These efforts should ultimately reduce costs and development time as vendors work to meet TSA's screening requirements.

TSA also makes every effort to effectively coordinate and collaborate with our airport field staff. During deployment of passenger screening technologies, TSA meets weekly with airports to discuss plans, status, and any issues that arise. TSA has also initiated a TSO focus group in which OST periodically meets with a select group of TSOs to gather their input on new technology and process requirements for passenger screening. As part of TSA's OT&E testing conducted for all equipment, TSA gathers input from airport operators and TSOs to ensure the equipment is functioning effectively in an operational environment. Additional outreach for feedback and input will be implemented for the FSD and their staff as appropriate.

General Conclusion

To protect the security of the traveling public, TSA must be flexible and able to adapt quickly to changes in terrorist tactics. This overarching objective is reflected in every research and development (R&D) and technology deployment decision made by the Agency. TSA will continue to strive toward optimizing technological investments based on thorough R&D analysis and risk-management principles, as well as the collaborative testing and evaluation of new technologies.

Recommendation 1: Conduct a complete risk assessment, including threat, vulnerability, and consequence assessments, which would apply to the PSP.

Concur: TSA concurs and has initiated approaches that identify risks at both the strategic and detailed level. At the strategic level, TSA is updating the initial ADRA. Final completion is expected in November 2009 and approval is expected in fourth quarter of calendar year 2009. At a more detailed level, TSA has been developing the RMAT, an agent-

based, high-detail simulation model that can be used to model specific risk scenarios (for example, specific types and sizes of explosives). The RMAT also can be used to model the risk-reduction potential (across the portfolio of risks) of specific technologies or other countermeasures (for example, a specific piece of equipment deployed in a given percentage of locations). The RMAT tool will be used to generate reports that apply specifically to the passenger screening process and will allow PSP to perform analysis at a level not previously available while not disrupting real world checkpoint operations.

Recommendation 2: Develop cost–benefit analyses to assist in prioritizing investments in new checkpoint screening technologies.

Concur: TSA concurs and is incorporating an approach that combines those risks identified in the RMAT tool with detailed Life Cycle Cost Estimates (LCCEs) to make an informed decision on screening technologies that balances levels of risk (based on current threats) with cost-effective procurement projections of available technologies. In addition, as multiple technologies are implemented and overlapped at the checkpoint, the RMAT scenario can be revisited to model the possible effect of the new systems.

Recommendation 3: Develop quantifiable performance measures to assess the extent to which investments in research, development, and deployment of checkpoint screening technologies achieve performance goals for enhancing security at airport passenger checkpoints.

Concur: TSA understands the importance of developing quantifiable performance measures to ensure that investments support goals and enhance security at the checkpoint. TSA already collects quantifiable performance attributes for all potential acquisitions with regard to metrics, such as detection, false alarm rate, and operational availability. These attributes serve as the baseline against which new technology submissions are evaluated and tested. TSA will work to compare and integrate technology performance measures with those included in the PART and to determine what measures improve checkpoint security when overlapped with multiple systems.

Recommendation 4: After conducting a complete risk assessment and completing cost–benefit analyses and quantifiable performance measures for the PSP, incorporate the results of these efforts into the PSP strategy as determined appropriate.

Concur: TSA concurs and will, upon availability, combine results from the RMAT with LCCEs for possible technology solutions that strike a balance between both risk and efficient use of funding. TSA believes that the RMAT process provides highly valuable insights into capability and risk priorities. However, because of the fundamental uncertainty associated with a dynamic terrorist risk, RMAT and the use of proxy measures cannot be assumed to represent risk reduction measures and will instead be used to provide proxy measures and general "what-if" analysis and risk insight. The projected performance of these technologies will be compared against the long term performance metrics for PSP as established by the most recent PART (2008) in order to ensure linkage between goals and technology implementations.

Recommendation 5: To the extent feasible, ensure that operational tests and evaluations have been successfully completed before deploying checkpoint screening technologies to airport checkpoints.

Concur: TSA has prepared a Test and Evaluation Master Plan (TEMP) for the PSP program and is implementing a formal testing process specified in the TEMP, consistent with DHS's new Acquisition Directive 102. The TEMP establishes a framework for incorporating phased-oriented test and evaluation activities that facilitate the acquisition process. All PSP technology projects follow this testing process, which includes, at a minimum, QT&E conducted by the TSL and OT&E conducted by TSA. OT&E tests the product in an airport setting to validate its operational suitability. TSA has established a robust T&E paradigm to ensure that candidate security technology systems are evaluated for operational effectiveness and suitability prior to deployment.

Recommendation 6: Evaluate whether TSA's passenger screening procedures should be revised to require use of appropriate screening procedures such as pat downs where emerging technologies, including the ETPs and whole body imagers, are currently being used at airports, until it is determined that the machines can meet all of their explosives detection requirements in an operational environment.

Concur: TSA was informed by the TSL that all Atlantic-1 requirements for the ETP were met prior to the pilot testing of machines in the field. The use of the ETP at the checkpoint does not prevent nor prohibit the TSO from exercising judgment and performing additional screening procedures, such as a pat-down, when they feel that it is warranted. In addition, as per current SOP guidance, a pat-down is required for ETP alarm resolution. TSA will complete a review of the explosives trace portals to determine if they are cost-effective and operationally feasible to continue using in airports. For WBI, the TSL IT&E has conducted a series of laboratory tests evaluating the performance of whole body imagers. IT&E performed more than five lab assessment quality test series of WBIs (with various devices and/or operational procedures) starting in February 2007 and continuing to present. These tests have compared TSO performance while using WBI devices to that of a manual pat-down process. Also, in the event of a WBI alarm, current SOPs require a minimum of a pat-down. All results indicate the WBI technology is an effective alternative to the pat-down process.

Recommendation 7: Evaluate all future checkpoint screening technologies prior to testing or using them at airports to determine whether appropriate passenger screening procedures, such as pat downs, should remain in place until the performance of the technologies has been validated through operational test and evaluation.

Concur: TSA will continue to follow its formal test and evaluation process to ensure all checkpoint screening technologies are operationally effective prior to testing or using them in airport settings.

Recommendation 8: Evaluate the benefits, such as the explosives detection effectiveness and deterrent effect, of the ETPs that are being used in airports, and compare the benefits to the costs to operate and maintain this technology to determine whether it is cost-effective to continue to use the machines in airports.

Concur: TSA has already implemented this recommendation through a current and ongoing process of evaluation for the ETP that includes periodic Program Management Reviews (PMRs) with the vendor during which cost-related items are discussed. The detection effectiveness of the ETP has been established in multiple lab tests, but TSA does not feel that deterrence is a measurable quality. TSA has already begun making progress implementing GAO's recommendations. This progress demonstrates our commitment to continual improvement to ensure the security of the traveling public.

Thank you for the opportunity to provide comments to the draft report.

Sincerely yours,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen M. Lord, (202) 512-8777 or LordS@gao.gov

Staff Acknowledgments

In addition to the contact named above, Robert Goldenkoff, Acting Director; E. Anne Laffoon and Steve Morris, Assistant Directors; and Joseph E. Dewechter, Analyst-in-Charge, managed this assignment. Carissa Bryant, Chase Cook, Orlando Copeland, Neil Feldman, and Ryan MacMaster made significant contributions to the work. Charles Bausell, Jr., Richard Hung, and Stanley Kostyla assisted with design, methodology, and data analysis. Michele Mackin assisted with acquisition and contracting issues. Sally Williamson, Linda Miller, and Kathryn Godfrey provided assistance in report preparation, and Thomas Lombardi provided legal support.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper

Radiation Safety Engineering Assessment Report for the Rapiscan Secure 1000 in Single Pose Configuration

VERSION 1.0

NSTD-09-1085

October 2009

Prepared for:

U.S. Department of Homeland Security
Transportation Security Administration
Office of Security Technology
701 South 12th Street
Arlington, VA 22202

Prepared by:

The Johns Hopkins University
Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099

Please note:
This document is disseminated in the interest of information exchange. The Johns Hopkins University Applied Physics Laboratory (JHU/APL) assumes no liability for its contents or use thereof. This plan does not constitute a standard, specification, or regulation. JHU/APL does not endorse products or manufacturers. Trade and manufacturer's names appear in this report only because they are considered essential to the object of this document.

Please send comments to:
Mr. David S. Bogdan
Program Manager
JHU/APL
11100 Johns Hopkins Road
Laurel, MD 20723-6099
Phone: 240-228-4762
E-mail: David.Bogdan@jhuapl.edu

Authors:
The following JHU/APL staff authored this document:

D. Bisson
L. Cosentino
E. Hooks
P. Karnik

Radiation Safety Engineering Assessment Report for the Rapiscan Secure 1000 in Single Pose Configuration

Executive Summary

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) is providing technical support to the United States (U.S.) Department of Homeland Security (DHS) Transportation Security Administration (TSA) in evaluating X-ray systems used for screening vehicles and personnel. TSA directed JHU/APL to conduct an independent radiation safety engineering assessment of the Rapiscan Secure 1000 in Single Pose Configuration. The objectives of the assessment were to measure, verify, and report the parameters of system performance against TSA requirements, ANSI/HPS N43.17-2002, ANSI/HPS N43.17- 2009, and C.F.R. Title 21 Chapter I Subchapter J Part 1002 Records and Reports. When the radiation safety engineering assessment was conducted in July 2009, the ANSI/HPS N43.17-2002 standard was in effect, but the revised standard ANSI/HPS N43.17-2009 was voted on and approved by the ANSI/HPS N43.17 Standards Subcommittee and awaiting formal approval and publication by ANSI. For completeness, this report presents findings of the assessment against both ANSI/HPS N43.17-2002 and ANSI/HPS N43.17-2009 in relevant areas. Dose to scanned individuals and Negligible Individual Dose (NID) for the two standards reported in this document differ due to the methods of calculation required by each standard.

The Rapiscan Secure 1000 in Single Pose Configuration is a two-sided X-ray backscatter Whole Body Imager that can be used to detect objects concealed under a person's clothing. The single pose configuration consists of two Rapiscan Secure 1000 units (master and slave) placed facing each other that are controlled and operated through a common operator's console. The single pose configuration is achieved by the master unit scanning the front view and the slave unit scanning the back view of the subject instead of requiring the subject to pose twice for a front and back scan. To be scanned, the subject enters the inspection aisle of the Secure 1000 in Single Pose Configuration, faces the master unit and stands still. The subject's front and back sides are then scanned sequentially by the master and slave units in an automated manner with just one pose.

The radiation safety engineering assessment of the Rapiscan Secure 1000 in Single Pose Configuration included a review of prior third party radiation testing and detailed radiation safety testing conducted at Rapiscan's facility in Torrance, California from July 27 – 29, 2009. The results of the assessment are as follows:

- The system provided for radiation safety evaluation was an engineering unit built by the Rapiscan engineering team using components from their inventory and configured to be at the same version level and functionally equivalent to the system evaluated at the Transportation Security Laboratory (TSL).
- Performance differences were noted between the master and slave engineering units that may not appear in production systems that are subject to the quality control (QC) process. Where differences were noted the most conservative measurements were used.

- The dose to scanned individuals is within the requirements of ANSI/HPS N43.17-2002, 5.1:
  - Individual effective dose per screening (frontal and rear scan) of a subject is 1.58 μrem (0.0158 μSv), less than the 10 μrem (0.10 μSv) limit.
  - Individual effective dose is below 25 mrem if an individual is subject to fewer than 15,822 screenings in a twelve-month period (equivalent to 43 screenings per day, 365 days per year).
- The dose to scanned individuals is within the requirements of ANSI/HPS N43.17-2009, 6.1.1.1:
  - The average effective per screening (frontal and rear scan) of a subject is 1.48 μrem (0.0148 μSv), less than the 25 μrem (0.25 mSv) per screening limit.
  - Individual effective dose is below 25 mrem if an individual is subject to fewer than 16,891 screenings in a twelve-month period (equivalent to 46 screenings per day, 365 days per year).
- Individual effective dose is below Negligible Individual Dose (NID) (per ANSI/HPS N43.17-2002 5.3 and 2009 B.4) of 1 mrem (0.01 mSv) per year if an individual is subjected to:
  - fewer than 632 screenings in a year (based on 1.58 μrem/screening for N43.17-2002) or
  - fewer than 675 screenings in a year (based on 1.48 μrem /screening for N43.17-2009).
- The aluminum-equivalent total filtration is within the requirements of ANSI/HPS N43.17-2009, 7.1:
  - The X-ray beam is attenuated by approximately 1.18 mm of aluminum-equivalent total filtration for the master unit and 1.63 mm of aluminum-equivalent total filtration for the slave unit, greater than the minimum requirement of no less than 1 mm of aluminum-equivalent total filtration.
- **Additional action is recommended** to ensure that the National Council on Radiation Protection and Measurements (NCRP 1993) general public dose recommendation of less than 100 mrem (0.1 rem) per year is being met (ANSI/HPS N43.17-2002, 5.3 and ANSI/HPS N43.17-2009, B.4). Specifically:
  - An area exists above each of the units, due to primary beam overshoot, where the 100 mrem per year general public dose limit could potentially be exceeded. This area extends up to a height of about 14 ft and 4.6 ft behind each of the units.
  - A second area exists at the entry and exit locations of the scan area, where the 100 mrem per year general public dose limit could potentially be exceeded. This area extends approximately 1.7 ft from the side of the units at the entry and exit locations.

  - It is recommended that a survey of each installation site be conducted to ensure that the dose to any member of the general public is maintained below the 100 mrem (0.1 rem) per year general public limit and to ensure that doses are kept "As Low As Reasonably Achievable" (ALARA).
  - For the area above the units, a beam stop may be considered to ensure the general public dose is maintained.
- The dose to bystanders is within the requirements of ANSI/HPS N43.17-2002, 5.4 and ANSI/HPS N43.17-2009, 6.2:
  - Dose to bystanders is less than 2 mrem in any one hour period, varying from 0.043 to 0.704 mrem at a very conservative 100% duty and 100% occupancy and 0.003 to 0.053 mrem with a 30% duty factor and 25% occupancy factor applied.
- The dose to workers is within the requirements of ANSI/HPS N43.17-2002, 5.4 and ANSI/HPS N43.17-2009, 6.2:
  - Dose to personnel at any Secure 1000 in Single Pose Configuration workstation is below 100 mrem/year (or 50 μrem/hour) when there are fewer than 238 screenings/hour (assuming 50 weeks per year, 40 hours per week, 8 hours per day).
- The system meets the shielding requirements of ANSI/HPS N43.17-2002, 5.5 and ANSI/HPS N43.17-2009, 6.3:
  - Leakage dose rate at 30 cm from any external surface of the master and slave unit are not distinguishable from background exposure.
- The system provides necessary indicators and controls, access panel interlocks, and operational interlocks required by ANSI/HPS N43.17-2002, 6.1, 6.2.1, 6.2.2, ANSI/HPS N43.17-2009, 7.2.1 (a), (b), (c), (d), (e), (i), (l), (m), (n), 7.2.2 (b), (c), and TSA to prevent unauthorized system access, conduct safe operation, and provide an emergency stop capability.
- Depending on the position of the generator, the radiation warning label on the X-ray tube may not be clearly visible. The label may need to be placed in a more visible location. The shielding assembly does not have a warning label as required by ANSI/HPS-N43.17-2002, 6.4 and ANSI/HPS N43.17-2009, 7.3.
- The draft Operator Manual, draft Maintenance Manual, and Specification Sheet provide the information required by ANSI/HPS N43.17-2002, 6.6 and ANSI/HPS N43.17-2009 7.5 (b), (c), (d), (e), and (f) with the exception of technique factors (peak kilovoltage, electrical current, scan time) for each mode and total aluminum equivalent filtration. Final documents should be reviewed when completed and it is recommended that document revisions include information required for technique factors and additional information required by ANSI/HPS N43.17-2009, 7.5 (a), (g), (h), (i), and (j).
- Rapiscan's Site Acceptance Test (SAT) provides functional system tests and a radiation survey that must be completed and approved for system acceptance. Installation procedures were not provided. Since the system evaluated was installed by Rapiscan,

requirements ANSI/HPS N43.17-2002, 7.2 and ANSI/HPS N43.17-2009, 8.1.2 were not evaluated.

- A Radiation Safety Product report filing is required by FDA C.F.R. 21 Subchapter J Part 1002, ANSI/HPS N43.17-2002 4, and ANSI/HPS N43.17-2009 4. The existing Rapiscan FDA filing is for the Secure 1000 system, dated 1992. The Secure 1000 in Single Pose Configuration is configured differently than Secure 1000 from the filing; however there is no filing for the new configuration. The FDA responded to the 1992 filing stating *"...this product is not actively regulated under the device authorities of the Food Drug and Cosmetic Act (FFDCA). The Performance Standard for Diagnostic X-Ray Systems and Their Major Components does not apply to the Secure 1000."*

This Page Intentionally Blank

Radiation Safety Engineering Assessment Report for the Rapiscan Secure 1000 in Single Pose Configuration
Table of Contents

Executive Summary iii

1. Background 1
2. Purpose 1
3. Test Objectives 1
4. Assumptions and Constraints 1
   - 4.1 Assumptions 1
   - 4.2 Constraints 1
   - 4.3 Risks and Risk Mitigation 2
5. System Description 2
6. Instrumentation 6
7. Applicable Standards 6
8. Radiation Safety Engineering Assessment Findings 7
   - 8.1 Configuration of System Evaluated 7
   - 8.2 Assessment of Prior Third Party Radiation Testing 8
   - 8.3 Dose to Scanned Individuals for ANSI/HPS N43.17-2002 9
   - 8.4 Dose to Scanned Individuals for ANSI/HPS N43.17-2009 15
   - 8.5 Negligible Individual Dose 16
   - 8.6 Dose to General Public, Bystanders, and Workers 17
     - 8.6.1 Area Survey 17
     - 8.6.2 Dose to General Public 25
     - 8.6.3 Dose to Bystanders 28
     - 8.6.4 Dose to Workers 30
   - 8.7 Leakage Dose Rate 32
   - 8.8 Physical Safety 33
     - 8.8.1 Indicators and Controls 33
     - 8.8.2 Access Panel Interlocks 37
     - 8.8.3 Operational Interlocks 38
     - 8.8.4 Emergency Stop Capability 40
     - 8.8.5 Automatic Termination 41

8.8.6 Ground Fault 41
8.8.7 Labeling 41
8.8.8 Modifications 43
8.8.9 Information for the End User 43
8.8.10 Records Maintained by Manufacturers 43
8.8.11 Installation Procedures 44
8.8.12 Radiation Surveys 44
8.9 Radiation Safety Product Report 44
9. Conclusions and Recommendations 45
10. References 47
Appendix A. Configuration of the Secure 1000 System in Single Pose Configuration A–1

List of Figures

Figure 5-1. 3-D View of the Secure 1000 in Single Pose Configuration (Reference [4]) 3
Figure 5-2. Top View of the Secure 1000 in Single Pose Configuration (Reference [4]) 4
Figure 5-3. Side View of the Secure 1000 in Single Pose Configuration (Reference [4]) 4
Figure 5-4. Back View of One X-Ray Cabinet of the Secure 1000 in Single Pose Configuration (Reference [4]) 5
Figure 8-1. Secure 1000 in the Single Pose Configuration Torrance, CA 8
Figure 8-2. Ion Chamber Location for Exposure Readings 11
Figure 8-3. Ion Chamber Configuration for HVL Readings 11
Figure 8-4. Filtered Exposure Readings and HVL 13
Figure 8-5. Rapidose kVp Meter Configuration 14
Figure 8-6. Regions for Area Survey 17
Figure 8-7. X-Ray Scattering Source 18
Figure 8-8. X-ray Generator Position During Area Survey 19
Figure 8-9. Ion Chamber at Location 3 and 12 During Area Survey 20
Figure 8-10. Locations of Highest Radiation Readings 25
Figure 8-11. Dose to General Public Above Units 27
Figure 8-12. Dose to General Public at Entry and Exit Locations 28
Figure 8-13. Locations for Dose to Bystander Measurements 30
Figure 8-14. Locations for Dose to Workers Measurements 31
Figure 8-15. Locations for Leakage Dose Measurements 32
Figure 8-16: "Servicing" Mode 33
Figure 8-17: "Screening" Mode 35
Figure 8-18: Scan Button and Status Screen on Unit 35
Figure 8-19: "Ready" for Scan Screen 36
Figure 8-20: Key Switch 36
Figure 8-21: Scan Indicator on Units 37
Figure 8-22: Access Panel Door and Door Interlock 38
Figure 8-23: Emergency Stop Button 40
Figure 8-24: Secure 1000 in Single Pose Configuration Label 42
Figure 8-25: Radiation Warning Label 42

List of Tables

Table 6-1. Instruments 6
Table 8-1. Master Unit HVL Data 12
Table 8-2. Slave Unit HVL Data 12
Table 8-3. Subject Effective Dose per Scan and per Screening 15
Table 8-4. Subject Effective Dose per Scan and per Screening 16
Table 8-5. Master Unit Regions with Highest Radiation Reading 21
Table 8-6. Slave Unit Regions with Highest Radiation Readings 22
Table 8-7. Master Unit Exposure Readings 23
Table 8-8. Slave Unit Exposure Readings 24
Table 8-9. Dose to Bystanders 29
Table 8-10. Dose to Workers 31

1. BACKGROUND

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) is providing technical support to the United States (U.S.) Department of Homeland Security (DHS) Transportation Security Administration (TSA) in evaluating X-ray systems used for screening vehicles and personnel. TSA directed JHU/APL to conduct an independent radiation safety engineering assessment of the Rapiscan Secure 1000 in Single Pose Configuration.

2. PURPOSE

This report summarizes the radiation safety engineering assessment findings for the Secure 1000 in Single Pose Configuration. Test objectives, assumptions and constraints, system description, instrumentation, applicable standards, and radiation safety engineering assessment analysis and findings are provided.

3. TEST OBJECTIVES

The objectives of the radiation safety engineering assessment of the Secure 1000 in Single Pose Configuration were to measure, verify, and report the parameters of system performance against TSA requirements, ANSI/HPS N43.17-2002 (Reference [1]), ANSI/HPS N43.17- 2009 (Reference [2]), and C.F.R. Title 21 Chapter I Subchapter J Part 1002 Records and Reports (Reference [3]).

4. ASSUMPTIONS AND CONSTRAINTS

This section describes key assumptions, constraints, risks and risk mitigations.

4.1 Assumptions

The key assumptions made for this evaluation were that the vendor would provide a complete set of technical details and documentation as requested and that the system would be available in a timely manner. All requested documentation and information was provided to JHU/APL at the California (CA) site. The system was available for three days of testing and Rapiscan engineers were available at all times during the test period to ensure that all testing was completed.

4.2 Constraints

The radiation safety evaluation was conducted at the vendor site using a configuration comprised of two Secure 1000 engineering units dated 2005 and 2007. The Secure 1000 in Single Pose Configuration provided for evaluation was built by the Rapiscan engineering team using components from their inventory and was configured to be at the same version level and functionally equivalent to the system evaluated at the Transportation Security Laboratory (TSL).

The preferred location for testing would have been at JHU/APL using a Secure 1000 in Single Pose Configuration system that passed Rapiscan production and quality control checks to ensure consistency of performance and integrity of the system. However, a spare system was not available to facilitate this.

4.3 Risks and Risk Mitigation

The successful implementation and execution of the radiation safety engineering assessment depended on conditions and events that have inherent risks associated with them. This section describes the identified key risks, planned risk mitigation, and any risk mitigation actions taken.

Risk: The system evaluated may be configured differently than the system deployed to the operational environment.

Planned Risk Mitigation: Through the review of documentation, JHU/APL will verify that the radiation safety evaluation conducted is sufficient to ensure compliance with requirements, standards, and regulations. If needed, additional testing will be conducted.

Mitigation Action: The system evaluated was an engineering system and performance differences were noted between the master and slave units. It is assumed that production units that are subjected to the quality control (QC) process would provide equal performance or better, therefore, the assessment conducted is considered sufficient. However, radiation surveys should be conducted for each installation site as required and it should be verified that the differences in performance observed in the engineering unit are not observed in production units.

Risk: It may not be possible to take measurements due to the system configuration or other physical constraints.

Mitigation: JHU/APL will use the best information available and analytical engineering practices to address the situation.

Mitigation Action: Rapiscan engineers supported the radiation safety testing and provided all necessary configuration changes required to conduct a complete assessment.

5. SYSTEM DESCRIPTION

The Rapiscan Secure 1000 in Single Pose Configuration is a two-sided X-ray backscatter Whole Body Imager that can be used to detect objects concealed under a person's clothing. The single pose configuration consists of two Rapiscan Secure 1000 units (master and slave) placed facing each other that are controlled and operated through a common operator's console. The single pose configuration is achieved by the master unit scanning the front view and the slave unit scanning the back view of the subject instead of requiring the subject to pose twice for a front and back scan. To be scanned, the subject enters the 864 mm (34 in wide) inspection aisle of the Secure 1000 in Single Pose Configuration, faces the master unit, and stands still. The subject's front and back sides are then scanned sequentially by the master and slave units in an automated

manner with just one pose. The master and slave units of the Secure 1000 in Single Pose Configuration are of identical construction and generate an X-ray image by scanning in both the horizontal and the vertical direction, on each side of the system. The vertical scan is achieved by the X-ray generator assembly moving along a 1219 mm (48 in) long lead screw, and the horizontal scan is achieved by the rotation of a chopper wheel at 2400 rpm. According to the vendor, exposure to the subject screened by the Secure 1000 in Single Pose Configuration is less than 10 μrem per scan, and the scan rate for both scans is approximately 6 seconds. After the subject is scanned, the front and back views are displayed on the operator's console on a high-resolution color monitor.

The dimensions (depth, width, and height) of the Secure 1000 in Single Pose Configuration are 2665 mm (105 in) by 2030 mm (80 in) by 1368 mm (54 in). The net weight of the system is 1000 kg (2200 lbs). Figures 5-1, 5-2, and 5-3 show a three-dimensional view, a top view, and a side view of the Secure 1000 in Single Pose Configuration. Figure 5-4 shows a view of the back of one of the X-ray cabinets.

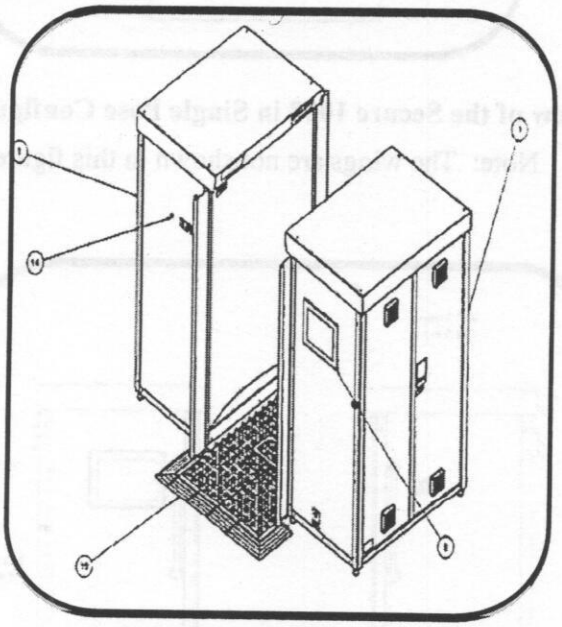


Figure 5-1. 3-D View of the Secure 1000 in Single Pose Configuration (Reference [4])

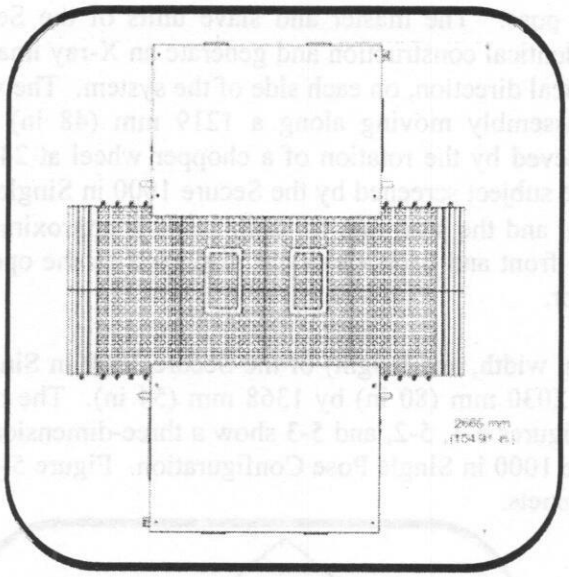


Figure 5-2. Top View of the Secure 1000 in Single Pose Configuration (Reference [4])

Note: The wings are not shown in this figure.

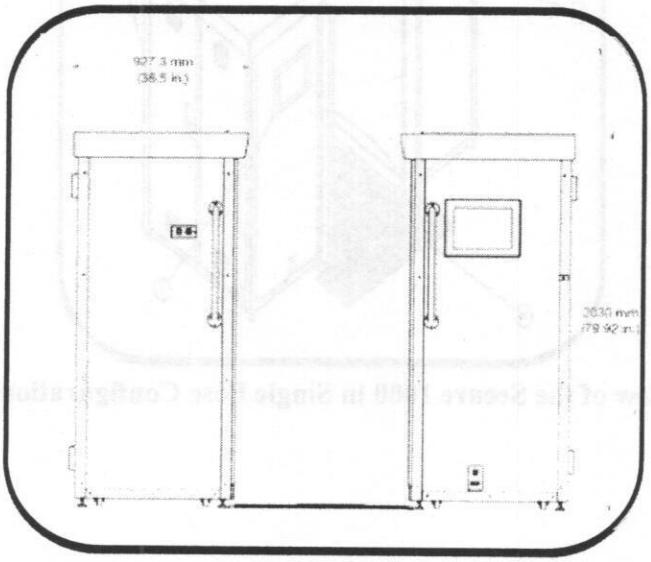


Figure 5-3. Side View of the Secure 1000 in Single Pose Configuration (Reference [4])

Note: The wings are not shown in this figure.

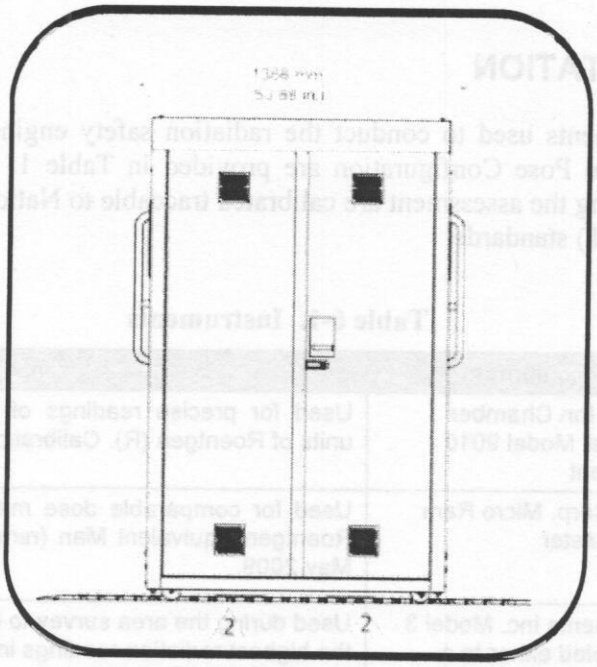


Figure 5-4. Back View of One X-Ray Cabinet of the Secure 1000 in Single Pose Configuration (Reference [4])

Note: The wings are not shown in this figure.

6. INSTRUMENTATION

The radiation instruments used to conduct the radiation safety engineering assessment of the Secure 1000 in Single Pose Configuration are provided in Table 1. All radiation-measuring instruments used during the assessment are calibrated traceable to National Institute of Standards and Technology (NIST) standards.

Table 6-1. Instruments

Instrument/Equipment	Purpose
Radcal Corp 1800 Ion Chamber coupled to a Radcal Model 9010 Controller Instrument	Used for precise readings of radiation exposure in units of Roentgen (R). Calibration date: 7 July 2009.
Thermo Electron Corp. Micro Rem Radiation Survey Meter	Used for comparable dose measurement in units of Roentgen Equivalent Man (rem). Calibration date: 19 May 2009.
Ludlum Measurements Inc. Model 3 Survey Meter coupled either to a Ludlum Model 44-9 Pancake Geiger-Mueller (Pan-GM) Probe or a Ludlum Model 44-3 Thin Crystal Sodium Iodide (NaI) Scintillator Probe	Used during the area survey to identify the area with the highest radiation readings in terms of counts per minute (cpm). Calibration date: 30 June 2009.
Radcal Rapidose (with tripod)	Used for kVp measurement. Calibration date: 24 June 2009.

7. APPLICABLE STANDARDS

The radiation safety engineering assessment was conducted to verify conformance with the ANSI and FDA standards and regulations listed below.

- ANSI/HPS N43.17-2002, American National Standard Radiation Safety for Personnel Screening Systems Using X-rays (Reference [1])
- ANSI/HPS N43.17- 2009 Final for Publication, American National Standard Radiation Safety for Personnel Screening Systems Using X-ray or Gamma Radiation (Reference [2])
- U.S. Food and Drug Administration Title 21, Volume 8, Chapter I Food and Drug Administration Department of Health and Human Services, Subchapter J Radiological Health, Part 1002 Records and Reports (Reference [3])

When the radiation safety engineering assessment was conducted in July 2009, the ANSI/HPS N43.17-2002 standard was in effect, but the revised standard ANSI/HPS N43.17-2009 was voted on and approved by the ANSI/HPS N43.17 Standards Subcommittee and awaiting formal approval and publication by ANSI. For completeness, this report presents findings of the assessment against both ANSI/HPS N43.17-2002 and ANSI/HPS N43.17-2009 in relevant areas.

Dose to scanned individuals and Negligible Individual Dose (NID) for the two standards reported in this document differ due to the methods of calculation required by each standard.

8. RADIATION SAFETY ENGINEERING ASSESSMENT FINDINGS

The radiation safety engineering assessment of the Rapiscan Secure 1000 in Single Pose Configuration included a review of prior third party radiation testing and detailed radiation safety testing conducted at Rapiscan's facility in Torrance, California from July 27 – 29, 2009. The results of the assessment include findings for the following: system configuration, third party radiation testing, dose to scanned individuals, negligible individual dose, dose to general public, dose to bystanders, dose to workers, leakage dose rate, and physical safety. The following sections provide details of the assessment.

8.1 Configuration of System Evaluated

Images of the Secure 1000 in Single Pose Configuration as configured during JHU/APL testing are provided in Figure 8-1. Prior to conducting the testing, Rapiscan provided a configuration list (reference Appendix A for the configuration list) and identified the following differences between the configuration of the Torrance, CA system evaluated by JHU/APL and the systems undergoing qualification testing at the TSL:

- The LCD monitor of the TSL system is older (Rev 2) than the monitor of the CA system (Rev 4).
- The TSL system has a monitor for both sides of the system, where the CA system only has a monitor for the master side of the system.
- The power driver board of the TSL system is older (Rev 1) than the power driver board of the CA System (Rev 2).
- The software of the TSL system is older (version 3.03.01) than the software of the CA system (version 3.03.03). Rapiscan reported that there were no software changes that impact X-ray generation or radiation safety.

JHU/APL conducted an audit of the system configuration at the Torrance, CA test site, additional differences identified were as follows:

- The system provided for radiation safety evaluation was an engineering unit built by the Rapiscan engineering team using components from their inventory and configured to be at the same version level and functionally equivalent to the system evaluated at the TSL.
- Since the CA system is an engineering unit,
  - the components were not subject to the QC process used for production units,
  - the master unit was dated 2007 and the slave unit was dated 2005, and
  - the slave unit X-ray generator tube was of a previous generation.
- At the beginning of radiation safety testing, the X-ray generator in the master unit was replaced due to a damaged high voltage (HV) power supply.
- Performance differences were noted between the master and slave engineering units that may not appear in production systems that are subject to the QC process. Where differences were noted, the most conservative measurements were used.

- Many of the part number labels did not match the part numbers on the configuration list, Rapiscan indicated that they did not maintain the part number labels on the engineering system.
- The engineering system did not implement the emergency stop capability. The slave unit had an emergency stop button, however the button connections were not wired to the system and the button was not operable. The master unit did not have an emergency stop button.

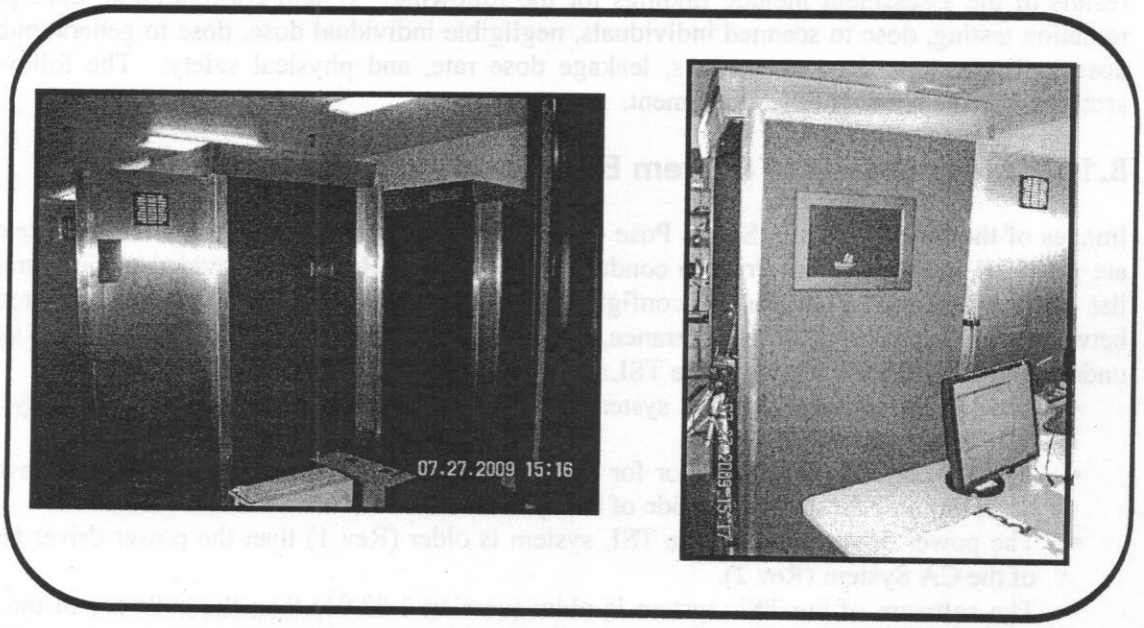


Figure 8-1. Secure 1000 in the Single Pose Configuration Torrance, CA

8.2 Assessment of Prior Third Party Radiation Testing

Medical and Health Physics Consulting (Donald V. Farley, M.S., D.A.B.M.P.) conducted radiation assessments to verify that the system was in compliance with requirements stated in ANSI/HPS N43.17-2002; 5.1, 5.4, and 5.5. The reports for these assessments are dated March 21, 2006 (Reference [5]), June 5, 2008 (Reference [6]), and October 28, 2008 (Reference [7]). An additional assessment was conducted by National Institute of Standards and Technology (NIST) with report dated July 9, 2008 (Reference [8]). Findings from the review of the above reports are as follows:

- The Medical and Health Physics Consulting assessment was conducted for compliance with ANSI/HPS N43.17-2002 5.1 Subject Dose Limitation, 5.4 Dose to Bystanders and 5.5 Shielding. Although the reports indicate compliance with sections 5.1, 5.4 and 5.5, the following points should be considered:
  - The reports do not indicate that an X-ray scattering source was used to determine dose to bystanders.

- A complete area survey was not conducted with the new configuration of two units facing each other to determine exposure to bystanders and operators.
- A complete radiation leakage survey at 30 cm from all surfaces was not conducted with the new configuration of two units facing each other.
- Readings were taken with one active X-ray unit. The second X-ray unit was deactivated. Exposure from both active units should be measured and reported.
- The evaluation does not assess compliance with other ANSI/HPS N43.17 requirements such as indicators, controls, keys and safety interlocks.

- The NIST report provides an assessment based on a review of the Medical and Health Physics Consulting report dated June 5, 2008 and indicates that the Rapiscan Dual Secure 1000 conforms to dose limitation requirements of ANSI/HPS N43.17-2002. The following observations were highlighted in the report:
  - Noted that the second X-ray unit was deactivated.
  - Noted that no data was received regarding radiation scattered from the screened individuals into adjacent areas.
  - Noted that based on the size of the ion chamber used by Medical and Health Physics Consulting, it is uncertain whether the shield intercepted the entire beam.
  - Recommended that "Exposure measurements should be made at the back of each unit while the opposite unit is scanning to verify proper shielding of the primary beam". Medical and Health Physics Consulting took measurements on the back of one inactive unit in a follow up report.
  - Noted that there was a design change to the curvature of the front panel of the Secure 1000 since the Medical and Health Physics Consulting test.

8.3 Dose to Scanned Individuals for ANSI/HPS N43.17-2002

Standard:

- The effective dose shall not exceed 10 μrem (0.10 μSv) per scan of the subject's front. (ANSI/HPS N43.17-2002, 5.1 Subject Dose Limitations)
- The facility shall be operated to ensure that no individual scanned receives from the facility an effective dose in excess of 25 mrem (0.25 mSv) in any twelve-month period. (ANSI/HPS N43.17-2002, 5.1 Subject Dose Limitations)
- The x-ray beam shall be attenuated by no less than 1 mm of aluminum-equivalent total filtration before exiting the beam exit surface. (ANSI/HPS N43.17-2009, 7.1 Filtration)

Assessment Results:

- The average effective dose per scan for the front of a subject is 1.10 μrem (0.011 μSv).
- The average effective dose per screening (frontal and rear scan) of a subject is 1.58 μrem (0.0158 μSv).
- Individual effective dose is below 25 mrem if individual is subject to less than 15,822 screenings in a twelve-month period which is equivalent to 43 screenings per day (365 days per year).

- The X-ray beam is attenuated by approximately 1.18 mm of aluminum-equivalent total filtration for the master unit and 1.63 mm of aluminum-equivalent total filtration for the slave unit.
- The operating potential of the master and slave unit is 50 kV at 5.0 mA.

To determine subject effective dose, readings were made with one unit at a time to understand the subject dose from a single unit. For these measurements, Rapiscan engineers used a special "servicing mode" to disable one unit and conduct operational scans with the other unit. When used in the operational mode, the Single Pose system X-ray scan is less than 6 seconds in duration (less than 3 seconds for the master unit and less than 3 seconds for the slave unit); therefore 3-second scans for a single unit were used for the measurements. To support the subject effective dose measurement, readings were conducted for half value layer (HVL), kVp, and subject dose at 30 centimeters from the exit panel.

To determine the HVL, the following was conducted for each unit (master and slave):

- Using servicing mode, Rapiscan engineers disabled one unit and configured the other unit for the operational parameters of 50 kV, 5.0 mA, chopper wheel speed 2400 RPM, and operational scans where the X-ray generator travels along the lead screw for a 3-second scan.
- The ion chamber was placed in front of a unit and centered at the location where the X-ray beam passed during a scan, as shown in Figure 8-2. To shield the ion chamber from extraneous radiation within the Rapiscan facility, a piece of lead was placed on top of the chamber and bent to form around the chamber, as seen in Figure 8-3.
- Five 3-second scans with a single unit were conducted with 0 mm Al to determine the unfiltered initial exposure.
- Five 3-second scans with a single unit were conducted with 0.51 mm Al, as shown in Figure 8-3. This was repeated for 1.02 mm Al, 2.04 mm Al, and 3.06 mm Al when the half value of the initial exposure was obtained.

The X-ray beam is attenuated by approximately 1.18 mm of aluminum-equivalent total filtration for the master unit and 1.63 mm of aluminum-equivalent total filtration for the slave unit. Table 8-1 provides the data for the master unit and Table 8-2 provides the data for the slave unit. Figure 8-4 shows the filtered exposure readings and HVL.

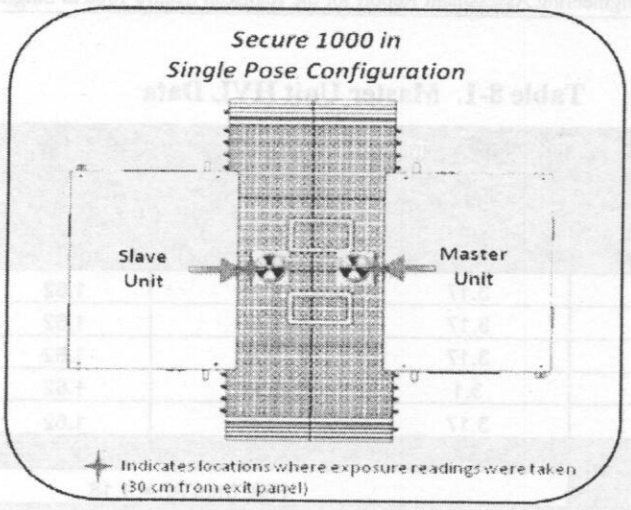


Figure 8-2. Ion Chamber Location for Exposure Readings

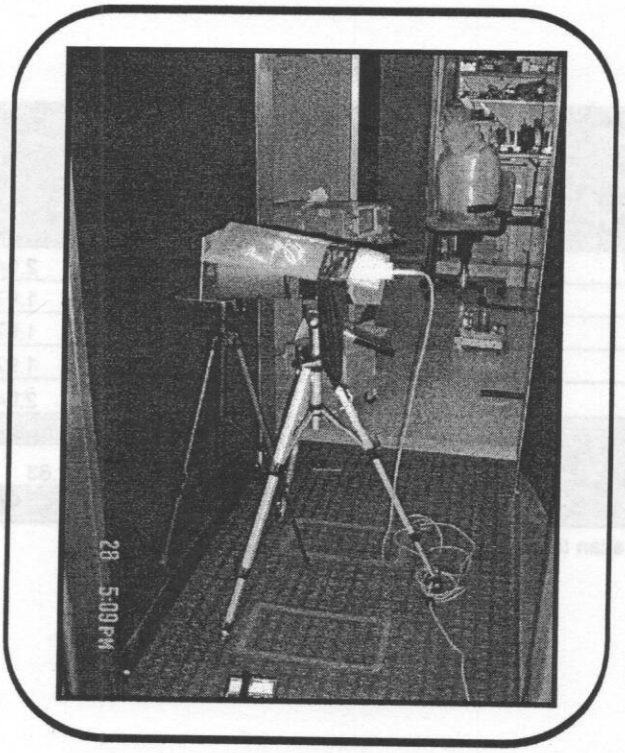


Figure 8-3. Ion Chamber Configuration for HVL Readings

Table 8-1. Master Unit HVL Data

Master Unit					
Scan Number	Exposure Reading for 0 mm Al (μR)[1]	Exposure Reading for 0.51 mm Al (μR)[1]	Exposure Reading for 1.02 mm Al (μR)[1]	Exposure Reading for 2.04 mm Al (μR)[1]	Exposure Reading for 3.06 mm Al (μR)[1]
1	4.58	3.17	2.39	1.62	1.06
2	4.5	3.17	2.46	1.62	1.06
3	4.64	3.17	2.39	1.62	1.06
4	4.57	3.1	2.46	1.62	1.06
5	4.58	3.17	2.46	1.62	1.06
Average	4.574	3.156	2.432	1.62	1.06
Average/2	2.287	HVL (mm Al) = 1.18			
COV	0.011	0.010	0.016	0.000	0.000

1. Master unit scan for total scan time of 3 seconds.

Table 8-2. Slave Unit HVL Data

Slave Unit					
Scan Number	Exposure Reading for 0 mm Al (μR)[1]	Exposure Reading for 0.51 mm Al (μR)[1]	Exposure Reading for 1.02 mm Al (μR)[1]	Exposure Reading for 2.04 mm Al (μR)[1]	Exposure Reading for 3.06 mm Al (μR)[1]
1	4.58	3.45	2.82	2.04	1.48
2	4.64	3.38	2.75	1.97	1.41
3	4.58	3.45	2.82	1.97	1.41
4	4.65	3.38	2.82	1.97	1.41
5	4.58	3.38	2.75	2.04	1.41
Average	4.606	3.408	2.792	1.998	1.424
Average/2	2.303	HVL (mm Al) = 1.63			
COV	0.008	0.011	0.014	0.019	0.022

1. Slave unit scan for total scan time of 3 seconds.

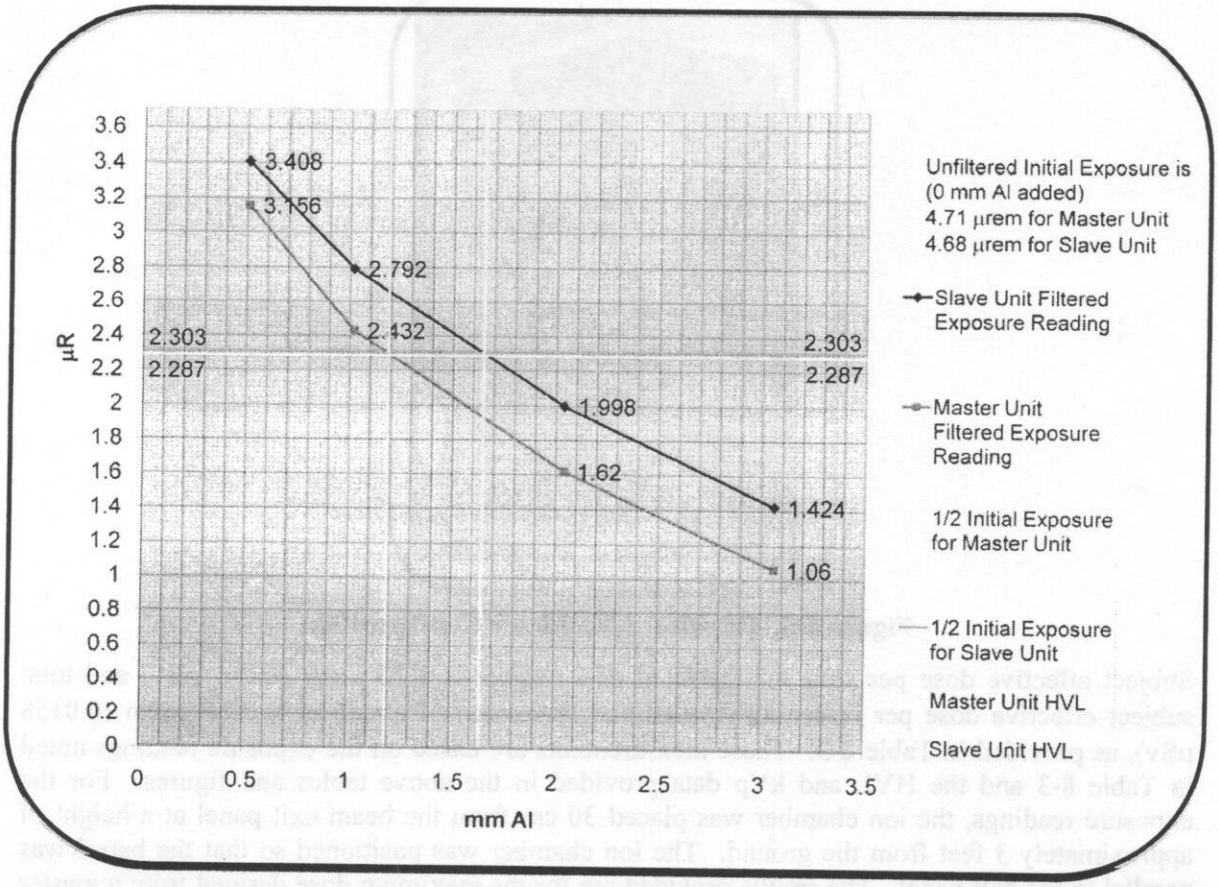


Figure 8-4. Filtered Exposure Readings and HVL

To obtain kVp measurements, the Rapidose kVp meter was placed in front of the X-ray beam as shown in Figure 8-5. Rapiscan engineers used servicing mode to configure the system for 50 kV, 5.0 mA, chopper wheel speed 1200 RPM, and operational 3-second scans. Multiple readings were conducted for both units. Due to the minimum beam hardness (2 mm Al) specified for the Rapidose kVp meter, the measurements of kVp made may not be accurate within +/- 5%. The indicated operating potential on both the master and slave units was 50 kV and the measurements made with the Rapidose (although not verified to required accuracy) indicate that the operating potential of the units does not exceed 50 kV. Therefore, as a conservative measure, the dose conversion coefficients are selected based on 50 kV.

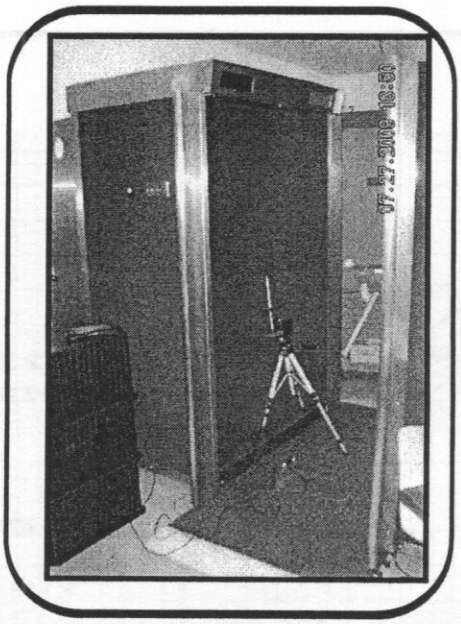


Figure 8-5. Rapidose kVp Meter Configuration

Subject effective dose per scan for the front of a subject is 1.10 μrem (0.011 μSv) and total subject effective dose per screening (frontal and rear scan) of a subject is 1.58 μrem (0.0158 μSv), as provided in Table 8-3. These measurements are based on the exposure readings noted in Table 8-3 and the HVL and kVp data provided in the above tables and figures. For the exposure readings, the ion chamber was placed 30 cm from the beam exit panel at a height of approximately 3 feet from the ground. The ion chamber was positioned so that the barrel was parallel to the exit panel. The results provided are for the maximum dose derived from a master frontal scan at 30 cm from the master beam exit panel and slave rear scan at 30 cm from the slave beam exit panel. Since the distance between these two points in the scan area is approximately 18.4 inches; it is conceivable that a scanned individual could be exposed to a consecutive master and slave scan at these locations.

Dose to scanned individuals for the two standards reported in this document differ due to the methods of calculation required by each standard.

Table 8-3. Subject Effective Dose per Scan and per Screening

	Average Exposure per Scan[3] (μR/scan)[4]	HVL	kVp[5]	Dose Conversion Coefficient[6]	Effective Dose per Scan (μrem/scan)
Master Unit Frontal Scan[1] at 30 cm from Master Unit Beam Exit Panel	4.77	1.18 mm Al	50	Front 0.23	1.1
Slave Unit Rear Scan[2] at 30 cm from Slave Unit Beam Exit Panel	4.8	1.63 mm Al	50	Rear 0.1	0.48

	Average Exposure per Screening[3] (μR/screening)[4]				Effective Dose per Screening (μrem/screening)
Master + Slave Unit (Frontal + Rear Scan)	9.57				1.58

1. Master unit scan for total scan time of approximately 3 seconds. Data for scans is as follows: Scan 1 – 4.72 μR, Scan 2 – 4.65 μR, Scan 3 – 4.65 μR, Scan 4 – 4.72 μR, Scan 5 – 4.65 μR.
2. Slave unit scan for total scan time of approximately 3 seconds. Data for scans is as follows: Scan 1 – 4.65 μR, Scan 2 – 4.8 μR, Scan 3 – 4.65 μR, Scan 4 – 4.73 μR, Scan 5 – 4.72 μR.
3. Background exposure 0.0006 μR subtracted and energy correction factor 1.02 applied.
4. Results provided above are for the maximum dose derived from a master frontal scan and slave rear scan.
5. Due to the minimum beam hardness (2 mm Al) specified for the Rapidose kVp meter, the measurements of kVp made may not be accurate within +/- 5%. The indicated operating potential on both the master and slave units was 50 kV and the measurements made with the Rapidose (although not verified to required accuracy) indicate that the operating potential of the units does not exceed 50 kV. Therefore, as a conservative measure, the dose conversion coefficients are selected based on 50 kV.
6. ANSI/HPS N43.17-2002 Dose Conversion Coefficient for frontal and rear exposures.

8.4 Dose to Scanned Individuals for ANSI/HPS N43.17-2009

Standard: The reference effective dose shall not exceed 25 μrem (0.25 mSv) per screening. The reference effective dose received by individuals from one facility shall not exceed 25 mrem (250 mSv) over a twelve month period. (ANSI/HPS N43.17-2009, 6.1.1.1)

Assessment Results:

- The average effective dose per screening (frontal and rear scan) of a subject is 1.48 μrem (0.0148 μSv).
- Individual effective dose is below 25 mrem if an individual is subject to fewer than 16,891 screenings in a twelve-month period which is equivalent to 46 screenings per day (365 days per year).

Based on the data collected for dose to individual ANSI/HPS N43.17-2002 measurements as described in Section 8.3, dose to individual for ANSI/HPS N43.17-2009 was determined. The average effective dose per screening (frontal and rear scan) of a subject is 1.48 μrem (0.0148 μSv), as provided in Table 8-4. These measurements are based on the exposure readings and HVL data provided in Table 8-1, Table 8-2, Table 8-3, and Figure 8-4. The results provided are for the maximum dose derived from a master frontal scan at 30 cm from the master beam exit panel and slave rear scan at 30 cm from the slave beam exit panel. Since the distance between

these two points in the scan area is approximately 18.4 inches, it is conceivable that a scanned individual could be exposed to a consecutive master and slave scan at these locations.

Dose to scanned individuals for the two standards reported in this document differ due to the methods of calculation required by each standard.

Table 8-4. Subject Effective Dose per Scan and per Screening

	Average Exposure per Scan[3] (μR/scan)[4]	HVL	Dose Conversion Coeffiecient[5]	Effective Dose per Scan (μrem/scan)
Master Unit Scan[1] at 30 cm from Master Beam Exit Panel	4.77	1.18 mm Al	0.1298	0.62
Slave Unit Scan[2] at 30 cm from Master Beam Exit Panel	4.80	1.63 mm Al	0.1793	0.86

	Average Exposure per Screening[3] (μR/screening)[4]			Effective Dose per Screening (μrem/screening)
Master + Slave Unit (Frontal + Rear Scan)	9.57			1.48

1. Master unit scan at location 30 cm from master beam exit panel for total scan time of approximately 3 seconds.
2. Slave unit scan at location 30 cm from beam exit panel for total scan time of approximately 3 seconds.
3. Background exposure subtracted and energy correction factor of 1.02 applied.
4. Results provided above are for the maximum dose derived from a master frontal scan and slave rear scan.
5. ANSI/HPS N43.17-2009 Dose Conversion Coefficient for master unit is 0.1298 (0.110 * 1.18) and slave unit is 0.1793 (0.110 * 1.63).

8.5 Negligible Individual Dose

Standard: Negligible Individual Dose (NID) is set at 1 mrem (0.01 mSv) per year. At radiation exposures below the NID, efforts to reduce the dose further are not warranted. When the number of subject examinations results in exposures above NID, reasonable efforts should be made to reduce the number of scans, taking into account the nature of the application. (ANSI/HPS N43.17-2002, 5.3 Dose minimization and negligible individual dose and ANSI/HPS N43.17-2009, B.4 Dose minimization and negligible individual dose)

Assessment Results:

- Based on 1.58 μrem/screening for frontal and rear scans (per ANSI/HPS N43.17-2002, reference Section 8.3 of this report), individual dose is below NID if the individual is subjected to less than 632 screenings in a year.
- Based on 1.48 μrem /screening (per ANSI/HPS N43.17-2009, reference Section 8.4 of this report), individual dose is below NID if the individual is subjected to less than 675 screenings in a year.

NID for the two standards reported in this document differ due to the methods of calculation required for dose to individuals by each standard.

8.6 Dose to General Public, Bystanders, and Workers

A survey of the areas surrounding the master and slave unit of the system was conducted to determine the dose to general public, bystanders, and workers. This section provides a description of how the area survey was conducted, area survey data collected, and an explanation of calculations performed to determine dose to general public, bystanders and workers.

8.6.1 Area Survey

To conduct the survey the areas surrounding the master and slave units were designated by regions (A to B, B to C, C to D, D to E, E to F, F to G, G to H, H to A, A to D, H to E), as shown in Figure 8-6. An X-ray scattering source, four 5-gallon water-filled containers holding approximately 150 pounds of water, were placed in stacked bins at the center position between the two units, as shown in Figure 8-7. The system was placed in a special configuration to conduct the area survey.

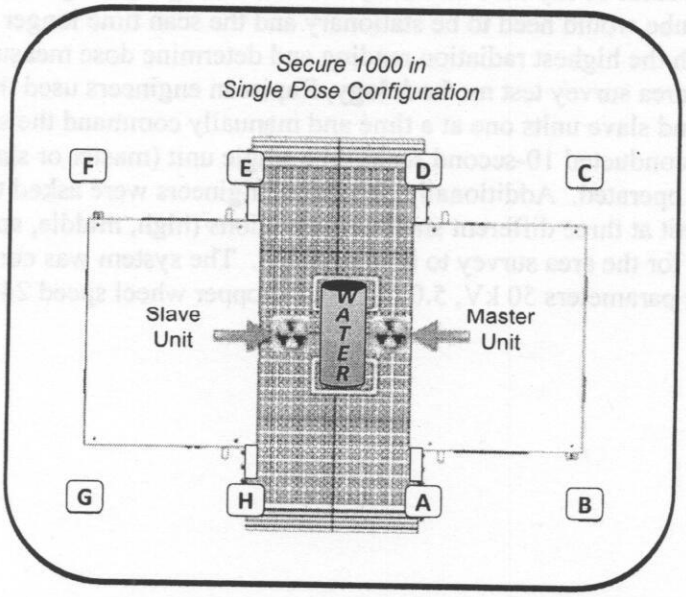
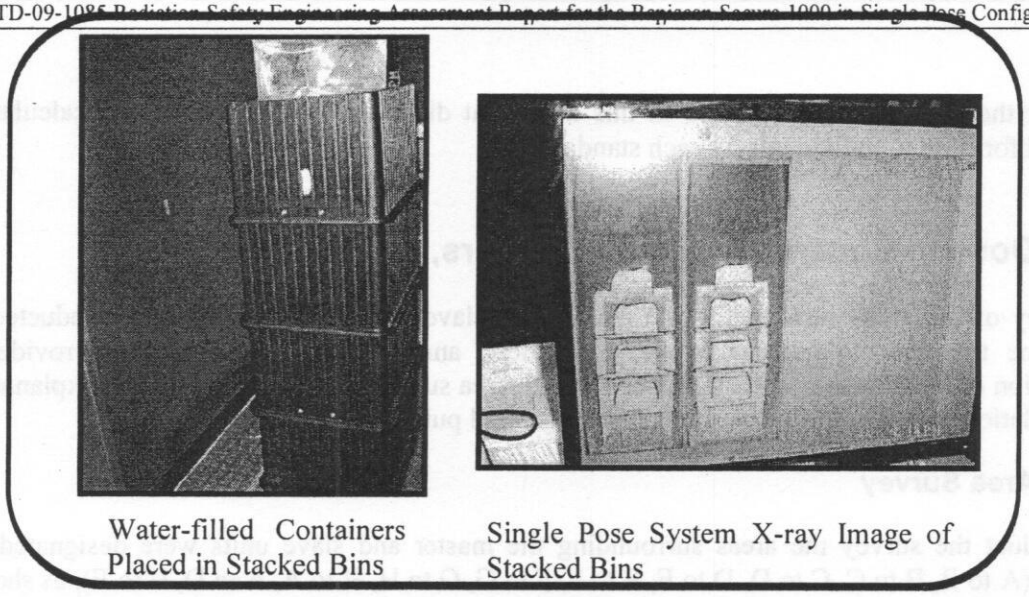


Figure 8-6. Regions for Area Survey



Water-filled Containers Placed in Stacked Bins

Single Pose System X-ray Image of Stacked Bins

Figure 8-7. X-Ray Scattering Source

When used in the operational mode, the Single Pose system X-ray scan is less than 6 seconds in duration (less than 3 seconds for the master unit and less than 3 seconds for the slave unit). It was determined that since X-ray tube assembly travelled along the long lead screw in less than 3 seconds, the X-ray tube would need to be stationary and the scan time longer in order to identify the area with the highest radiation reading and determine dose measurements. To facilitate JHU/APL area survey test methodology, Rapiscan engineers used the servicing mode to operate the master and slave units one at a time and manually command the system to scan. Rapiscan engineers conducted 10-second scans on a single unit (master or slave) while the second unit was not operated. Additionally, Rapiscan engineers were asked to place the X-ray generator on each unit at three different stationary positions (high, middle, and low as shown in Figure 8-8) in order for the area survey to be conducted. The system was configured for maximum operating parameters 50 kV, 5.0 mA, and chopper wheel speed 2400 rpm.

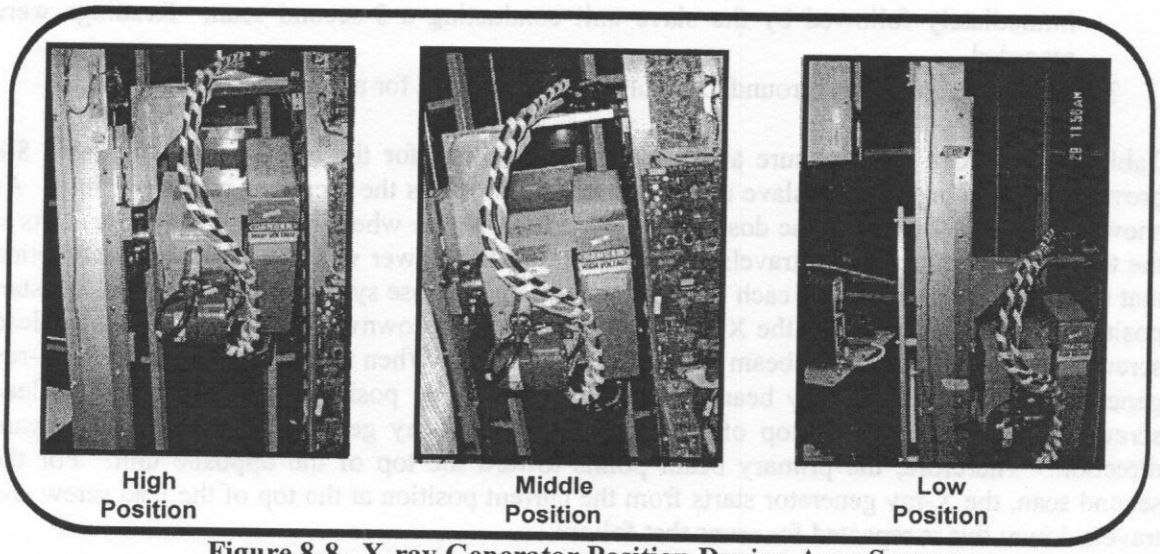


Figure 8-8. X-ray Generator Position During Area Survey

Each region surrounding the master unit (A to B, B to C, C to D, H to A, D to E, H to E (above the slave unit)) was surveyed followed by each region surrounding the slave unit (E to F, F to G, G to H, H to A, D to E, A to D (above the master unit)). The following steps were conducted for each region surveyed:

1. The X-ray tube was placed in a stationary position at a height 59 inches from the ground.
2. During multiple 10-second scans, the region was surveyed using the Ludlum Measurements Inc. Model 3 Survey Meter. Scans were repeated until the area with highest radiation reading was identified.
3. At this location, the counts per minute (cpm) reading from the Ludlum was recorded. An additional reading using the plastic scintillator was recorded to get a dose measurement (rem).
4. Steps 1-3 were repeated with the X-ray tube placed in a stationary position at height of 39 inches from the ground.
5. Steps 1-3 were repeated with the X-ray tube placed in a stationary position at height of 19 inches from the ground.

Table 8-5 provides the highest radiation reading data for the areas surrounding the master unit. Table 8-6 provides the highest radiation reading data for the areas surrounding the slave unit. Using the data from these tables, the location with the highest radiation reading in each region was identified and at that location precise readings of the radiation exposure (R) were made using the 1800 cc ion chamber. Figure 8-9 shows the ion chamber positioned at location 3 and 12. The following steps were conducted for the location of highest radiation reading in each region:

1. The 1800 cc ion chamber was placed at the location with the highest radiation reading.
2. Five scans were conducted with the system operating under maximum operating parameters using operational 6-second scans (note that the system was used in the standard operational scan mode), where the master unit conducts a 3-second scan and is

immediately followed by the slave unit conducting a 3-second scan. Readings were recorded.

3. Five readings of background exposure were conducted for a 6-second time period.

Table 8-7 provides the exposure and background readings for the master unit and Table 8-8 provides the readings for the slave unit. Figure 8-10 provides the locations of the readings. As shown in Table 8-7 and 8-8, the dose above the units is higher when the X-ray generator starts at the top of the lead screw and travels down because of the slower velocity of the vertical motion that occurs at the beginning of each scan. When the Single Pose system executes a scan, the start position (for the first scan) of the X-ray generator is angled downward at the bottom of the lead screw and therefore the X-ray beam is pointed to the floor. When the scan is initiated, the X-ray generator (and therefore x-ray beam) moves to a horizontal position as it moves up the lead screw and as it reaches the top of the lead screw the X-ray generator angles to an upward direction. Therefore, the primary beam points toward the top of the opposite unit. For the second scan, the X-ray generator starts from the current position at the top of the lead screw and travels down; this is repeated for scans that follow.

The scan has two phases that are monitored by the system, the "Bypass Phase" and "Main Phase". The "Bypass Phase" occurs during the first 0.5 seconds of the scan when the X-ray generator is energized and vertical motion starts. During this phase vertical motion and X-ray generator output are not monitored because as they are out of tolerance. The remaining 2.5 seconds are the "Main Phase", system monitoring transitions to this phase when vertical motion has reached the point where 30 lines of data have been acquired. At this time it is assumed that vertical motion and X-ray generation are stable and these parameters are monitored. Therefore, there is approximately 0.5 seconds at the beginning of each scan where vertical motion has not reached peak velocity and may result in slightly higher doses at the position where the scan starts.

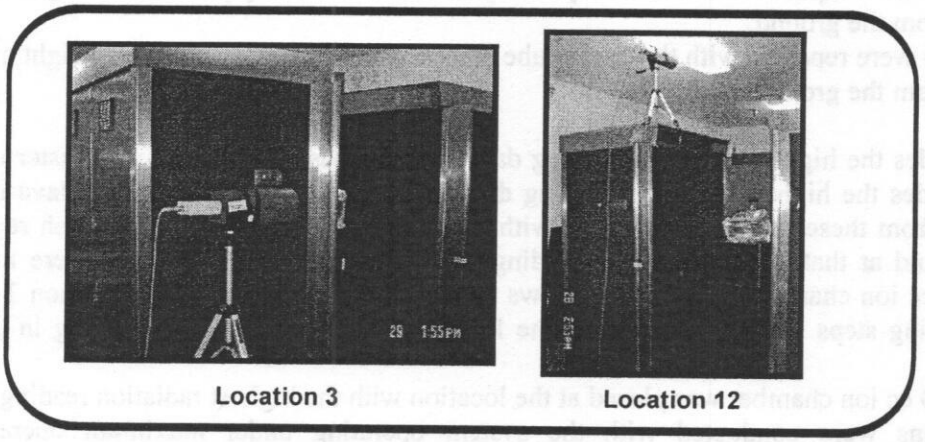


Figure 8-9. Ion Chamber at Location 3 and 12 During Area Survey

Table 8-5. Master Unit Regions with Highest Radiation Reading

Master Unit					
Region	X-ray Tube Height from Ground (Inches)	Radiation Instrument Height from Ground (Inches)	Radiation Instrument Distance from Left Side of Unit (Inches)	Ludlum Survey Meter with 44-3 (cpm)	Plastic Scintillator (µrem/hr)
A to B	59	59	4.5	5,000	40
	39	42	17.5	10,000	Not Distinguishable[2]
	19	26.5	10	11,000	Not Distinguishable[2]
B to C	59	50.5	26	400,000	70
	39	36.5	26.5	250,000	40
	19	39	27	Over Range[1]	130
C to D	59	54.5	15	110,000	30
	39	37.5	15.5	100,000	18
	19	26	19.5	40,000	15
D to E	59	48.5	17	120,000	15
	39	41.5	At Wing	300,000	20
	19	13	9	50,000	15
H to A	59	71	17	3,000	11
	39	43	At Wing	500,000	30
	19	14	29 in. from Location H	50,000	10
H to E (On Top of Slave Unit)	59	108	24 in. from Left Side, 13 in. from Front of Unit	Over Range[1]	5
	39	108	24 in. from Left Side, 13 in. from Front of Unit	Not Distinguishable[2]	N/R[3]
	19	108	24 in. from Left Side, 13 in. from Front of Unit	Not Distinguishable[2]	N/R[3]
A to D (On Top of Master Unit)	59	108.5	24 in. from Left Side, 13 in. from Front of Unit	20,000	< 10
	39	108.5	24 in. from Left Side, 13 in. from Front of Unit	Not Distinguishable[2]	N/R[3]
	19	108.5	24 in. from Left Side, 13 in. from Front of Unit	N/R[3]	N/R[3]

Note 1: Ludlum Survey Meter range is limited to 600,000 cpm.

Note 2: Reading taken during X-ray scan was not distinguishable from background reading.

Note 3: No readings were taken (N/R). Maximum readings found to be at the 59 inch X-ray tube height. Due to the time constraints, precise readings at other heights were not taken.

Table 8-6. Slave Unit Regions with Highest Radiation Readings

Slave Unit					
Region	X-ray Tube Height from Ground (Inches)	Radiation Instrument Height from Ground (Inches)	Radiation Instrument Distance from Left Side of Unit (Inches)	Ludlum Survey Meter with 44-3 (cpm)	Plastic Scintillator (µrem/hr)
D to E	59	72	At Wing	40, 000	10
	39	47	At Wing	590,000	70
	19	22	11.5	41,000	Not Distinguishable[2]
E to F	59	58	5	40, 000	14
	39	30.5	10.5	52,000	20
	19	26	8.5	110,000	10
F to G	59	52	24	Over Range[1]	1,800
	39	39	21.5	Over Range[1]	6,000
	19	28.5	26	Over Range[1]	6,000
G to H	59	63	45.5	110,000	16
	39	42	18.5	110,000	22
	19	14.5	5.5	220,000	30
H to A	59	71	At Wing	42,000	18
	39	46	At Wing	520,000	60
	19	17	5	42,000	Not Distinguishable[2]
A to D (Top of Master Unit)	59	108.5	24 in. from Left Side, 12 in. from Front of Unit	Over Range[1]	6,000
	39	108.5	24 in. from Left Side, 12 in. from Front of Unit	Not Distinguishable[2]	N/R[3]
	19	N/R[3]	N/R[3]	N/R[3]	N/R[3]
H to E (Top of Slave Unit)	59	108	24 in. from Left Side, 12 in. from Front of Unit	Not Distinguishable[2]	N/R[3]
	39	N/R[3]	N/R[3]	N/R[3]	N/R[3]
	19	N/R[3]	N/R[3]	N/R[3]	N/R[3]

Note 1: Ludlum Survey Meter range is limited to 600,000 cpm.

Note 2: Reading taken during X-ray scan was not distinguishable from background reading.

Note 3: No readings were taken (N/R). Maximum readings found to be at the 59 inch X-ray tube height. Due to the time constraints, precise readings at other heights were not taken.

Table 8-7. Master Unit Exposure Readings

Master Unit											
Location Number	Region	Ion Chamber Height from Ground (Inches)	Ion Chamber Distance from Left Side of Unit (Inches)	Ion Chamber Distance from Unit Panel (Inches)	Scan Number	Exposure Reading Ion Chamber (μR/screening[1])	Background Reading Ion Chamber (μR^2)	Average Exposure with Background Subtracted (μR/screening)	Energy Correction Ion Chamber	Average Exposure with Background Subtracted and Energy Correction Applied (μR/screening)
1	A to B	59	4.5	11 8 (30 cm)	1	0 28	0.14			
					2	0 21	0 21			
					3	0 21	0 21			
					4	0 21	0.14			
					5	0 21	0 21			
					Average	0.22	0.18	Exposure reading was not distinguishable from background exposure.		
2	B to C	39	27	11 8 (30 cm)	1	0.14	0.14			
					2	0.14	0 21			
					3	0.14	0.14			
					4	0.14	0.14			
					5	0.14	0.14			
					Average	0.14	0.15	Exposure reading was not distinguishable from background exposure.		
3	C to D	54.5	15	11 8 (30 cm)	1	0 21	0.14			
					2	0.14	0.14			
					3	0 21	0.14			
					4	0 21	0.14			
					5	0.14	0.14			
					Average	0.18	0.14	Exposure reading was not distinguishable from background exposure.		
5	D to E	41.5	At Edge of Wing	N/A	1	0.77	0.14			
					2	0.77	0 21			
					3	0.77	0.14			
					4		0 21			
					5		0 21			
					Average	0.77	0.18	0.59	1.02	0.60
9	H to A	43	At Edge of Wing	N/A	1	0 98	0.14			
					2	0 98	0 21			
					3	1 05	0.14			
					4		0 21			
					5		0 21			
					Average	1.00	0.18	0.82	1.02	0.84
12	H to E (On top of Slave Unit at 99 Inch Height)	99	24	13 from Front of Unit	1	1 34	0 21			
					2	1.41	0 21			
					3	1 34	0 21			
					4	1 34	0.14			
					5	1 34	0 21			
					6	1 34	0 21			
					7	1 34				
					8	1 34				
					9	1 34				
					10	1 34				
					Average	1.35	0.20	1.15	1.02	1.17
12	H to E (On Top of Slave Unit at 105 Inch Height)	105	24	13 from Front of Unit	1	0.70	0 07			
					2	1 55	0 07			
					3	0.70	0.14			
					4	1 55	0.14			
					5	0.70	0.14			
					6	1 55				
					7	0.70				
					8	1.48				
					9	0.70				
					10	1.48				
					Average	1.11	0.11	1.00	1.02	1.02

1. Master unit and slave unit consecutive scans for total scan time of approximately 6 seconds.
2. Background reading conducted for 6-second time period.

Table 8-8. Slave Unit Exposure Readings

Slave Unit										
Location Number	Region	Ion Chamber Height from Ground (Inches)	Ion Chamber Distance from Left Side of Unit (Inches)	Ion Chamber Distance from Unit Panel (Inches)	Scan Number	Exposure Reading Ion Chamber (μR/screening[1])	Background Reading Ion Chamber (mR[2])	Average Exposure with Background Subtracted (μR/screening)	Energy Correction Ion Chamber	Average Exposure with Background Subtracted and Energy Correction Applied (μR/screening)
4	D to E	47	At Wing Edge	N/A	1	0.21	0.14			
					2	0.21	0.14			
					3	0.21	0.07			
					4	0.21	0.21			
					5	0.21	0.14			
					Average	0.21	0.14	0.07	1.02	0.07
6	E to F	30.5	10.5	11.8 (30 cm)	1	0.07	0.07			
					2	0.14	0.07			
					3	0.07	0.07			
					4	0.07	0.07			
					5	0.14	0.07	Exposure reading was not distinguishable from background exposure.		
					Average	0.10	0.07			
7	F to G	52	24	11 8 (30 cm)	1	0.21	0.07			
					2	0.07	0.07			
					3	0.07	0.07			
					4	0.07	0.07			
					5	0.07	0.07	Exposure reading was not distinguishable from background exposure.		
					Average	0.10	0.07			
8	G to H	14.5	5.5	11 8 (30 cm)	1	0.14	0.07			
					2	0.14	0.14			
					3	0.14	0.14			
					4	0.14	0.14			
					5	0.14	0.14	Exposure reading was not distinguishable from background exposure.		
					Average	0.14	0.13			
10	H to A	46	At Wing Edge	N/A	1	0.21	0.07			
					2	0.21	0.14			
					3	0.28	0.14			
					4	0.21	0.14			
					5	0.21	0.14			
					Average	0.22	0.13	0.10	1.02	0.10
11	A to D (On Top of Master Unit at 104.75 Inch Height)	104.75	24	11.5 from Front	1	0.14	0.14			
					2	1.41	0.14			
					3	0.14	0.14			
					4	1.48	0.14			
					5	0.07	0.14			
					6	1.48				
					7	0.14				
					8	1.48				
					9	0.14				
					10	1.48				
					Average	0.80	0.14	0.66	1.02	0.67
11	D to A (On Top of Master Unit at 99.5 Inch Height)	99.5	24	11.5 from Front	1	0.28	0.14			
					2	1.34	0.14			
					3	0.91	0.07			
					4	1.27	0.07			
					5	0.49	0.07			
					6	1.27				
					7	0.35				
					8	1.34				
					9	0.84				
					10	1.27				
					Average	0.94	0.09	0.85	1.02	0.87

1. Master unit and slave unit consecutive scans for total scan time of approximately 6 seconds.
2. Background reading conducted for 6-second time period.

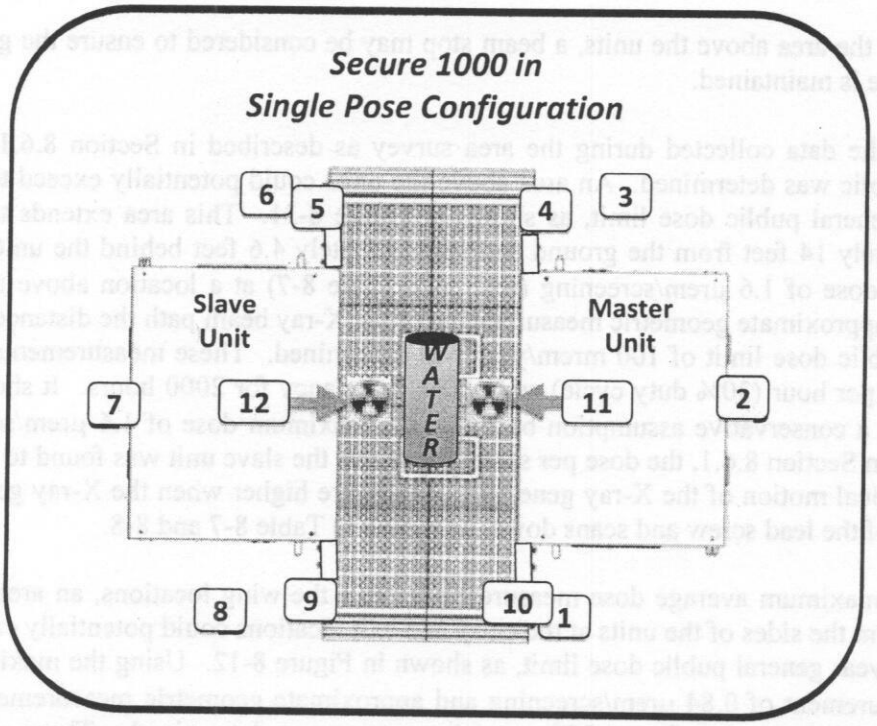


Figure 8-10. Locations of Highest Radiation Readings

8.6.2 Dose to General Public

Standard: NCRP 1993 recommends that members of the general public receive less than 1 mSv (0.1 rem) per year. These levels are subject to the radiation safety principle of ALARA. (ANSI/HPS N43.17-2002, 5.3 Dose minimization and Negligible Individual Dose and ANSI/HPS N43.17-2009, B.4 Dose minimization and Negligible Individual Dose)

Assessment Results:

- An area exists above each of the units, due to primary beam overshoot, where the 100 mrem per year general public dose limit could potentially be exceeded. This area extends up to a height of about 14 ft and 4.6 ft behind each of the units.
- A second area exists at the entry and exit locations of the scan area, where the 100 mrem per year general public dose limit could potentially be exceeded. This area extends approximately 1.7 ft from the side of the units at the entry and exit locations.
- The estimated annual dose and the associated exposed area are based on the maximum exposure readings taken at the time of the survey and from approximate geometric measurements of the X-ray beam path. A more precise measurement of the geometry would provide a better understanding of the area's boundaries, but was not possible due to the location of the system being evaluated.
- It is recommended that a survey of each installation site be conducted to ensure that the dose to any member of the general public is maintained below the 100 mrem (0.1 rem) per year general public limit and to ensure that doses are kept ALARA.

- For the area above the units, a beam stop may be considered to ensure the general public dose is maintained.

Based on the data collected during the area survey as described in Section 8.6.1, dose to the general public was determined. An area above the units could potentially exceed the 100 mrem per year general public dose limit, as shown in Figure 8-11. This area extends to a height of approximately 14 feet from the ground and approximately 4.6 feet behind the units. Using the maximum dose of 1.6 μrem/screening (reference Table 8-7) at a location above the slave unit and using approximate geometric measurements of the X-ray beam path the distance at which the general public dose limit of 100 mrem/year was determined. These measurements assume 180 screenings per hour (30% duty cycle) and 100% occupancy for 2000 hours. It should be noted that this is a conservative assumption based on the maximum dose of 1.6 μrem/screening. As discussed in Section 8.6.1, the dose per screening above the slave unit was found to be dependent on the vertical motion of the X-ray generator. Doses are higher when the X-ray generator starts at the top of the lead screw and scans down, as shown in Table 8-7 and 8-8.

Using the maximum average dose measurements from the wing locations, an area that extends 1.7 feet from the sides of the units at the entry and exit locations could potentially exceed the 100 mrem per year general public dose limit, as shown in Figure 8-12. Using the maximum average dose measurement of 0.84 μrem/screening and approximate geometric measurements of the X-ray beam path, an approximate 100 mrem/year area was determined. These measurements assume 180 screenings per hour (30% duty cycle) and 100% occupancy for 2000 hours.

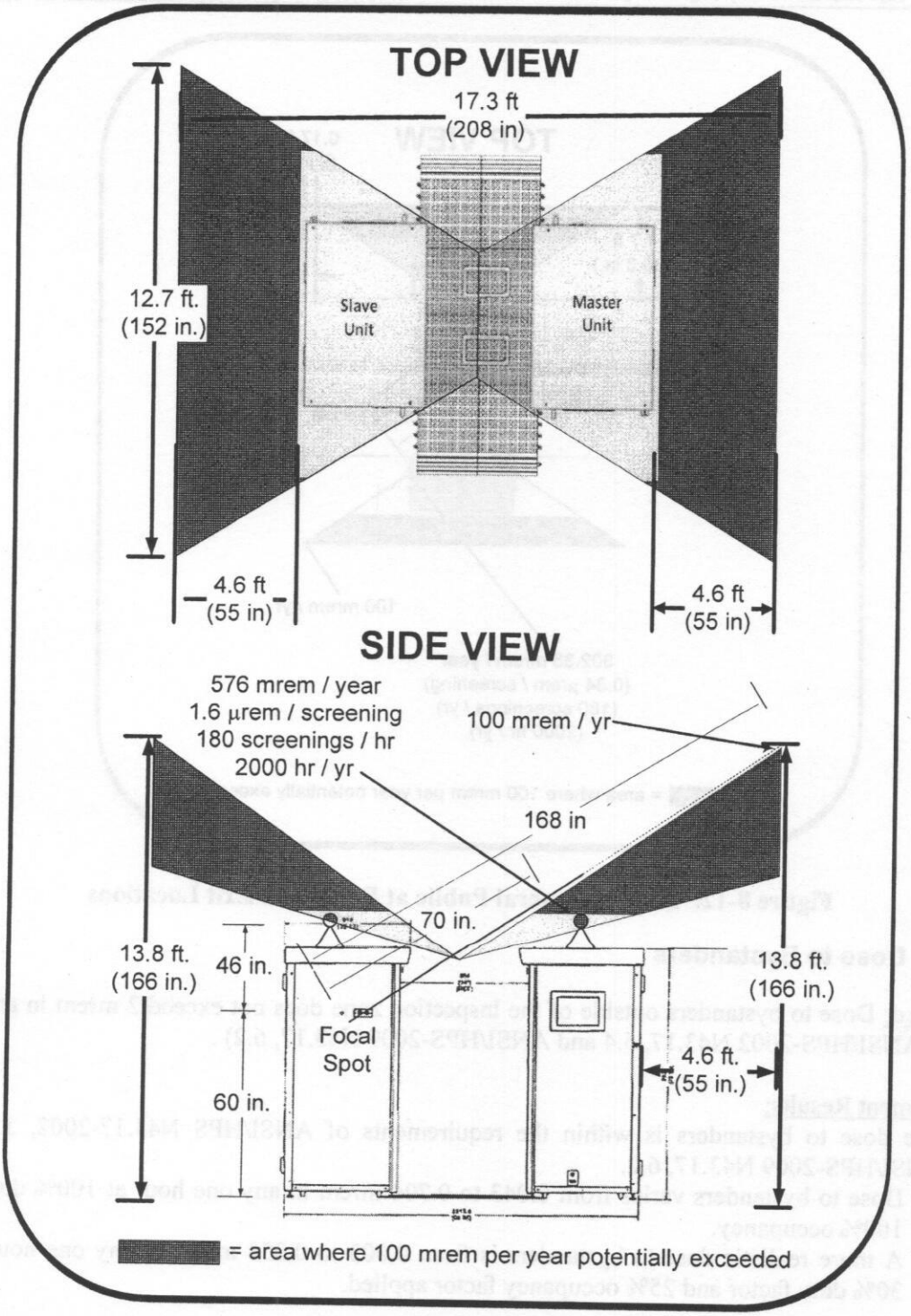


Figure 8-11. Dose to General Public Above Units

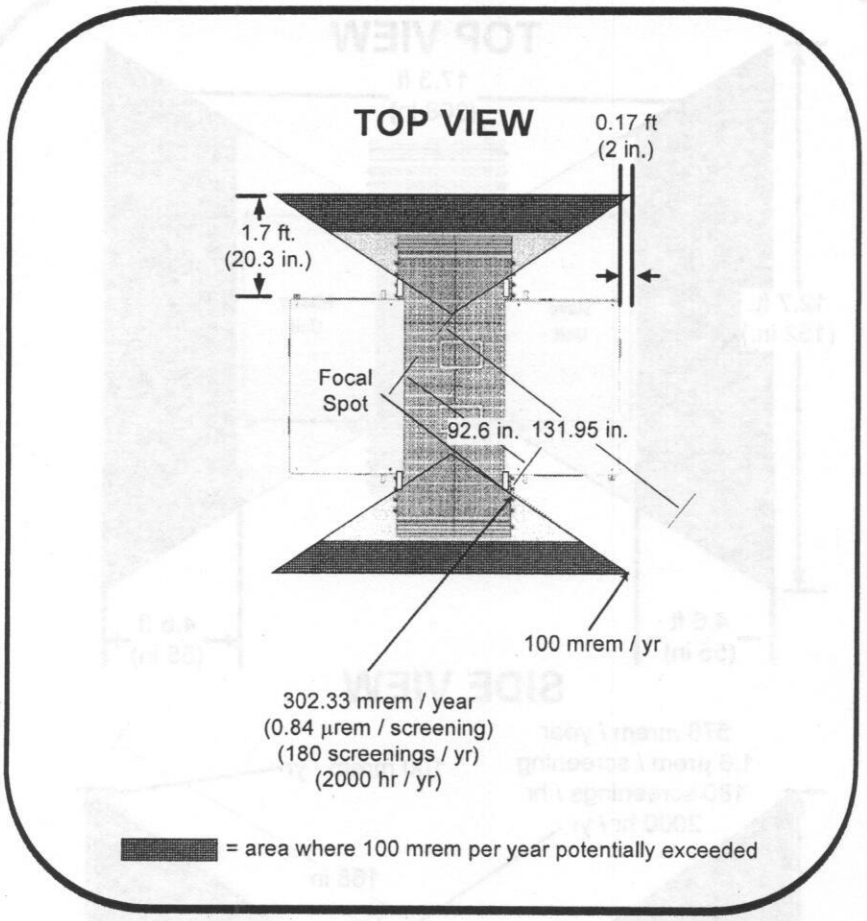


Figure 8-12. Dose to General Public at Entry and Exit Locations

8.6.3 Dose to Bystanders

Standard: Dose to bystanders outside of the inspection zone does not exceed 2 mrem in any one hour (ANSI/HPS-2002 N43.17, 5.4 and ANSI/HPS-2009 N43.17, 6.2) .

Assessment Results:

The dose to bystanders is within the requirements of ANSI/HPS N43.17-2002, 5.4 and ANSI/HPS-2009 N43.17, 6.2.

- Dose to bystanders varies from 0.043 to 0.704 mrem in any one hour at 100% duty and 100% occupancy.
- A more realistic dose to bystanders is from 0.003 to 0.053 mrem in any one hour with 30% duty factor and 25% occupancy factor applied.

Based on the data collected during the area survey as described in Section 8.6.1, dose to bystanders was determined. Table 8-9 provides the bystander dose measurements for the areas surrounding the master and slave unit and Figure 8-13 provides the locations where the 1800 cc ion chamber was placed for conducting exposure readings. The dose to bystanders is

indistinguishable from background radiation at the areas surrounding the right, back, and left side of the units (locations 1, 2, 3, 6, 7, 8). At the wings (locations 4, 5, 9, and 10) the dose to bystander varies from 0.043 mrem to 0.504 mrem in any one hour at 100% duty and 100% occupancy (from 0.003 mrem to 0.038 mrem in any one hour at 30% duty and 25% occupancy).

At locations directly above the units (locations 11 and 12), dose measurements were determined to assess the impact of primary beam overshoot on dose to bystanders that may occupy areas on floors or open spaces above the units. As discussed in Section 8.6.1, the dose per screening above the units was found to be dependent on the vertical motion of the X-ray generator. The dose to bystanders at locations directly above the units (locations 11 and 12) is 0.519 and 0.704 mrem in any one hour at 100% duty and 100% occupancy (0.039 and 0.053 at 30% duty and 25% occupancy). Therefore the dose to bystanders outside of the inspection zone does not exceed 2 mrem in any one hour.

Performance differences were found between the master and slave X-ray units, the slave unit has a harder beam. This is reflected in the results of the dose to bystander measurements. Note that the dose at the wings that resulted from the master X-ray unit (locations 5 and 9) were higher than the dose that resulted from the slave X-ray unit. The dose measurements directly above the units from the master unit were also higher than the slave unit. Since the assessment was conducted with engineering units, this may not appear in production systems that are subject to the quality control process.

Table 8-9. Dose to Bystanders

Location	Average Exposure Reading (μR/screening[1]) Ion Chamber	Average Background Reading (μR[2]) Ion Chamber	Average Exposure with Background Subtracted and Energy Correction Applied (μR/screening[3])	Equivalent Dose for 100% Duty[4] and 100% Occupancy (mrem[5] in any 1 hour)	Duty Factor[6] (D)	Occupancy Factor[7] (T)	Equivalent Dose (mrem/screening x D x T) (mrem[5] in any) 1 hour
4	0.21	0.14	0.071	0.043	0.30	0.25	0.003
5	0.77	0.18	0.602	0.361	0.30	0.25	0.027
9	1.00	0.18	0.840	0.504	0.30	0.25	0.038
10	0.22	0.13	0.100	0.060	0.30	0.25	0.004
11	0.94	0.09	0.865	0.519	0.30	0.25	0.039
12	1.35	0.20	1.174	0.704	0.30	0.25	0.053
1, 2, 3, 6, 7, 8	Exposure reading was not distinguishable from background exposure.						

1. Master unit and slave unit consecutive scans for total scan time of approximately 6 seconds.
2. Background reading represents the average of 5 sequential 6-second background readings for each location.
3. Energy correction factor 1.02 applied.
4. 100% duty factor based on 600 screenings in one hour for 6-second scan time.
5. Assuming 1mR = 1 mrem.
6. 30% duty factor based on 180 screenings in one hour for 6-second scan time (vendor supplied information).
7. Occupancy factor for partial occupancy based on ANSI/HPS N43.3.-2008 Table A-1.

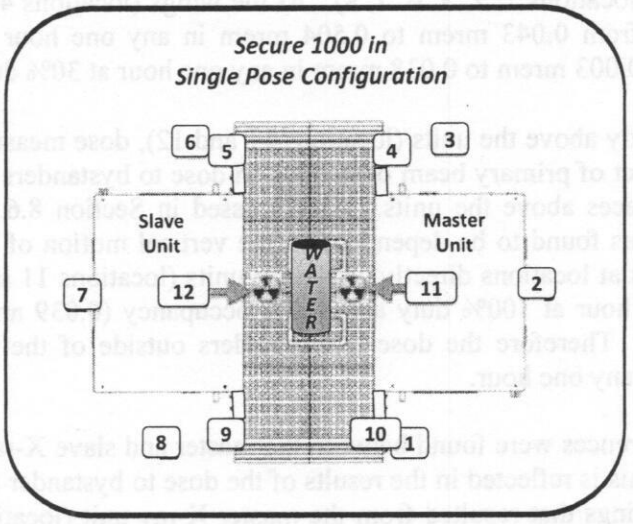


Figure 8-13. Locations for Dose to Bystander Measurements

8.6.4 Dose to Workers

Standard: Radiation dose to personnel at any work station does not exceed dose of 100 mrem/year (1 mSv) (ANSI/HPS N43.17-2002, 5.4 and ANSI/HPS N43.17-2009, 6.2)

Assessment Results:

The dose to personnel at any work station is below 100 mrem/year (or 50 μrem/hour) for 2000 hours/year when there are less than

- 476,304 screenings/year or
- 9,526 screenings/week or
- 1,905 screenings/day or
- 238 screenings/hour

Based on the data collected during the area survey as described in Section 8.6.1, dose to workers was determined. Table 8-10 provides the worker dose measurements for the areas surrounding the master and slave unit and Figure 8-14 provides the locations where the 1800 cc ion chamber was placed for conducting exposure readings.

Table 8-10. Dose to Workers

Location	Average Exposure with Background Subtracted and Energy Correction Applied (μR/screening)[1]	Number of Screenings per Hour for 30% Duty (screenings/hr)	Equivalent Dose for 30% Duty[2] (μrem/hour)	Occupancy Factor[3] (T)	Equivalent Dose for 30% Duty and 25% Occupancy (μrem/hr)	Number Hours Worked per Year (Based on 40 hours per week, 50 weeks per year) (hrs/year)	Maximum Dose per Year (Based on 2000 hours worked per year) (mrem/yr)[4]	Number of Screenings per Year to Reach 100 mrem (screenings/yr)	Number of Screenings per Week to Reach 100 mrem (Based on 50 Weeks per Year) (screenings/wk)	Number of Screenings per Day (Based on 5 Days per Week) (screenings/day)	Number of Screenings per Hour (Based on 8 Hours per Day) (screenings/hr)
4	0.071	180	12.85	0.25	3	2000	6	5,602,241	112,045	22,409	2,801
5	0.602	180	108.32	0.25	27	2000	54	664,673	13,293	2,659	332
9	0.840	180	151.16	0.25	38	2000	76	476,304	9,526	1,905	238
10	0.100	180	17.99	0.25	4	2000	9	4,001,601	80,032	16,006	2,001
1, 3, 6, 8	Exposure reading was not distinguishable from background exposure.										

1. Average exposure reading and background reading is provided in Table 8-9. Energy correction factor 1.02 applied.
2. Duty factor based on 180 screenings in one hour for 6 second scan time (vendor supplied information).
3. Occupancy factor for partial occupancy based on ANSI N43.3-2008 Table A-1.
4. Assuming 1 mR = 1 mrem.

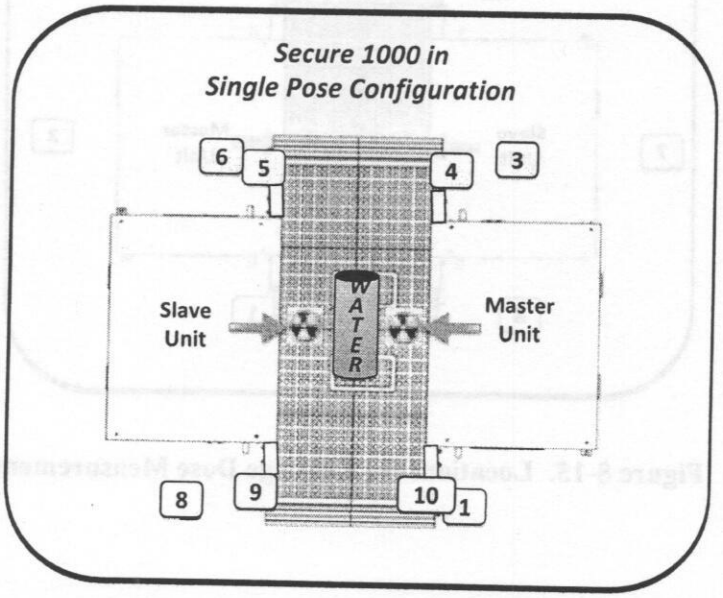


Figure 8-14. Locations for Dose to Workers Measurements

8.7 Leakage Dose Rate

Standard: Leakage dose rate at any point 30 cm from any external surface, excluding the beam exit surface, shall not exceed 0.25 mrem (2.5uSv) in any one hour (ANSI/HPS N43.17-2002, 5.5 Shielding and ANSI/HPS N43.17-2009, 6.3 Shielding)

Assessment Results:

- Leakage dose rate at 30 cm from any external surface of the master and slave unit are not distinguishable from background exposure using the 1800 cc ion chamber.
- The system meets the ANSI/HPS N43.17-2002, 5.5 and ANSI/HPS N43.17-2009, 6.3 Shielding requirements for sealed units.

Based on the data collected during the area survey as described in Section 8.6.1, leakage dose rate was determined. Figure 8-15 provides the locations where the 1800 cc ion chamber was placed for conducting exposure readings; these locations were 30 cm from the external surface of the unit. As indicated in Figure 8-15 and Section 8.6.1, these readings were taken with water placed between the master and slave units as an X-ray scattering source. Since it was found that the leakage dose measurements were not distinguishable from background exposure, it was not necessary to make additional measurements without a scattering source.

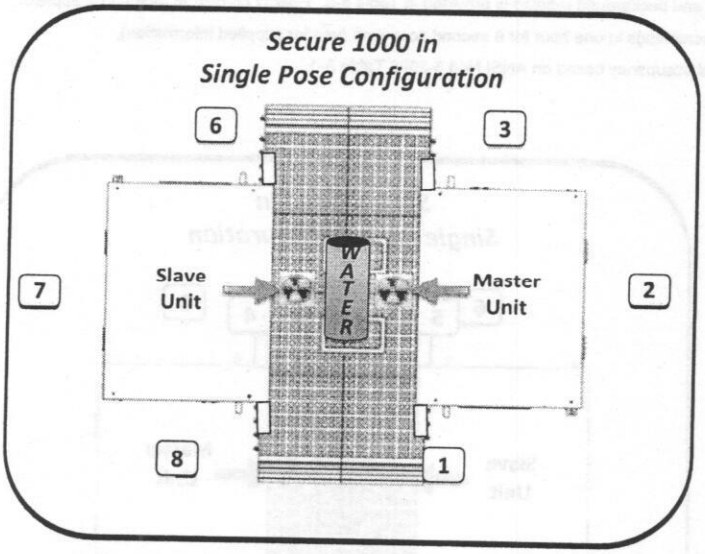


Figure 8-15. Locations for Leakage Dose Measurements

8.8 Physical Safety

Safety features related to operation and use of the Secure 1000 in Single Pose Configuration were reviewed and tested to ensure personal safety of operators, scanned individuals, and the general public and to verify compliance with ANSI/HPS N43.17-2002 and 2009. A series of tests, inspections and documentation reviews were conducted to assess the physical safety of the system. Note that ANSI/HPS N43.17-2009 7.2.1 (f), (h), (j), (m), and 7.2.2 (d), (e), and 7.6 (h) were not evaluated. The following sections provide assessment findings.

8.8.1 Indicators and Controls

Standard: ANSI/HPS N43.17-2002, 6.1 Indicators and controls. ANSI/HPS N43.17-2009, 7.2.1 Requirement for all systems (a), (b), (c), (d). ANSI/HPS N43.17-2009, 7.2.2 Requirements for general-use systems using x-ray sources (b).

Assessment Results: Rapiscan Secure 1000 in Single Pose Configuration meets the requirements of ANSI/HPS N43.17-2002, 6.1, ANSI/HPS N43.17-2009, 7.2.1 (a), (b), (c), (d), and ANSI/HPS N43.17-2009, 7.2. (b).

The system has two operational modes available to system operators, "managing" and "screening". Peak kilovoltage (kV), mA, and scan time (which is dictated by disabling X-rays once 480 data lines are collected) are preset by the vendor and are not alterable by the system operator at the inspection console with either operational mode. These factors are accessible to technicians in "servicing" mode, as shown in Figure 8-16. The only time a scan can be executed from the inspection console is when the system is in "servicing" mode.

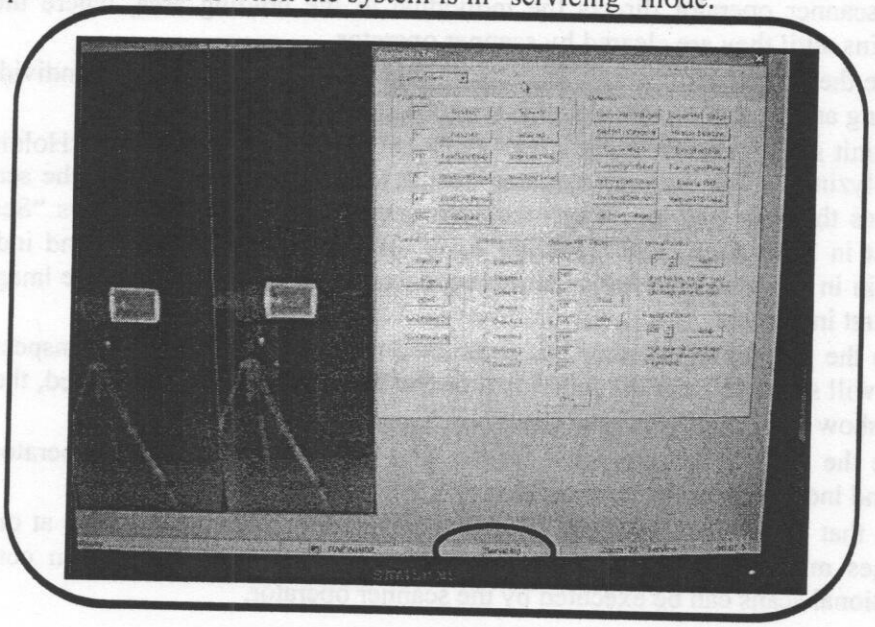


Figure 8-16: "Servicing" Mode

In an operational setting there will be at least two operators, the inspection operator and the scanner operator. The inspection operator will be stationed at the inspection console at a location where the screening area (and the individual being screened) is not visible. At the inspection console, "managing" and "screening" modes are available, however, the system must be in the "screening" mode to conduct scans. At all times, "screening" or "managing" is clearly visible at the bottom of the screen to indicate the current mode, as shown in Figure 8-17. The "managing" mode is for supervisors and provides capabilities that include user management, archive management, setting management, and report and raw data management. The only mode available to the inspection operator is "scanning" mode. The responsibility of the inspection operator is to log in to the console at the beginning of the shift, view the X-ray images, and determine if the scanned individuals should be cleared or searched.

The scanner operator will be located near the exit of the scan area, where the scan button and status screen is mounted to the side of one of the units, as shown in Figure 8-18. Scans are executed by pressing the scan button shown in Figure 8-18. The operational scenario for scanning individuals is as follows:

- The scanner operator directs an individual to stand in the scan area.
- The unit status screen shows "Scan Area" is "Ready for Next Person" as shown in Figure 8-19.
- The scanner operator presses the scan button. The unit status screen shows
  - "Scan Area" as "Scan in Progress" and "Holding Area" as "Analyzing" and then
  - "Scan Area" as "Scan Complete. Move to Holding Area." and "Holding Area" as "Analyzing."
- The scanner operator directs the individual to the holding area, where the individual remains until they are cleared by scanner operator.
- While the inspection operator is analyzing the image and the scanned individual is in the holding area, a second individual is scanned.
- The unit screen shows "Scan Area" as "Ready for Next Person" and "Holding Area" as "Analyzing". The scanner operator directs the second individual to the scan area, and presses the scan button. When the scan is complete the screen shows "Scan Area" as "Wait in Scan Area" and "Holding Area" as "Analyzing". The second individual will remain in the scan area until the inspection operator has completed the image review of the first individual.
- Once the inspection operator has completed the image review, at the inspection console they will select to clear the individual or conduct a search. Once selected, the unit screen will show "Holding Area" as "Clear" or "Conduct Search".
- Once the analysis is completed for the first individual, the scanner operator directs the second individual to the holding area.
- Note that the system will only allow two scans to remain in the queue at one time, the images must be cleared by the inspection operator at the inspection console before additional scans can be executed by the scanner operator.

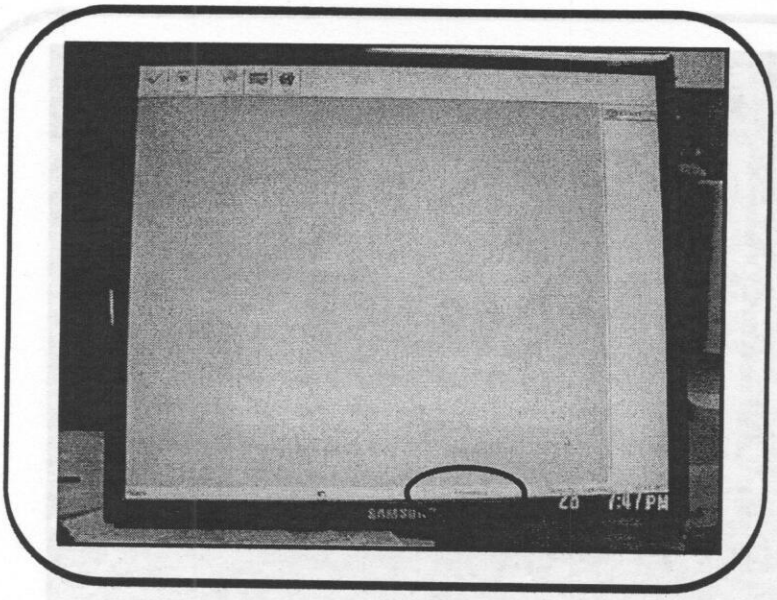


Figure 8-17: "Screening" Mode

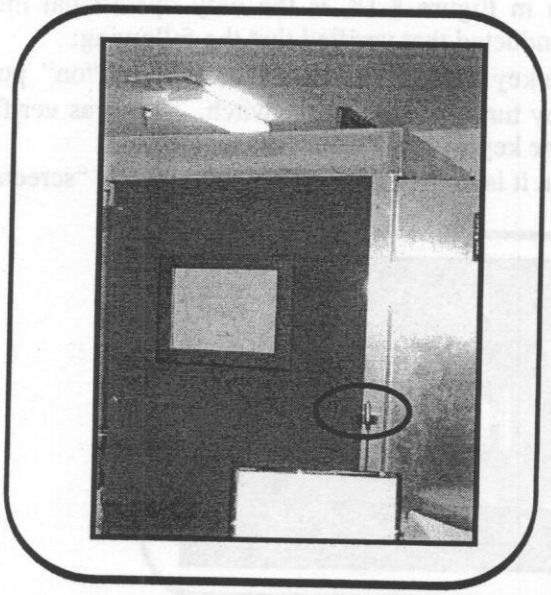


Figure 8-18: Scan Button and Status Screen on Unit

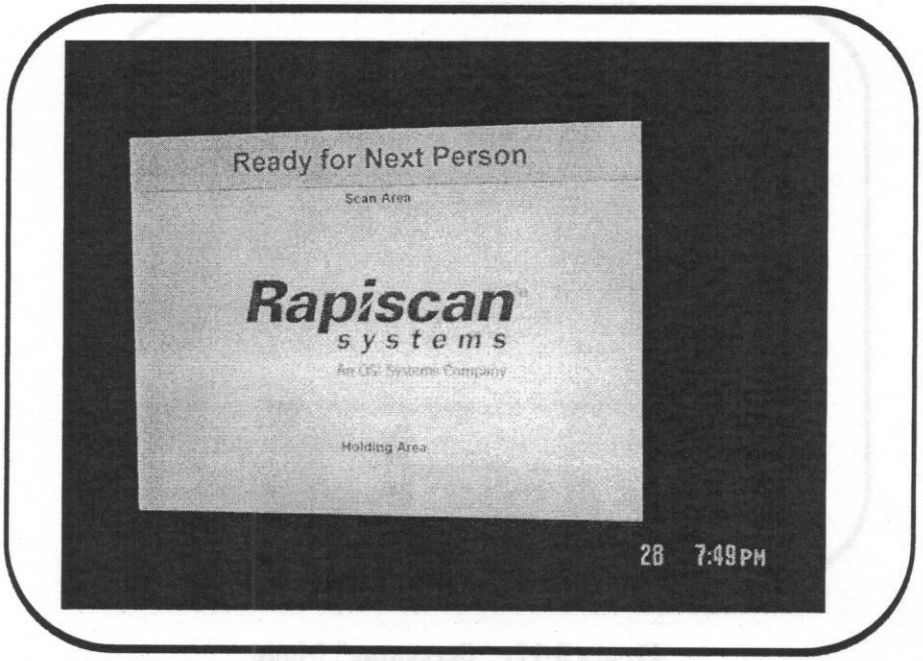


Figure 8-19: "Ready" for Scan Screen

Power to the system is controlled by a key switch, shown in Figure 8-20. The key switch has three positions, "off", "standby", and "on". When the key is placed on "standby" the system waits for commands from the operator console and will time out if commands are not received. A separate scan button, shown in Figure 8-18, is the only operational mode mechanism for executing a scan. Tests were conducted that verified that the following:

- To power the system, the key switch must be on "standby" or "on" position.
- X-rays are not emitted by turning on the key switch. This was verified with a radiation meter and operation of the key switch.
- The key is captured when it is in the ON position required for "screening" mode .

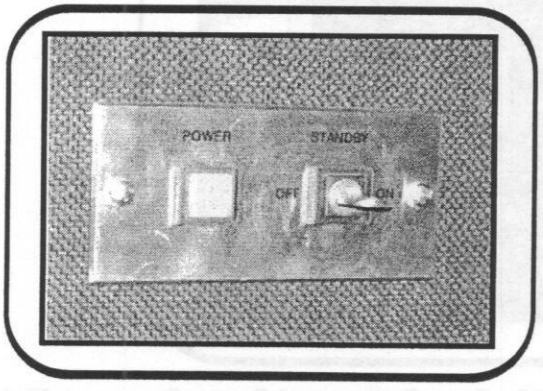


Figure 8-20: Key Switch

The "SCAN IN PROGRESS" light on the beam exit side of each unit is clearly visible and operates when a scan is in progress. Additionally, the screen on the side of the unit indicates that a scan is in progress. The light and screen are clearly visible from the location where the scan button can be operated, as shown in Figure 8-21.

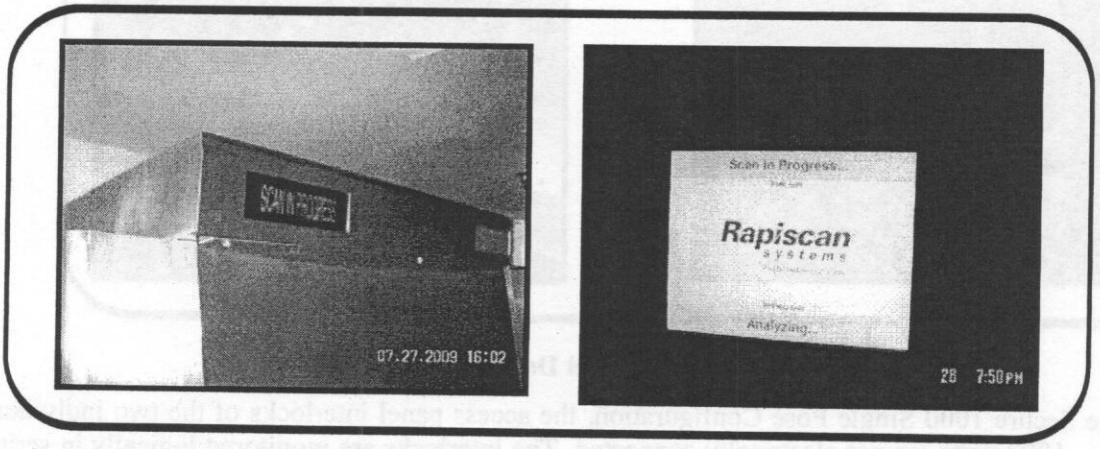


Figure 8-21: Scan Indicator on Units

8.8.2 Access Panel Interlocks

Standard: ANSI/HPS N43.17-2002, 6.2.1 Access panel interlocks. ANSI/HPS N43.17-2009, 7.2.1 Requirement for all systems (i). ANSI/HPS N43.17-2009, 7.2.2 Requirements for general-use systems using x-ray sources (c).

Assessment Results: Rapiscan Secure 1000 in Single Pose Configuration meets the requirements of ANSI/HPS N43.17-2002, 6.2.1 Access panel interlocks, ANSI/HPS N43.17-2009, 7.2.1 Requirement for all systems (i), and ANSI/HPS N43.17-2009, 7.2.2 Requirements for general-use systems using x-ray sources (c).

Each Secure 1000 master and slave unit has access panels doors that require a key for access. Use of the key latches the top and bottom of the door. A mechanical sensor at the bottom of the door is depressed when the door is closed. If the door is opened, the sensor is released and the interlock prevents operation of the system. Tests were conducted that verified that the doors will not open without a key and that scans cannot be conducted when the doors are opened and the mechanical door sensor is released. The key lock and mechanical door sensor are shown in Figure 8-22.

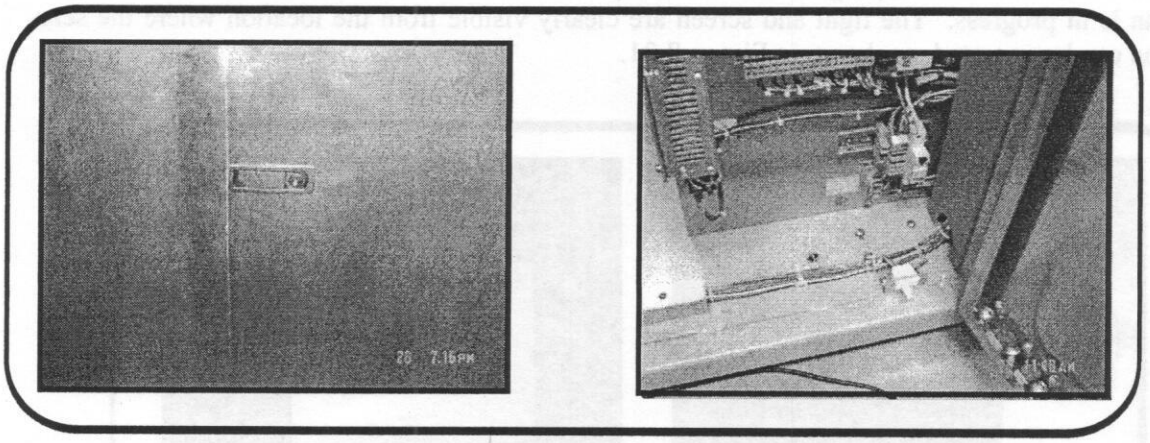


Figure 8-22: Access Panel Door and Door Interlock

In the Secure 1000 Single Pose Configuration, the access panel interlocks of the two individual Secure 1000 units are not electrically connected. The interlocks are monitored logically in series from the master to slave unit by software on the operator's console. Both master and slave access panel interlocks must be enabled for a scan to initiate and complete. If the master access panel interlock is disabled, the slave unit is put in soft standby mode even if its access panel interlock is enabled. No scan is possible in this condition. If the master unit's access panel interlock is disabled by opening the door while a scan on the master unit is in progress, the scan terminates immediately and a scan with the slave unit is not initiated. If the slave unit access panel interlock is disabled when a scan on the master unit is in progress, the system will complete the master unit's scan and then terminate the scan.

8.8.3 Operational Interlocks

Standard: ANSI/HPS N43.17-2002, 6.2.2 Operational interlocks. ANSI/HPS N43.17-2009, 7.2.1 Requirement for all systems (l), (n).

Assessment Results: Rapiscan Secure 1000 in Single Pose Configuration meets the requirements of ANSI/HPS N43.17-2002, 6.2.2 Operational interlocks and ANSI/HPS N43.17-2009, 7.2.1 Requirement for all systems (l), (n).

The system has multiple operational interlocks that are monitored by the system and terminate X-ray production if thresholds are not met or discrepancies are detected. Based on technical discussions with Rapiscan engineers and the safety features description provided in Reference [9], the major system parameters monitored are as follows:

- X-ray tube head kV and mA: This system operates at the maximum limits of the tube at 50 kV at 5.0 mA. In addition, X-rays will terminate if there is over voltage or over current.

- Reference detector signal: A detector with a Photodiode is placed in the X-ray beam, the X-ray intensity is monitored for radiation levels out of range and detector signal is monitored for a level of 2.5 V with a low and high cutoff threshold of 1.92V and 2.92V.
- Velocity of vertical motion: An optical interrupter switch that travels with the X-ray tube generates electrical pulses to monitor vertical motion. An up controlled brushless DC servo motor drives a 4-foot long lead screw mounted on bearings. There are only three moves, "scan-up", "scan-down", and "home". The home function is accomplished automatically when the servo motor controller is initially energized by its power relay. X-rays are terminated if vertical motion stops.
- Velocity of horizontal motion (chopper speed) of the scanned beam: An optical interrupt sensor located on the chopper wheel assembly is used to monitor that the rotational velocity of the chopper wheel is maintained at 2400 RPM. An IR LED shines through the slits to a photo sensor as the chopper wheel rotates. Chopper wheel speed is monitored to determine if it is necessary to speed up or slow down the chopper motor in order to achieve the correct frequency. X-rays are terminated if the chopper wheel speed is out of tolerance.
- X-ray tube head temperature: X-rays will terminate if the X-ray tube temperature is out of range.
- Main watch dog timer (monitor by software): Monitoring includes the reference detector, chopper wheel timer, vertical motion timer, microprocessor commands (X-rays terminated if commands are not received), and software malfunctions.
- Microcontroller (monitor by hardware): Microcontroller codes look for at least 480 lines of data and once achieved X-ray is disabled. Monitors include vertical motion, horizontal motion, and door sensor.

The scan has two phases that are monitored by the system, the "Bypass Phase" and "Main Phase". The "Bypass Phase" occurs during the first 0.5 seconds of the scan when the X-ray generator is energized and vertical motion starts. During this phase vertical motion and X-ray generator output are not monitored because as they are out of tolerance. The remaining 2.5 seconds are the "Main Phase", system monitoring transitions to this phase when vertical motion has reached the point where 30 lines of data have been acquired. At this time it is assumed that vertical motion and X-ray generation are stable and these parameters are monitored. The X-ray scan is terminated if at any time the monitoring circuits detect an abnormality. Note, Rapiscan provided a documented short description of the safety features (Reference [9]) and in discussion provided an updated description to supplement some of the documented descriptions that are outdated.

Testing was conducted that verified that the X-ray scan terminated if the door was opened (mechanical door sensor tripped) and that a normal control sequence is required to initiate a scan.

Standard: ANSI/HPS N43.17-2002, 6.2.2 Operational interlocks, subject exposure during a malfunction. In the event of a malfunction, the system shall terminate x-ray production rapidly enough to limit the subject exposure to a "dose times exposed area" of 250 μSv cm2 (25 mrem cm2). (For example: 25 μrem over a 1000 square centimeter area or 50 μrem over a 500 square

centimeter area, etc.). Additionally, no location on the subject's body shall receive a dose exceeding 25 mrem, regardless of the exposed area.

Assessment Results: Assuming maximum exposure time to a subject in the event of a malfunction is approximately 3 seconds, the maximum dose per area is 0.42 μrem/cm^2, which is significantly less than the 25 mrem cm^2 limit.

The assessment of subject exposure during a malfunction is based on a single point failure analysis, where the vertical motion of the X-ray tube stopped and was undetected by the system. Since the system limits the exposure time by monitoring the maximum number of scan lines, the maximum exposure time is limited to approximately 3 seconds. The total dose from a 3-second scan has been determined to be much less than the 10 μrem per scan limit. However, to be very conservative, a maximum dose of 10 μrem per scan will be used for the following analysis. The beam width at the subject is approximately 4 mm (0.4 cm). Assuming a subject width of 60 cm, an exposure of a 24 cm^2 area would result. Averaging the total dose of 10 μrem over a 24 cm^2 area results in a maximum dose per area of 0.42 μrem/cm^2. This is significantly less than the 25 mrem cm^2 limit specified by the ANSI N43.17-2002 standard.

8.8.4 Emergency Stop Capability

Requirement: TSA requires that screening systems have an emergency stop capability. ANSI/HPS N43.17-2009, 7.2.1 Requirement for all systems (e).

Assessment Results: Rapiscan indicated that an emergency stop button is provided on the master and slave unit delivered to the TSL. The engineering system evaluated did not have the full emergency stop capability implemented, therefore it was not tested.

The Secure 1000 in Single Pose Configuration that JHU/APL evaluated was an engineering system, and the emergency stop button capability was not fully implemented on the units evaluated. The slave unit had an emergency stop button (shown in Figure 8-23), however the button connections were not wired to the system and the button was not operable. The master unit did not have an emergency stop button. Rapsican informed JHU/APL that in the system at TSL both the master and slave are equipped with emergency stop buttons.

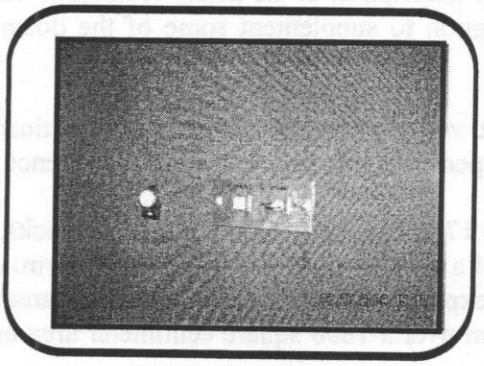


Figure 8-23: Emergency Stop Button

8.8.5 Automatic Termination

Standard: ANSI/HPS N43.17-2002, 6.2.3 Automatic termination. ANSI/HPS N43.17-2009 7.2.1 Requirements for all systems (g).

Assessment Results: Rapiscan Secure 1000 in Single Pose Configuration meets the requirements of ANSI/HPS N43.17-2002, 6.2.3 Automatic termination and ANSI/HPS N43.17-2009 7.2.1 Requirements for all systems (g).

JHU/APL measured the external emission of X-rays at the completion of the scanning cycle, and verified that no X-Rays were being emitted. Rapiscan indicated that the scanning cycle ends and X-ray generation terminates when 480 lines of data are collected or vertical motion stops.

8.8.6 Ground Fault

Standard: ANSI/HPS N43.17-2002, 6.3 Ground fault. ANSI/HPS N43.17-2009 7.2.1 Requirements for all systems (g).

Assessment Results: Rapiscan informed JHU/APL that the system has an interlock that will terminate X-rays if there is a ground fault, as required by ANSI/HPS N43.17-2002, 6.3 and ANSI/HPS N43.17-2009 7.2.1 (g).

8.8.7 Labeling

Standard: ANSI/HPS N43.17-2002, 6.4 Labeling. ANSI/HPS N43.17-2009, 7.3 Labeling.

Assessment Results: Rapiscan Secure 1000 in Single Pose Configuration meets the requirements of ANSI/HPS N43.17-2002, 6.4 Labeling and ANSI/HPS N43.17-2009, 7.3 Labeling.

The master and slave unit each have a label that is permanently affixed to the system that includes the name and address of the manufacturer, manufacture date, model number, and serial number (see Figure 8-24). Since an engineering unit was evaluated, the serial number on the label was incorrect.

Figure 8-24: Secure 1000 in Single Pose Configuration Label

ANSI/HPS-N43.17-2002, 6.4 and ANSI/HPS N43.17-2009, 7.3 require that the radiation source and shielding assembly have a clear and visible radiation warning label, and that this label is visible from any point where service access might be gained. JHU/APL verified the existence of this label (shown in Figure 8-25), however the label is affixed to the outside of the tube, and its visibility is dependent on the position of the tube. There is no label on the shielding assembly.

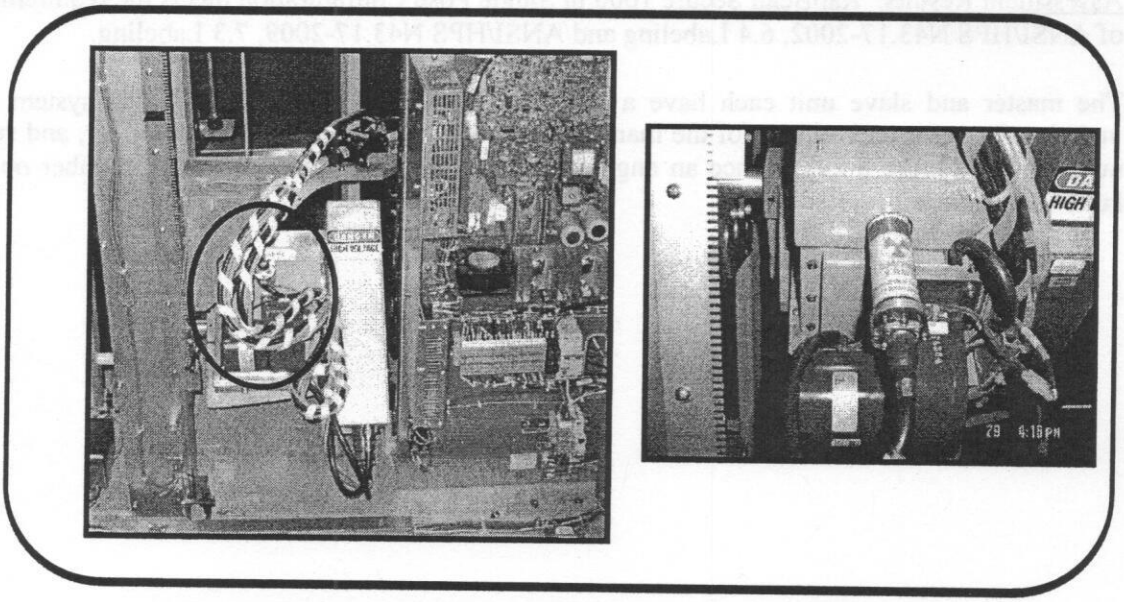


Figure 8-25: Radiation Warning Label

8.8.8 Modifications

Standard: ANSI/HPS N43.17-2002, 6.5 Modifications and ANSI/HPS N43.17-2009, 7.4 Modifications.

Assessment Results: Rapiscan informed JHU/APL that system changes are controlled by an Engineering Change Notice (Reference [10]), Request for Waiver, or Request for Deviation and that labels are updated to reflect any changes in compliance with ANSI/HPS N43.17-2002, 6.5 Modifications and ANSI/HPS N43.17-2009, 7.4 Modifications.

8.8.9 Information for the End User

Standard: ANSI/HPS N43.17-2002, 6.6 Information to be provided to the end user and ANSI/HPS N43.17-2009 7.5 Information to be provided to the end user.

Assessment Results: The draft Operator Manual (Reference [11]), draft Maintenance Manual (Reference [12]), and Specification Sheet (Reference [4]) provide the information required by ANSI/HPS N43.17-2002, 6.6 and ANSI/HPS N43.17-2009 7.5 (b), (c), (d), (e), and (f) with the exception of technique factors (peak kilovoltage, electrical current, scan time) for each mode and total aluminum equivalent filtration. Final documents should be reviewed when completed and it is recommended that document revisions include technique factors and other information required by ANSI/HPS N43.17-2009, 7.5 (a), (g), (h), (i), and (j).

Rapiscan provided a draft Operator Manual and Maintenance Manual that were being revised for the single pose configuration of the Secure 1000. JHU/APL reviewed the draft documents and verified that the documents include safety practices and warnings, licensing that may be required, operational procedures for safe operation, and preventive maintenance requirements for safe operation. The specifications sheet includes kV and mA, however, the manuals do not include the technique factors (peak kilovoltage, electrical current, scan time) for each mode and total aluminum equivalent filtration as required by ANSI/HPS N43.17-2002 and 2009. It is recommended that this information is included in the updated document and that the final documents be reviewed when they are complete. Additionally, it is recommended that information required by ANSI/HPS N43.17-2009, 7.5 (a), (g), (h), (i), and (j) are included in the revisions of the documents.

8.8.10 Records Maintained by Manufacturers

Standard: ANSI/HPS N43.17-2002, 6.7 Records to be maintained by manufacturers and ANSI/HPS N43.17-2009, 7.6 Records to be maintained by manufacturers.

Assessment Results: Rapiscan informed JHU/APL of processes and records that meet the requirements for ANSI/HPS N43.17-2002, 6.7 and ANSI/HPS N43.17-2009, 7.6 (a) through (g).

JHU/APL reviewed the requirements of ANSI/HPS N43.17-2002 6.7 with Rapiscan and Rapiscan indicated that there are processes and records in place the meet the requirements of 6.7. Quality control procedures are in place which include final factory acceptance testing prior to

delivery. Service notifications are used by the service department maintenance, service, and training.

8.8.11 Installation Procedures

Standard: ANSI/HPS N43.17-2002, 7.2 Installation and ANSI/HPS N43.17-2009, 8.1.2 Installation.

Assessment Results: Rapiscan's Site Acceptance Test (SAT) provides functional system tests and a radiation survey (Reference [13]) that must be completed and approved for system acceptance. Installation procedures were not provided. Since the system evaluated was installed by Rapiscan, requirements ANSI/HPS N43.17-2002, 7.2 Installation and ANSI/HPS N43.17-2009, 8.1.2 were not evaluated.

8.8.12 Radiation Surveys

Standard: ANSI/HPS N43.17-2002, 7.7 Radiation surveys and ANSI/HPS N43.17-2009, 8.1.7 Radiation surveys.

Assessment Results: An assessment of Rapiscan third party radiation survey reports is provided in Section 8.2 of this report. A review of the reports found that the surveys did not conduct a complete area survey with the two unit configuration to determine dose to bystanders, an X-ray scattering source was not used for the area survey, an assessment of radiation leakage with the two unit configuration was not conducted, the assessment was conducted with one unit active and the second unit inactive, and the reports did not include evaluation of other ANSI/HPS N43.17 requirements such as safety interlocks.

8.9 Radiation Safety Product Report

Standard: FDA C.F.R. 21 Subchapter J Part 1002 Radiation Safety Product Report, ANSI/HPS N43.17-2002 4. Federal, state, and local regulations, ANSI/HPS N43.17-2009 4. Federal, state, and local regulations.

Assessment Results: The existing Rapiscan FDA filing is for the Secure 1000 system, dated 1992. The Secure 1000 in Single Pose Configuration is configured differently than Secure 1000 from the filing, however there is no filing for the new configuration. The FDA responded to the 1992 filing stating *"...this product is not actively regulated under the device authorities of the Food Drug and Cosmetic Act (FFDCA). The Performance Standard for Diagnostic X-Ray Systems and Their Major Components does not apply to the Secure 1000."* (Reference [14], [15], [16]).

9. CONCLUSIONS AND RECOMMENDATIONS

A radiation safety engineering assessment of the Secure 1000 in Single Pose Configuration was conducted to measure, verify, and report the parameters of system performance against TSA requirements, ANSI/HPS N43.17-2002, ANSI/HPS N43.17- 2009, and C.F.R. Title 21 Chapter I Subchapter J Part 1002 Records and Reports. Concluding observations are as follows:

- The system provided for radiation safety evaluation was an engineering unit built by the Rapiscan engineering team using components from their inventory and configured to be at the same version level and functionally equivalent to the system evaluated at the TSL.
- Performance differences were noted between the master and slave engineering units that may not appear in production systems that are subject to Rapiscan's production and quality control processes. Where differences were noted the most conservative measurements were used.
- The dose to scanned individuals is within requirements of ANSI/HPS N43.17-2002, 5.1 limit of 10 μrem/scan of subject's front and of ANSI/HPS N43.17-2009, 5.1 limit of 25 μrem/screening.
- The dose to bystanders is within the 2 mrem in any one hour requirement (assuming 30% duty and 25% occupancy) for ANSI/HPS N43.17-2002 and 2009.
- The leakage dose rate is within the 0.25 mrem in any hour requirement for ANSI/HPS N43.17-2002 and 2009.
- The dose to workers is within the 100 mrem in any one hour requirement (assuming 30% duty and 25% occupancy for 2000 hours) for ANSI/HPS N43.17-2002 and 2009.
- Areas exist above the units and at the entry/exit locations where the 100 mrem per year general public dose limit could potentially be exceeded. It is recommended that a survey of each installation site be conducted to ensure that the dose to any member of the general public is maintained below the 100 mrem (0.1 rem) per year limit and to ensure that doses are kept ALARA. For the area above the units, a beam stop may be considered to ensure the general public dose limit is maintained.
- The system provides necessary interlocks to prevent unauthorized system access and provides emergency stop buttons.
  - Since an engineering system was evaluated, only one unit had an emergency stop button and it was not wired, therefore functional performance could not be validated.
  - The vendor reported that the TSL system incorporated an emergency stop button on each unit (master and slave).
- Depending on the position of the generator, the radiation warning label on the X-ray tube may not be clearly visible. The label may need to be placed in a more visible location. The shielding assembly does not have a warning label as required by ANSI/HPS-N43.17-2002, 6.4 and ANSI/HPS N43.17-2009, 7.3.
- The Secure 1000 in Single Pose Configuration draft Operator Manual and draft Maintenance Manual provided were under revision, the final version of the documents should be reviewed.
- The draft Operator Manual, draft Maintenance Manual, and Specification Sheet provide the information required by ANSI/HPS N43.17-2002, 6.6 and ANSI/HPS N43.17-2009 7.5 (b), (c), (d), (e), and (f) with the exception of technique factors (peak kilovoltage,

electrical current, scan time) for each mode and total aluminum equivalent filtration. Final documents should be reviewed when completed and it is recommended that document revisions include information required for technique factors and additional information required by ANSI/HPS N43.17-2009, 7.5 (a), (g), (h), (i), and (j).

- Rapiscan's Site Acceptance Test (SAT) provides functional system tests and a radiation survey that must be completed and approved for system acceptance. Installation procedures were not provided. Since the system evaluated was installed by Rapiscan, requirements ANSI/HPS N43.17-2002, 7.2 and ANSI/HPS N43.17-2009, 8.1.2 were not evaluated.
- The existing Rapiscan FDA filing is for the Secure 1000 system, dated 1992. The Secure 1000 in Single Pose Configuration is configured differently than Secure 1000 from the filing, however there is no filing for the new configuration. The FDA responded to the 1992 filing stating *"...this product is not actively regulated under the device authorities of the Food Drug and Cosmetic Act (FFDCA). The Performance Standard for Diagnostic X-Ray Systems and Their Major Components does not apply to the Secure 1000."*

10. REFERENCES

[1] ANSI/HPS N43.17-2002, American National Standard Radiation Safety for Personnel Screening Systems Using X-rays, American National Standards Institute Inc., April 3, 2002

[2] ANSI/HPS N43.17- 2009 Final for Publication, American National Standard Radiation Safety for Personnel Screening Systems Using X-ray or Gamma Radiation, American National Standards Institute Inc., July 7, 2009

[3] U.S. Food and Drug Administration Title 21, Volume 8, Chapter I Food and Drug Administration Department of Health and Human Services, Subchapter J Radiological Health, Part 1002 Records and Reports

[4] Rapiscan Systems Secure 1000 DV Specifications Sheet

[5] Farley, Donald V., M.S., D.A.B.M.P., Medical and Health Physics Consulting, Radiation Report on Rapiscan Systems Secure 1000, 21 March 2006

[6] Farley, Donald V., M.S., D.A.B.M.P., Medical and Health Physics Consulting, Radiation Report on the Rapiscan Systems Secure 1000, 5 June 2008.

[7] Farley, Donald V., M.S., D.A.B.M.P., Medical and Health Physics Consulting, Supplement to Report Dated 5 June 2008, 28 October 2008.

[8] Cerra, Frank, National Institute of Standards and Technology Assessment of Radiation Safety and Compliance with ANSI N43.17-2002 Rapiscan Dual Secure 1000 Personnel Scanner, 9 July 2008.

[9] OSI Systems Pvt. Ltd., Safety Features Secure 1000, Prepared by D. Anant, 10 July 2005

[10] Rapiscan Systems Engineering Change Notice Form R-0028-11, 2 April 2008

[11] Rapiscan Systems Secure 1000 Whole Body Imager Operator Manual Draft, Rapiscan Document Number 9210668, Revision 3, 15 April 2009

[12] Rapiscan Systems Secure 1000 Personnel Scanner Maintenance Manual Draft, Rapiscan Document Number 9210669, Revision 2, 15 July 2009

[13] Rapiscan Systems Secure 1000 Radiation Emission Measurement Form R-0338-4

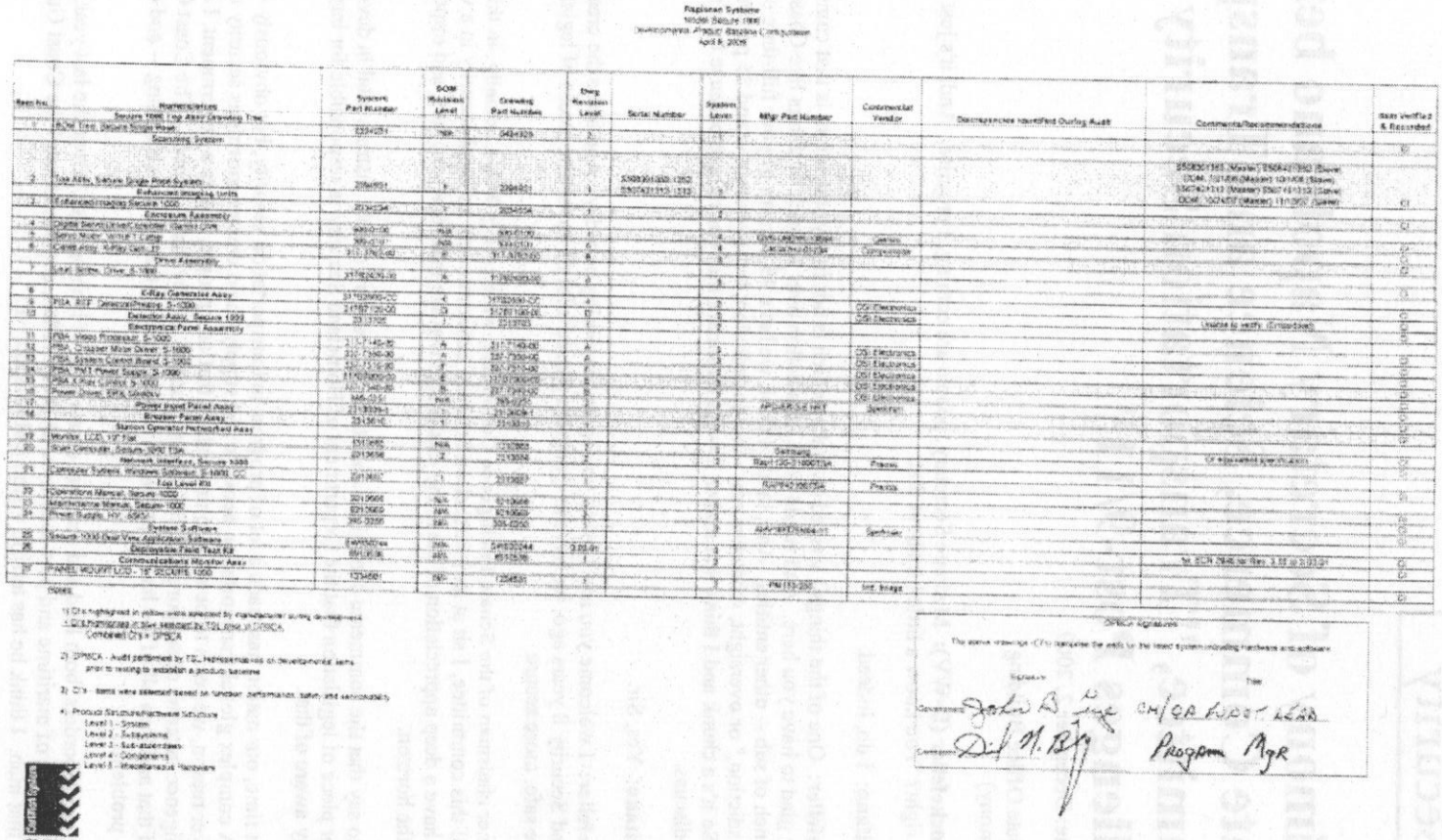
[14] Department of Health and Human Services Letter to IRT Corporation (Mr. Crosby and Dr. Smith), Ref: OCS 9110663-03, 17 August 1992

[15] Smith, Steve W., Nicolet Imaging Systems, Detection of Objects Concealed Under Persons' Clothing Using the SECURE System, 77071-A11, November 1991

[16] Rapiscan Secure Products Secure 1000 Concealed Object Detection System, Addendum November 1998

APPENDIX A. CONFIGURATION OF THE SECURE 1000 SYSTEM IN SINGLE POSE CONFIGURATION

The following document was provided to JHU/APL by Rapiscan, and is the configuration document for the Secure 1000 System in Single Pose Configuration.



Rapiscan Systems
10080 Secure 1000
Configuration Product Baseline Configuration
April 9, 2009

Item No.	Nomenclature Secure 1000 Top Assy Drawing Tree	System Part Number	DOM Revision Level	Drawing Part Number	Dwg Revision Level	Serial Number	System Level	Mfgr Part Number	Commercial Vendor	Discrepancies Identified During Audit	Comments/Recommendations	Item Verified & Recorded
1	Root Tree, Secure Single Pose	5334251	10A	5404329	A		1					C
	Scanning System											
2	Top Assy, Secure Single Pose System	2066951	A	2066951	A	53003010001352 53074211151333	2				53030011A1 (Master) 2500A1 (TBD Slave) DOM: 10/14/08 (Master) 10/14/08 (Slave) 53074211J (Master) 2501J1313J (Slave) DOM: 10/24/07 (Master) 11/13/07 (Slave)	C1
	Enhanced Imaging Units											
3	Enhanced Imaging Secure 1000	2034294		2034294	A		2					
	Enclosure Assembly											
4	Digital Secure Linear Controller, Gamma 2DIR	9400136	10B	9400136	A		3					C
5	Control Module, Vertical Carrier	9400137	10B	9400137	A		3	Vertical Carrier Module	Unknown			C
6	Control Assy, Turntable Gantry	9400138	10B	9400138	A		3	Turntable Gantry Control Assy	Unknown			C
	Drive Assembly											
7	Belt, Timing, Drive, S-1000	31758243-01	A	31758243-01	A		3					C
	X-Ray Generator Assy											
8	X-Ray Generator Assy	53103000-02	A	53103000-02	A		3					C
9	PSA, 80P, Detector/Imaging, S-1000	31758243-02	B	31758243-02	A		3		OEI Electronics			C
10	Detector Assy, Secure 1000	53113000		53113000	D		3		OEI Electronics		Unable to verify (Unspecified)	C
	Electronics Panel Assembly											
11	PSA, Video Processor, S-1000	31774345-80	A	31774345-80	A		3		OEI Electronics			C
12	PSA, Stepper Motor Driver, S-1000	31774345-80	A	31774345-80	A		3		OEI Electronics			C
13	PSA, System Control Board, S-1000	31774345-80	A	31774345-80	A		3		OEI Electronics			C
14	PSA, HVT Power Supply, S-1000	31774345-80	A	31774345-80	A		3		OEI Electronics			C
15	PSA, X-Ray Control, S-1000	31774345-80	A	31774345-80	A		3		OEI Electronics			C
16	Power Driver, SPA, Gantry	31774345-80	A	31774345-80	A		3		OEI Electronics			C
17	Primary Input Panel Assy	9400135	10B	9400135	A		3	APC-UPS 3.0 1kVA	Generic			C
18	Breaker Panel Assy	21-3039-1		21-3039-1			3					C
	Station Operator Networked Area	53136-10	1	21-3040-1	A		3					C
19	Monitor, LCD, 19" Flat	5313656		5313656			3					C
20	Shelf Controller, Gamma 2000 PSA	9213656	10B	9213656	A		3	Gantry				C
	Network Interface, Secure 1000		A	9213656	A		3	Rapiscan-9400136	Proprietary		Or equivalent user-supplied	C
21	Computer System, Windows, Software, S-1000, OS	2013400	1	2013400			3	Rapiscan-2013400	Proprietary			C
	Top Level Kit											
22	Operations Manual, Secure 1000	9215600	10B	9215600	A		3					C
23	Maintenance Manual, Secure 1000	9215650	10B	9215650	A		3					C
24	Hose Supply Kit, 40M	9513200	2B	9513200	A		3					C
	Software			9513200								
25	Secure 1000 Operator Application Software	53100000-01	10A	53100000-01	A		3	Application-01	Rapiscan			C
26	Deployable Field Test Kit	9513536	10A	53100244	3.00-01		3					C
	Communications Monitor Assy		10A	9513536	A		3					C
27	PANEL MOUNT LCD - 19" SECURE 1000	1234561	1B	1234561	A		3	PM193-000	Intl. Image			C

NOTES:

1) ID's highlighted in yellow were selected by manufacturer during development.
2) ID's highlighted in blue selected by TSL-ISM or DPSCA.
Combined ID's = DPSCA

3) DPSCA - Audit performed by TSL Representatives on developmental items prior to testing to establish a product baseline

4) ID's - items were assessed based on function, performance, safety, and serviceability

5) Product Structure/Hardware Structure
Level 1 - System
Level 2 - Subsystems
Level 3 - Sub-assemblies
Level 4 - Components
Level 5 - Miscellaneous Hardware

Certificate Signature
ISO 9001

DPSCA Signatures

The above mentioned ID's comprise the units for the tested system including hardware and software.

Signature: John B Lyle Title: CM/QA AUDIT LEAD
Signature: Dirk M. Bly Title: Program Mgr

Homeland Security

Testimony of Secretary Napolitano before the Senate Commerce, Science and Transportation Committee, "Transportation Security Challenges Post-9/11"

Release Date: December 2, 2009

Russell Senate Office Building
(Oral Testimony)

Sen. Jay Rockefeller (D-WV): Madame Secretary, people are coming, I promise. And, it's just -- everyday is one of those days, right? You know a little bit about that.

Sec. Napolitano: I do, indeed.

Sen. Rockefeller: One of the things I wanted to make, which is not in my statement, is that commerce committee -- we're really glad to have you here. And we do have jurisdiction over a bunch of things like Coast Guard, TSA and then there's a bunch of sub -- other entities. And, in all, I think we have 49 percent of your full-time employees come over our, quote, "jurisdiction," or oversight, whatever you -- not jurisdiction, but oversight -- and 35 percent of your discretionary spending. So it's a chunk and I think that makes it -- it's important that you're here because they're extremely important subjects to discuss.

Sec. Napolitano: Yes, Sir.

Sen. Rockefeller: I welcome you and I thank you again for joining us today. And since the creation of the Department of Homeland Security 8 years ago, we have in Congress passed a lot of important pieces of legislation; try to make our nation more safe, more secure.

As the former chairman of the Senate Intelligence Committee, which really helps, actually, in this job, and now as chairman of this committee, I sit at an intersection between economic and national security in a very, very interesting way, and I have a deep appreciation of the many challenges that we face, that you face, and opportunities either lurking or simply on the horizon.

I'm proud to say that the commerce committee and its members were deeply instrumental in developing all or part of every major piece of legislation that the Department of Homeland Security is responsible for implementing. And we're very acutely aware of that.

During that time, our nation has made a lot of progress in transportation security, but obviously we have a lot of work that remains. A complex global transportation network and supply chain creates enormous security challenges for our nation. For whatever reason, we seem to be slow to understand that as a people, and as a government, I don't think we've done our due diligence in terms of supporting DHS, giving you the money that you need. The Coast Guard is an incredible example of that and then all of the harbor problems and everything that you're struggling -- and doing well -- but you've got money problems.

We have porous borders, both land and sea, that create a lot of inherent risk. Over the last year, I've had the opportunity to discuss the state of maritime and port security with Adm. Allen, commandant of the Coast Guard. I have an enormous regard for that man. I think he has terrific vision and perspective.

And, you know, he's very worried, and sort of reinforced my concept on a lot of things, but one of them was just the concept of small vessels. There are so many small vessels out there. What do we do about small vessels; what does he do; what do you do? I'll be introducing legislation early next year on this issue and I look forward, Madame Secretary, to

working with you as we develop that.

I also want to highlight that I remain deeply concerned about the state of aviation security, and especially general aviation security and air cargo security. In particular, we remain far too vulnerable in general aviation. I've always felt that and it's a battle where nobody ever seems to advance the ball, particularly. But I mean that whenever I've been out to Dulles airport I can never remember passing through any metal detector; I never remember having any check on anything. And that should not be. And it's sort of easy and since we all experience that, we notice it and other people would be inclined to notice that too, and they may have ill intent. I think your predecessor shared that view -- or your predecessors -- shared that view. And I look forward to hearing your views on this specific problem on the state of aviation security.

Both Congress and the administration must balance important but competing needs, maintain an efficient flow of commerce while ensuring that no terrorists can enter our country by land, air or sea. And they can, and we all know that.

I understand this balance and I am committed that we in Congress do all we can to make sure that it's achieved, and work with you to help you to make sure that it's all achieved. I understand the GAO -- the General Accountability Office -- is releasing a report for the committee today about the 100 percent scanning mandate for maritime cargo. That's something that the House is really up on.

I have my questions about whether that's doable and I want to talk about that with you because it's a very important subject and you can increase your security if we had all the machinery for it and could afford it, but you might slow down commerce, which I suppose could happen, but when you're talking about all the ports around the world, it becomes pretty complex.

The GAO highlights the enormous difficulty of meeting this mandate due to the global nature of supply chain logistics and simply a lack of technology, sufficient technology. That does not mean that we should not continue to strengthen our security protocols to prevent high-risk cargo from entering this country whether by land, sea or air, but it's a big problem.

We need to work harder to find ways to balance our security needs with our need to move goods and people efficiently. That's always the challenge. And they are not mutually exclusive; they don't have to be mutually exclusive.

You know, the two DNIs, President Bush's and President Obama's, both in an intelligence hearing in the last administration and this hearing -- of sort of global threats, both of them flat out came and said that cyber-security is the greatest threat to national security. Everything else was after that.

We hear that, it goes right through our head, we don't do that much about it, and the various agencies do, and there are, you know, 50 federal agencies claiming jurisdiction and 20 congressional committees or subcommittees claiming jurisdiction, so it's a mess. But it's a mess which stands as our major national security threat. To date, Congress has not spent as much time on cyber security as transportation security, and that has to change. That's our fault. I'm committed to making cyber security a focus for this committee and for this Congress. I want to work with you on that.

The interconnectedness between government and private industry on this critical issue cannot be ignored in the 21st century, and, again, it's the number-one threat. Two different people two years apart said exactly the same thing -- two different administrations, two points of view.

Along with Senator Snowe, I've been working on legislation that aims to address the threats that we face from cyber terrorists who intend to wreck havoc on our infrastructure. Madame Secretary, as you and I have discussed, I've called the White House to develop a national security strategy, coordinate new roles with new responsibilities across old boundaries, and the Congress and the White House and every government agency has to be a part of that solution. And that's very easy to say and extremely tough to get people to acquire the necessary discipline to focus.

We call for somebody who reports to the president -- well, that becomes controversial -- is that a czar? And I sort of don't worry about that. If people say it's the number-one national security threat, to me, that's about all you need to know.

Anyway, we have enormous respect for you. I respect you very much. Over the last eight years, your department has experienced a lot of growing pains. I know you are the right person to move the agency forward. I'm totally confident of that. I look forward to being your partner -- I think we all do -- in solving top-security challenges. And I turn now to the distinguished ranking member, Sen. Hutchinson from the state of Texas.

Sen. Kay Bailey Hutchinson (R-TX): Well, thank you very much, Sen. Rockefeller, for calling this meeting. Welcome, Madame Secretary. I want to start by saying securing our transportation network and infrastructure is essential for our

national defense as well as our economic prosperity, and they are both very important roles.

Texas is home to 29 ports, including the Port of Houston, which is one of the busiest ports in the world. It ranks first in the United States in foreign waterborne tonnage and is home to one of the world's largest petrochemical complexes as well as the U.S. Strateg ic Petroleum Reserve.

A terrorist incident at a major U.S. port could cause a devastating loss of life and deliver a huge blow to our economy. For years, I've worked with my colleagues on both sides of the aisle to strengthen our nation's port security and our transportation network. And while we have made great strides since 9/11, the Department of Homeland Security faces ever-evolving threats and still must meet numerous challenges. I want to address the transportation security officers, the screeners at airports and other places -- some places, and talk about collective bargaining. While federal law, of course, prohibits screeners from striking, allowing screeners to collectively bargain through a union could have serious consequences on the Transportation Security Administration's fundamental security mission.

I hope that you will talk about that issue and how you intend to address it because I think it is very important for us to know that our screeners will not be able to strike and will not have bargaining that causes work slowdowns and shortages and all of the things that are just short of a strike.

Secondly -- and this is something with which you have much familiarity, I know -- is the movement of goods across our land borders. This is an integral aspect of our economy and must be conducted in a secure and also efficient manner. Unfortunately, the wait times at many of our border crossings have increased while the flow of goods has decreased.

During the floor debate on the SAFE Port Act, I secured an amendment that increased the number of U.S. Customs and Border Protection officers by 275. Now, this is an issue on our land ports; it's also an issue on our water porters where, in some cases, we are having to divide a screener or a transportation border patrol person with a port and an airport in the same area. And that's not a good situation.

I welcome your views on how we can meet our resource needs along the nation's land borders, water borders and airports because I think these are the key issues that we must address. I will ask questions; I will not go further in my statement but I do also have questions about the screening of cargo at both our airports and our water ports. That's another area, as well as, of course, the land ports and the technology for that. So you have a huge job and we know that. That agency is young and it is an amalgamation of many of our security agencies. But your responsibility is also critical, so I welcome you and look forward to asking you questions and hearing what you have to say.

Sen. Rockefeller: Madame Secretary, I should say to my colleagues -- it may be both parties -- but I know our party, we're having a health-care caucus -- I think it's our 1,733rd health-care caucus -- at 11:30. And so what I want to do, with apologies to colleagues on both sides, is to head directly to you so you can make your statement, and then we'll ask you all kinds of questions.

Sen. Frank Lautenberg (D-NJ): (Inaudible, off mike.)

Sen. Rockefeller: We'd be -- they're all entered automatically into the record but the timing of this is -- Sen. Lautenberg, this is not unusual. This is the way we usually do it. When we're not pressed, we don't do it, but we do do it usually. Please proceed.

Sec. Napolitano: Well, thank you, Mr. Chairman, Sen. Hutchison, members of the committee for the opportunity to testify on the many actions that the Department is taking to secure our country and, at the same time, helping to strengthen the foundation of our economic prosperity. In the interest of time, I have submitted a longer written statement and ask that it be included in the record. But I would like to focus my opening remarks today on one particular issue -- and that is the security of containerized maritime cargo.

For years the Department of Homeland Security and other federal agencies have been working to mitigate the threat, particularly of a nuclear device being brought into the country. That was the intent behind Congress' mandate that the Department scan 100 percent of maritime cargo headed into the United States by the year 2012.

Now, when the Departm ent looks to mitigate any threat, we look to two guiding principles: first a multilayered approach to security, making us more safe than relying on any single layer. And, second, risk management as a way -- as the best way to make sure that our actions are prioritized and that our resources are focused correctly.

Now, for various reasons, it is difficult to measure in absolute terms the risk of the threat of a nuclear device being brought into the United States. But when we look at our vulnerabilities to this threat, it is clear that we are vulnerable across a number of pathways. And one of these pathways is maritime shipping containers. But there are others -- private

airplanes, as you mentioned, Senator; small boats, as you also mentioned; overland smuggling -- are just some examples.

So when we think about securing the borders of the United States, one useful analogy is that of a home. A house has a front door, but it also has a number of other possible entryways -- other doors, the windows, even the chimney. Now, here security has definitely improved at the front door -- in this case, the maritime cargo pathway. But other possible entryways also merit our attention.

So therefore, we have been building a layered approach to maritime cargo security. We collect advanced information on cargo entering the United States: who has it, where it's going, who may have had access to it, so that we can focus on higher-risk cargo. We work with partners in the shipping industry to improve their security. Once we ensure that a company has put strong security measures in place, we focus on higher-risk shipments.

DHS personnel right now are located at 58 ports in 44 other countries, working with 44 officials -- 44 -- other countries working with foreign officials to help ensure the security of U.S.-bound cargo. And, on top of these measures, there is the 100-percent scanning requirement being advanced by pilot projects at five foreign ports. Now, DHS has learned a great deal from these pilots, but it has also encountered a number of steep challenges. Some of these issues relate to the limits on current technology. Technology doesn't exist right now to effectively and automatically detect suspicious anomalies and cargo. This makes scanning difficult and time-consuming.

Available technology is also limited in their ability to see accurately through very dense cargo and density often can be the measure of something being disguised. Other challenges are logistical. Many ports do not have a single point through which most of the cargo passes, which means that 100-percent scanning would either severely slow trade or require a redesign of the port.

And, on that note, the costs of 100-percent scanning are very steep, especially in a down economy. DHS equipment costs alone would be about $8 million for every one of the 2,100 shipping lanes at the more than 700 ports that ship to the United States. So therefore, DHS is compelled to seek the time extensions authorized by law with respect to the scanning provision.

But the scanning provision has served and is serving its purpose, allowing DHS to focus on this important issue and to gain expertise in it. And so, in the view of the department, while we need to continue the current efforts, we need to address the security of maritime cargo through a wider lens: how to mitigate the threat against all potential pathways including, metaphorically, the other doors, the windows and the chimney.

I look forward to working with you and the Congress on an approach to secure all vulnerable pathways that could be used to smuggle a nuclear device into our country. Let me, if I might, just briefly mention other actions we are taking to help secure some of the other pathways into our country. These include significant strides in ensuring the security of air cargo. These efforts include work by the Coast Guard to collaborate with our partners at other ports and with the small boat community to identify potential dangers and identify a small boat strategy. Our efforts also include work with the general aviation community to devise rules to help secure the country from a dangerous weapon being smuggled here via private aircraft.

So as you can see, we are taking action, but much work remains. So I look forward to working with this committee and with this Congress on addressing this and other threats. I thank you again for the opportunity to testify. I'll look forward to addressing some of the issues that you have raised in your own statements and to answer to the best of my ability the questions that you might have. Thank you.

Sen. Rockefeller: Thank you very much, Madame Secretary. Let me start out with a relatively small thing, but which seems to be very fixable and we can be a part of that. The drug trade is transporting enormous amounts of cash via vessels on the high seas since our money laundering laws were tightened post-9/11. I understand from the Department of Justice -- and they had a big conference on this fairly recently -- there was a general agreement that we need to tighten up laws so that we can prosecute. We cannot prosecute at this point. And so, what I'm asking is that if you agree that existing laws are insufficient in order to prosecute these criminals and have you evaluated the threat with the Department of Justice and do you need additional authority and can we help with additional authority so that these criminals can be prosecuted?

Sec. Napolitano: Mr. Chairman, I think that in that connection I would defer to the Department of Justice who would have the actual prosecutorial responsibility. But I would inform the committee that we have seen an uptick in cash going by sea that is being used in the drug trade, proceeds of the drug trade -- also drugs coming in by sea. That may be an indicator that many of the measures we're taking at the land border, particularly the southwest border, are having an impact because we are now inspecting so much more of the south-bound lanes than -- way more than ever previously.

And we have dog teams, in fact, down at the southwest border that are trained to sniff out bulk cash that would be going

south into Mexico as the proceeds of the drug trade. So if there is any good news there, it may be that we're forcing these drug cartels into the ocean.

Sen. Rockefeller: All right. But, then --

Sec. Napolitano: The answer is yes.

Sen. Rockefeller: Yes. That's what I wanted. Just one more and then we'll proceed. Protecting the nation from security risks posed by nearly 13 million small vessels -- I just had no idea that there were 13 million small vessels that exist -- is an absolutely monumental task. There are parallel security threats in the general aviation sector, which I've mentioned, which has been long unaddressed as a matter of vulnerability in our aviation industry. So I want you to respond to that.

I understand that you and Adm. Allen are preparing a revised small-vessel security strategy. When will that be finished? That's one question. It's my understanding that DHS has a number of related, but not coordinated programs to address small-vessel security. How will you integrate these multiple programs into one comprehensive layered security approach?

Sec. Napolitano: The answer to your question, is the small- vessel strategy, the revised strategy will be available by the beginning of 2010. So we're well along. We have incorporated comments from the small-vessel community. We are integrating it into our strategy -- in particular for how we secure the ports -- and Sen. Hutchison, you mentioned the ports in Texas and other ports. And, again, we get to that theory of the layered-risk approach, measuring risk, layering various things. But, for example, having different checks as vessels enter the ports, particularly some of our larger ports, are some of the mechanisms that we're now using.

Sen. Rockefeller: All right. And you have the American Waterways Watch. You have the Citizens Action Network, Pleasure Boat Reporting System -- and it's all voluntary, of course. Is that in any way helpful?

Sec. Napolitano: Those are helpful, yes.

Sen. Rockefeller: But insufficient.

Sec. Napolitano: I think we need an overall strategy and we need to continue to work on the small-boat issue. I would not sit here today and tell you we have solved that problem.

Sen. Rockefeller: I thank you and Senator Hutchison.

Sen. Kay Bailey Hutchison (R-TX): Thank you, Mr. Chairman. Let's start on the collective bargaining issue. What is your view about the effort to have collective bargaining among the transportation security administration screeners and personnel?

Sec. Napolitano: Thank you, Senator. I think that we can accomplish collective bargaining and also do that in such a fashion that we never at one moment sacrifice any bit of security, that that can be built into any collective bargaining agreement. By the way, I'd like to thank the committee for supporting the nomination of Erroll Southers to be the head of TSA. Obviously, he would have a point position on that particular issue.

Sen. Hutchison: And what would be the safeguards? I mean, I mentioned earlier and addressed that -- the slowdowns, the sick-outs (ph) -- that sort of thing could have terrible consequences on our security. So what would you do to protect the traveling public from this kind of diminishment of capability if there were collective bargaining?

Sec. Napolitano: Senator, now I speak now as a former governor and a former state attorney general. There are examples around the country of collective bargaining agreements with law enforcement agencies that have similar responsibilities, where you have carve- outs, in effect, in the collective bargaining context to make sure that those types of things are not part of the collective bargaining agreement.

We would anticipate, in this context with the TSOs that we would be able to reach such an understanding. I will say, by the way, that I worked as a TSO screener last Wednesday -- the busiest travel day of the year -- and got a little bit of insight into what their life is like on the line. And I also saw a lot of different kinds of shoes.

Sen. Hutchison: Well, let me say, Madame Secretary, I appreciate that and I think they're doing a great job, because of course, we all travel so much. And I think they are doing a great job. But what about the need for flexibility when there is a threat, a crisis, where you have to do something very quickly? Is that on your agenda for protection as well, if you're going to go into collective bargaining, where someone can be called, they can work more than the established number of hours? Do you have that kind of flexibility and are you going to use it?

Sec. Napolitano: Well, the answer is yes, but I will give you an example: Even without a collective bargaining agreement right now, our TSA employees have been very eager to, whenever we've had an emergency and we need to, for example, bring more people down to help staff an airport in a hurricane, when people who work there have to stay home and work with their families because their house has been destroyed or whatever. And we have never had a problem in my experience with employees being willing to move to a place where a crisis is occurring.

Sen. Hutchison: Well, this is something that we will want to watch very carefully, because I think it has some pretty strong consequences if it's done and if it's not done right. Let me ask one more question and then I will be finished for this round. Guantanamo Bay detainees being tried in New York -- we all know that a decision has been made to do that. I have two questions. Number one, were you consulted about the security issues that would surround such a trial before the attorney general made that decision? And secondly, are you going to take extra measures during that trial to protect the traveling public while that is going on in New York?

Sec. Napolitano: Well, the Department of Homeland Security is part of the review team that President Obama established in connection with closing the prison part of Gitmo -- not all of Gitmo, but where the detainees are. And the answer is that we have been working on a host of security issues. And I would anticipate we will be working not just with DOJ, but also with the city of New York as they prepare for the trial.

Sen. Hutchison: So were you consulted in the beginning, before the decision was made to bring them to New York for trial?

Sec. Napolitano: I was not -- not in the sense of being consulted as to whether security concerns would preclude the ability to try them in New York, but I'm very comfortable with the decision to try them in New York.

Sen. Hutchison: Thank you, Mr. Chairman.

Sen. Rockefeller: Thank you, Senator Hutchison. Senator Lautenberg?

Sen. Frank Lautenberg (D-NJ): Secretary Napolitano, we are very comforted by the fact that you're in charge there. You come with a great record of public service and you've shown a firm hand since you're here. So with that, I ask two years ago, Congress acted to require 100 percent scanning of all shipping containers.

Now, one of the things that we know is that our only threat isn't nuclear, obviously. The worst attack we've had on American shores was not nuclear, but it was devastating. So we've got lots of places to look. Threats don't only exist in containers, as you have noted. Do we see any concrete improvements in cargo scanning that have been made since January of this year?

Sec. Napolitano: Well, Senator I would point to at least two. One is that at the end of January of this year, the so-called "ten- plus-two" interim rule went into effect, and I look forward to this January, when we'll see even more compliance with this rule. This is a rule that really provides shippers to provide more advance information about what is in a container, who's had access to it, who's packed it and the like that we can then use and evaluate against a number of risk measures that CBP now has.

And in addition, we have seen our ability, now, particularly with ARRA money and some other monies that the Congress has supplied, an ability to build up even more on some of our port security. And that has occurred since the beginning of the year.

Sen. Lautenberg: Let me ask you this: Since the task of securing 100 percent scanning is so monumental, is there a linear approach that says let's look to those ports that come under most concern? I'm sure that we have identified those, would we not? And but also, one of the things that I looked at -- I'm chairman of the service transportation subcommittee -- and when we looked at where we have to be concerned, we've got to look at mass transit, passenger rail -- frequent targets of terrorist attacks.

Last week, a terrorist bombing of a Russian train resulted in the loss of 26 lives. But those threats have not influenced our transportation security efforts to the level that, frankly, I think ought to be required in terms of balance. What steps are being taken now by the administration to protect those millions of Americans who daily travel by mass transit or passenger rail service?

Sec. Napolitano: Well, Senator, I'd like the opportunity to provide you with a more detailed answer in writing, because a number of steps have been and are being taken, from the deployment of grant monies to localities that operate mass transit busses -- you know, those sorts of things -- streetcars and light rail and the like. I think in terms of grants in 2010, Congress appropriated $300 million for that purpose and then the recovery act added another $150 million in FY2010. And those grant monies are being deployed. I think we are also deploying a number of portable monitors, more transit

officers, particularly in large transit hubs.

In addition, we have deployed behavioral detection officers under the so-called SPOT program, to give you just an indication of a few of the things that are happening in the land transportation environment where passengers are involved.

Sen. Lautenberg: We're out of time, but obviously, there is a lot to talk about. And I will take the liberty of inviting you in so that we can have a discussion of some of the issues. And I appreciate your service, thank you.

Sec. Napolitano: Yeah, I look forward to that. Thank you, Senator.

Sen. Rockefeller: Thank you, Senator Lautenberg. Senator Isakson?

Sen. Johnny Isakson (R-GA): Thank you very much, Mr. Chairman. Madame Secretary, first of all two compliments. I want to thank you for the tremendous effort you and the department and FEMA made in Georgia during the recent floods. I appreciate your flying down the Georgia and seeing firsthand and I have to tell you the response of TSA has been -- I mean, of FEMA has been fantastic and we're very grateful.

Secondly, we had an issue with approvals from your department with regard to African landings by Delta airlines in a number of their locations which ran into a lot of difficulty, but since that time, I want to thank you for the effort you've paid on that. I understand that things with regard to Angola and Liberia are moving along nicely. And with another request that's come -- that's all the compliments; the next things are the questions.

Sec. Napolitano: Okay, now I'm ready.

Sen. Isakson: We have a -- Delta has announced it wants to fly into Malabo in Equatorial Guinea on the West Coast of Africa, which is a gateway location. Equatorial Guinea has already issued an advance approval and is doing everything that's been asked of them, but they need assistance -- not in terms of money, but in terms of the Safe Skies for Africa program from FAA and TSA.

And in a recent meeting in Atlanta, a TSA official announced that three African countries would get that assistance. I just want to urge you to make sure Equatorial Guinea is one of the three that gets the Safe Skies Africa assistance so that, that can in fact take place as soon as possible.

Sec. Napolitano: Thank you.

Sen. Isakson: And secondly, we talked a little bit on the plane going to Georgia about AirTran and a pre-clearance request they'd made in Aruba. As you know, in a number of places, it's important for pre- clearance by Customs and Border Patrol so that people transferring back into the United States are cleared when they leave so that they can land at a regular terminal gate and leave without going through Customs and Border Patrol at the point that they leave.

That request was rejected, which I have been told -- and I don't know this to be a fact, so it's not an accusation; it's a rumor -- but that's the first time pre-clearance has been rejected by TSA. I would like to ask you, Aruba is a tremendous source of travel back and forth -- primarily vacation travel. Atlanta is a -- Hartsfield is a huge point they leave from. There are already 20 to 24 flights on a Saturday, which is the big travel day for tourism.

And it requires a little extra personnel on behalf of the department to make the pre-clearance possible, but you already have 20 to 24 flights leaving during a five-hour window on Saturday anyway, so I'd really like for that application to be looked at again and see if there's anything we can do to facilitate that.

Sec. Napolitano: Senator we'll be happy to review that application again.

Sen. Isakson: And lastly, a question. On the US-VISIT program, we require biometrics, primarily in the form of fingerprints, which are validated when someone comes into the United States by air at the US-VISIT program. It is my understanding that it is the third phase of the program is getting ready to be announced, which will also require, in terms of airport -- leaving the country, a revalidation of the fingerprint to ensure the person leaving is the person, in fact, that is supposed to be leaving.

But that's not going to be required at our seaports or at our border crossings with Canada and Mexico on the ground. And 80 percent of the people that come to the United States come either by sea or by those -- the Canadian border or the Mexican border, as I'm told. Why would we not check those borders as well, when they leave, to validate that the person leaving is in fact the person that we think they are?

Sec. Napolitano: Senator I'll get back to you, but let me just -- my educated guess is that with respect to the Mexico and Canadian travelers, that the volume, in terms of number of passengers and number of lanes is such that the logistics of

employing that for the exiting visitors at those land ports would be prohibitive. And that's really the bulk of what we're talking about.

Sen. Isakson: Well, I appreciate your answer and I appreciate your following up on both the Equatorial Guinea as well as the Aruba AirTran flight. Thank you very much. Thank you, Mr. Chair.

Sec. Napolitano: You bet.

Sen. Rockefeller: Thank you, Senator Isakson. Senator Pryor?

Sen. Mark Pryor (D-AR): Thank you, Mr. Chairman. And Madame Secretary, thank you for being here today. It's always good to see you and be with you. Let me ask you a few questions -- one about trucking, specifically trucking with Mexico.

There's been some news reports recently that have been critical of the Border Patrol's Customs Trade Partnership Against Terrorism Program, and the gist of these news reports is that some Mexican gun and drug smugglers are actually using this program because it allows the trucks to get through the border quicker and I guess with less security. Are you aware of that? Are you aware of those news reports?

Sec. Napolitano: I'm not aware of those news reports. I am familiar with the C-TPAT's program however.

Sen. Pryor: Well, there's been some that basically are saying now that the cartels down in Mexico have figured out that that's a way to get things in and out of Mexico. So I just wanted you to be aware of that and maybe talk to your folks about, you know, how valid that is and if there's anything that Homeland Security needs to do to make sure that we minimize that type of activity.

Sec. Napolitano: Oh, absolutely, because those are the kinds of programs -- again, we're always looking, you know, to improve security, but we also have the responsibility to help trade and commerce move --

Sen. Pryor: Right.

Sec. Napolitano: -- and that is a particularly difficult balance to strike at our land ports. So we will take a look at those news reports, Senator.

Sen. Pryor: Well, I agree. I appreciate that, and I know that we have had some, you know, terrible news out of Russia in the last few days, and Senator Lautenberg asked about that. And it may be a little too early to have a lessons learned based on rail security and bombs on trains, or on train tracks. But I would be interested to know as you follow up with Senator Lautenberg about, you know, what we can do better and your assessment of how secure our rail system is in this country.

Sec. Napolitano: Indeed.

Sen. Pryor: And another thing is there's been some -- let's see -- DHSIG report that has looked at FEMA's use of four primary sourcing mechanisms. One is warehouse goods, two is mission assignments, three, interagency agreements, and four, contracts. And basically, the DHIG has said that FEMA does not have a clear, overarching strategy that can guide decision making on which of these sourcing mechanisms should be used to meet a particular need. Are you familiar with that DHSIG assessment?

Sec. Napolitano: Senator, I'm familiar generally. I have not read the IG report, but I can say we have confidence that the current administrator of FEMA is addressing any and all concerns that have been raised by the IG, and he's doing it very rapidly.

Sen. Pryor: Yeah, one of the concerns I think that's raised is that in a disaster we need to make sure that we can deliver the critical commodities needed in that locality, and I think it raises a question about that. And the other thing I had for you generally in that same vein is -- I know one of the things that we've talked about in this committee previously and in Homeland Security as well is trying to make sure that DHS and FEMA are working with local and state leaders and doing a better job of coordinating with various industry groups, even like the trucking industry or the retailers or whoever it may be to try to make sure that we can all interconnect when we need to to get what we need done done at a critical moment. Are you comfortable -- are you satisfied that we have been making progress there and there's sufficient cooperation and communication?

Sec. Napolitano: Senator, I think and believe very strongly that we have improved cooperation there quite substantially, both from FEMA itself and through the Office of Intergovernmental Programs. And it's everything from regular e-mails,

conference calls, and all the rest. And that kind of cooperation, that linkage up with state and locals is absolutely key, not just on the crisis management kinds of issues that FEMA is concerned with, but also with the national and homeland security issues that we also need to be working closely with state and locals on. So the answer is yes, and that continues to be a priority of ours.

Sen. Pryor: And, of course, that ties in with the H1N1 and other, you know, pandemic threats out there to make sure we have that coordination, that preparation on the front end. Thank you, Mr. Chairman.

Sen. Rockefeller: Thank you, Senator Pryor.

Senator DeMint.

Sen. Jim DeMint (R-SC): Thank you, Mr. Chairman, and thank you, Madame Secretary, for your briefing and your service to our country. I want to focus just a few minutes on TSA workers and just a few questions related to them, and I guess they're the group we're most exposed to, as congressmen and senators fly all over the country. We're with them every week. But do you believe the current labor policies of your agency adequately protects the rights and interests of TSA workers?

Sec. Napolitano: Senator, we work hard with our employee workforce to address their issues and their interests. And so we work hard with them on a whole host of things.

Sen. DeMint: But do you think an outside agency or group are needed at this point to help establish work requirements or staffing -- standardize the staffing functions or actually help to prescribe how the workforce is managed?

Sec. Napolitano: By outside groups, senator, do you mean a union?

Sen. DeMint: Yes.

Sec. Napolitano: Senator, as I mentioned to Senator Hutchison -- and again, I go back to my experience as a governor, as a state attorney general, my familiarity with --

Sen. DeMint: Right.

Sec. Napolitano: -- these issues. The answer is, is that often times in the process of interaction with the union there are issues raised that management didn't have prior knowledge of, but in any event, all the security type issues can and are addressed, and security for an agency like TSA would always come first.

Sen. DeMint: Well, that's good to hear, and I've certainly seen, you know, the collective bargaining work at the local level when there's a close working relationship, but we're talking around 50,000 people here all over the country. What I've seen since we've implemented the whole homeland security agency -- as you know, in the beginning it was very controversial about unionization, collective bargaining. In fact, we had to suspend all that because there was a belief that with all the collective bargaining agreements we could not pull all the agencies together and do all the changes that were necessary.

One of the I think good aspects of TSA has been -- is their flexibility, their ability to change constantly and use a continuous quality improvement model step-by-step, making changes. And when you see the variety of airports and the different carriers and the different routes and all that are all over the country, the need for flexibility at almost every airport is key. And it's completely inconsistent with the collective bargaining idea that you're going to somehow standardize various aspects of work requirements and the functions. I mean, how can you unionization and collective bargaining enhance security at our airports?

Sec. Napolitano: Well, senator, the answer is collective bargaining and security are not mutually exclusive concepts, and they're done -- and these types of agreements are negotiated all the time all over the United States. And as I said before, security always is our number one interest at the department.

Sen. DeMint: Well, the concern is -- it's easier for us as a Congress to start a new agency than to try to get another one to change, a lot of times because -- collective bargaining agreements. So there's really no example of -- up here that -- of the flexibility that would be needed. The types of changes and flexibility that I see continuously going on with TSA is certainly going to change to a degree if there is a third party involved in the decision making, which there will be. I mean, there's no reason for collective bargaining if there's not some standardization or requirement to appeal to that third party when changes are made.

But my question to you is not whether or not you've seen it work at a state or local level, but the whole point of homeland

security and particularly TSA is the security of our -- of the passengers, and if -- in the beginning -- and our debate -- and every previous administrator at TSA has said that collective bargaining is not consistent with the flexibility and the need to change. You were telling us that you're going to collectively bargain, even though there's apparently no reason to protect workers. There's not any reason to standardize various work requirements. Why do we need to bring collective bargaining into this process when we see TSA making the improvements that it needs to make our passengers more secure?

Sec. Napolitano: Well, thank you, senator, for noting the improvements of our -- of TSA and the employee workforce we have there, but again, I go back to the basic point that I do not think security and collective bargaining are mutually exclusive, nor do I think that collective bargaining cannot be accomplished by an agency, such as TSA, should the workers desire to be organized in such a fashion.

Sen. DeMint: Okay. Thank you for answering my question.

Sec. Napolitano: Thank you.

Sen. DeMint: Yield back.

Sen. Rockefeller: Thank you, senator, and now Senator Warner.

Sen. Mark Warner (D-VA): Thank you, Mr. Chairman, and thank you for holding this hearing, and it's great to see my former colleague, former gubernatorial colleague, Secretary Napolitano, and congratulations, and I echo some of my colleagues' earlier comments about the good job you're doing. I want to continue on another line of questioning with TSA, circumstances happened in my state and I believe a number of other states where airports -- if they're going through renovations -- in my particular state, the Richmond Airport -- went ahead at the encouragement of TSA when they were doing a renovation and did a next generation series of improvement of inline explosive detection equipment. And TSA said go for it. Do it. They went for it, did it three or four years ago. TSA promised them a reimbursement of close to $4 billion -- $4 million. They're still hanging out waiting for this reimbursement, and this is not the only airport that's fallen into this circumstance, and I raise this with Mr. Southers when he came by before his -- when we was going through -- still going through the confirmation process.

But I just want to raise it again at the secretarial level, that there are -- that Richmond Airport is not alone in this circumstance where airports at the instigation of TSA are going through putting in next generation detection equipment, and then if TSA doesn't honor their commitment to do the reimbursement, airports on a going forward basis are not going to take this kind of step that I think is necessary. Richmond went beyond what was required, kind of went to next generation. They did it in a much more extensive way. And I just would ask your office to look into this circumstance, and the more we can get these dollars out so that airports get these commitments honored would be very, very helpful. I don't know if you're familiar with this or have heard from other airports who've raised this concern, but --

Sec. Napolitano: No, Senator, no other airports have raised that concern, but I certainly will (look into it?).

Sen. Warner: If you could look into it -- the Richmond circumstance has been now hanging out for a number of years. We found a series of other airports. This was not a one-off circumstance, but it would be something I'd love to get some feedback on.

Secondarily, again, on a parochial basis, and -- but a airport that many of my colleagues fly in and out of, Dulles, where we went through an entire new passenger screening system and put in that -- but TSA's staffing shortages still make it -- we put in the new system. Staffing shortages are there so that folks are not being served in a timely manner. I don't know if that's kind of raised your radar screen as well, but I'd ask you to look into that circumstance as well. When a airport goes ahead and upgrades their system, they've got to make sure they've got personnel to go along with that.

Sec. Napolitano: Indeed. I'll be happy to look into that.

Sen. Warner: All right. One that -- a final point I wanted to raise -- and this is one that I know you would be -- will be sensitive to as a former governor, perhaps not completely applicable in terms of Arizona, but one of the things in terms of vessel escorts -- you know, the Coast Guard has been successfully partnering for a number of years with state and local law enforcement to do vessel escorts as we've come into ports. I know in our major part in Port Hampton Roads down in Norfolk literally 60 percent of the vessel escorts have not been provided by the Coast guard, but have been provided by state and local law enforcement as transports come in. State and local governments under enormous financial stress. And I'm just hoping that if this kind of ratio is maintained not only at Norfolk, but at other ports around the country, that next year's financial budgets at most state levels are going to be even worse than the last couple years, as you I know are well aware.

My hope would be that there could be some level of financial support still given to these state and local law enforcement areas that are clearly doing part of what would normally fall within the Coast Guard's responsibility to make sure that this very successful federal, local -- federal, state, local partnership in terms of vessel escorting is maintained.

Sec. Napolitano: Senator, yes, I'll be happy to flag that as well. That activity may already be covered under some of our existing grant programs. But I'll flag it as a concern.

Sen. Warner: We've heard concerns from, again, our local folks that they may be concerned, that they're not sure if they get cutbacks in their local and state budgets that they're going to be able to maintain this kind of partnership, and that would be to the detriment of all of us. So I appreciate your attention, and again, thanks to the chairman for holding this hearing.

Sen. Rockefeller: Thank you, Senator Warner, and Senator Brownback.

Sen. Sam Brownback (R-KS): Thank you, Mr. Chairman.

Secretary, welcome. Good to see you here. Look forward to continue working with you on the -- (inaudible) -- facility, and got through this year, and we'll be focusing on next year and continuing that program to build it and to get it up and running. Seems like to me the type of hearing that we're doing now lends itself to that much more credence for a program like that where you're trying to protect a domestic industry and do the research that's necessary to be able to protect against bioterrorism, agri-terrorism, and some other facilities and things.

I want to direct your attention to general aviation if I could. It's one of the main legs of the Kansas economy. It's really been decimated lately with this economy, hopefully starting to come back a little bit. The industry is very concerned about how it is -- then you regulate general aviation, and whether or not you're going to do it in such a fashion that it can no longer really provide the service that it needs to. GA flies -- 90 percent of the airports don't receive commercial flights. They only are reached by general aviation. And so there's a real convenience factor and there's a need, and yet if it's over regulated at a point that they can't provide that service in a small airport somewhere simply because of cost -- it's cost prohibitive, it shuts it down and it makes it less viable. I know you're aware of this. October, in 2008, there was a proposed rulemaking by TSA on the creation of a large aircraft security program intended to strengthen GA's security. There was a strenuous reaction from general aviation on that. I think --

Sec. Napolitano: That would be an accurate characterization.

Sen. Brownback: Good. I'm glad you got the message, 'cause -- they were deeply concerned about it at a time when already their sales and problems were mounting, and they constantly say just don't kill us, okay? I mean, yes, we need to do -- and we will work with you on common sense things we can do. They've put in writing seven areas of suggested improvements for that rulemaking. Identification of appropriate weight threshold is one that's key to them, possibility of a trusted pilot card, if you can look at that and review -- and a review of passenger watch list, matching procedures and prohibited items. That's another one. They've got several others, but the thing they need is that -- okay, let's have the balance here.

Security is the key thing, and we've got to provide the security. But if you do it in such a fashion that they just can't cost comply with it, you're just going to shut down a bunch of airport services because they just don't have the ability to match the cost of the security with providing the service into here, that it's only so much freight that it can carry. And I really hope you can work with the general aviation industry on this, 'cause it's just -- they view it as a life and death to them on the industry in the United States, whether or not they're going to be able to continue to serve these 90 percent of the markets that don't have commercial aviation.

I don't know if you have any thought or response to that. I would appreciate your thoughts on it.

Sec. Napolitano: Well, yes, and this was an area actually the chairman pointed out in his opening comments. It has been in a way -- when we look at vulnerability, risk, threat, general aviation is a concern, that an aircraft could be weaponized or used to bring something into the country. In terms of that, the comments that we have received from GA have been very useful. We have been very -- working very closely with that community. We've also been doing some reexamination of the modeling that was used, for example, on the weight threshold. The concern there, quite frankly, is what is the weight by which -- if an aircraft were to be flown again into a building, weaponized, how much fuel would be necessary to cause a building to implode, as we saw tragically on 9-11.

So they've been looking at remodeling on that and taking into account some of the concerns or information brought forth by the GA community. Also, in terms of -- how do you regulate who gets to fly these aircraft around the country because of the possibility of bringing in material that would be of danger? So I think that working with the GA community, taking into account their legitimate concerns about the industry and the airports and the transportation needs of the

country, but also taking into account the very significant security issues. We're hoping to get to the right place.

Sen. Brownback: We need you to work with us if you can, 'cause it's an industry that's very dependent upon -- these make sensible sort of regulations that can work, but still let the industry be able to fly.

Sec. Napolitano: Indeed.

Sen. Brownback: Thanks. Thanks, chairman.

Sen. Rockefeller: Thank you, Senator Brownback.

Senator Snowe.

Sen. Olympia Snowe (R-ME): Thank you, Mr. Chairman, and welcome, Secretary Napolitano. In fact, one of my staff people witnessed your work at TSA firsthand as a screener. They said you did an excellent job.

Sec. Napolitano: Thank you very much.

Sen. Snowe: I would like to address the issue of air cargo screening, and I know that the deadline for reaching 100 percent of screening of air cargo is scheduled for August of 2010. I'd like to have your reaction to the report that was issued last week by the department inspector general concerning air cargo screening, because it does, you know, raise some significant issues with respect to securing air cargo that, obviously, raises some significant concerns in terms of those deficiencies. At this point, you have said that more than 50 percent of air cargo has been screened. Is that correct, is being screened?

Sec. Napolitano: That is correct.

Sen. Snowe: Because it wasn't clear in the inspector general's report as to whether or not that had reached the 50 percent level. They also talked about the fact that their insufficient or lack of any background checks or training with respect to the personnel handling or accessing that cargo indicated -- and they didn't give the number -- of drivers we tested were -- handled or transporting air cargo without the required background checks. Also reviewed the drivers' records and identified that 23 percent did not satisfy the required training and testing requirements. So have you had a chance to review this report?

Sec. Napolitano: I have not personally read the entire report. I've read the summary of the report. I've met with TSA about the report, as well as other members of my staff. Many of the recommendations, or many of the concerns raised in it are things that we are working on right now, and I'll be happy to provide you with kind of a progress report as to where we stand, senator.

Sen. Snowe: Do you think it's possible to reach the 100 percent deadline, 100 percent of air cargo screening by August of 2010?

Sec. Napolitano: Well, we're at about 98 percent. We're going to be at about 98 percent, so I think that we'll be very close to it, yes.

Sen. Snowe: Even though the inspector general indicated that there were a lack of personnel. There's a shortage of TSA personnel in this regard.

Sec. Napolitano: Senator, again, subject to something that -- I know where I'm sitting here right now, but I believe we will be able to accomplish that.

Sen. Snowe: Yeah, the inspector general indicated -- and this has been a concern of ours, you know, obviously, since September 11th and the 9-11 Commission's recommendations on air cargo screening, and so it's one that has languished over the years. You know, we've been determined to close this loophole, and we're -- you know, we have mandated closing this loophole. So it really is important. And I know that there has been considerable progress made towards this, and we appreciate it, but we want to make sure that we stay on target. And so given these identifiable deficiencies, it does raise some concerns.

And the inspector general indicated as well that the process is focused on quantity rather than outcomes, ensuring corrective actions. And they, you know, indicate as a result the air cargo is vulnerable to the introduction of explosives and other destructive items before it's loaded onto planes, potentially creating risk for the traveling public.

Sec. Napolitano: Senator, yes, that's what the report says. We have made, I think even before the report was issued, significant progress on many of the things that are identified in there, because, as you know, reports often lag behind

when the concerns were actually raised. And so we will be happy to provide you with a briefing on the status, but we are making great progress there.

Sen. Snowe: Okay. And I appreciate that. And one further point on this, because I think it's so essential. It indicates that "TSA is unable to properly identify and address vulnerabilities, which continue to occur year after year without an effective inspection process for ensuring compliance of air cargo." So it went on to say that "TSA misses opportunities to strengthen aviation security against the introduction of unauthorized explosives, incendiary and other destructive substances of items into aircraft cargo." So that's obviously quite serious.

Sec. Napolitano: No doubt. We have, again, some responses on that, but again, I think that the key point is are we moving to where there is 100 percent or close to it assurance of air cargo screening in the air environment? And the answer is we are making significant progress there. And we will continue to use -- that's going to continue to be a priority. And again, I look forward to the confirmation of the new TSA administrator. Obviously, having an administrator in place would be very helpful.

Sen. Snowe: Okay, thank you.

Thank you, Mr. Chairman.

Sen. Rockefeller: Thank you, Senator Snowe.

Senator Cantwell.

Sen. Maria Cantwell (D-WA): Thank you, Mr. Chairman, and Secretary Napolitano, thank you for being here and thank you for your hard work and dedication. I think the president chose well when he put you into this position, and your background and history and experience I'm sure has come into use every single day that you've been in this position. I think I could ask you questions all day. I think that is probably the result of a state that has something like 75 different ports, you know, 15 of them which are probably working ports for the interests that you care about, a border crossing at Blaine that is probably one of the busiest border crossings between U.S. and Canada in the country, and, obviously, many other related issues to that. So I'm going to try to get through these, and if you could --

Sec. Napolitano: I'll keep my answers short.

Sen. Cantwell: Thank you. The first one has to do with, obviously, the Border and Custom agents, which -- you know, we were very involved here in increasing the funding to the Northern border. We worked very hard as a delegation and a group of people to work on that for many years, and we were glad we got it. You may remember the Rasam case in which a Port Angeles border agent was able to stop Mr. Rasam, who was the millennium bomber who came through. So that was before we had the resources, and we're very well ware of the dangers there. But we've also had these incidents, and this weekend's paper I think it best. "Illegal immigrant gets $48,000 in lawsuit against border agents."

And so that's what's going on, that we have this -- I appreciate that Allen Versen (ph) visited the state, and so he's had a lot of meetings, and he's had a lot of discussions with our stakeholders, and we really appreciate that. But we just have a lot o the Border Patrol acting very far away from the border in plain clothes, catching people by surprise. In this case, the border agents, you know, in a plain car, plain clothes came up to these two individuals who were at a bus stop. Now, it's probably within that 150 miles from the border, but it definitely is not next to the border. It was in Mount Vernon, Washington, so a good -- you know, a good 45 minutes probably at least from the border.

And so what I'm asking is what steps are we taking to ensure that the border agents don't engage in racial profiling and that all the Department of Homeland Security agencies are targeting the most significant threats at the Northern borders?

Sec. Napolitano: Well, obviously, racial profiling is repugnant to the law, and we do not racially profile. And that is part of our training, it's part of our supervision, and it's part of the ethos. Secondly, a good border policy requires several things. It requires trained personnel on the ground who are properly supervised, it requires technology, and in some instances it requires infrastructure. And so both at the Northern and the Southern borders what we are about is having strategies for those borders that meet the fact that they're different types of borders, different terrain and all the rest, but nonetheless that combine in a strategic fashion those three elements.

Sen. Cantwell: Well, I think we need to continue to have dialogue in the Northwest of what's going because I think when we end up seeing lawsuits being settled against border agents I think we have issues here that we need to address, and we appreciate your cooperation in working on that. A second issue, if I could, is obviously that that U.S.-Canadian border is very important for shipping and we've had by colleagues talk about security and safety of cargo and container traffic. What are we doing to help ensure that all of North America adopts a regime for border security so that we don't have Asian traffic deciding to go to Canada because they can skip the regime that the United States sets up for border security,

only to have that cargo travel all the way across the country and maybe enter, you know, someplace else that doesn't have that border security that you are establishing? So how do we get that North America regime established?

Sec. Napolitano: Well, if you're talking about, Senator, having almost like a perimeter policy around the continent, obviously that's somewhat difficult but I mean --

Sen. Cantwell: I'm saying there's billions of dollars of business -- of cargo container going in. We're probably, you know, 20 percent of all traffic coming from China. Now, if just up the road in Vancouver they decide they're not going to -- (inaudible) -- a security regime and it's cheaper and faster to go through Vancouver, all that traffic is going to go there and the U.S. is going to lose that transportation business. So what are we doing to help make sure that those ports adopt the same kind of regimes?

Sec. Napolitano: Well, I think, Senator, we are -- I am meeting regularly with my colleague -- my counterpart on the Canadian side -- as to what is necessary for security at those ports because there are certain things that are constants with respect to be it integrated port security, be it air security, be it land-border security. There are certain things that need to be done and need to be accomplished. But there are differences and there are very real differences between the two countries and I think part of that gets beyond my lane and gets into other departments in terms of negotiations as well.

Sen. Cantwell: Thank you. I see my time has expired, Mr. Chairman. Thank you.

Sen. Rockefeller: Thank you, Senator Cantwell. Senator Klobuchar?

Sen. Klobuchar: Thank you very much, Mr. Chairman. Thank you, Madame Secretary, for being here. I was just thinking of how full your plate is with H1N1 and the many other issues that you've had -- the Fort Hood shooting investigation and a lot of other ongoing changes with our security. So I thank you for your leadership and also the leadership you showed when we had the floods in the Red River Valley, which you remember involved not just North Dakota but Minnesota.

Sec. Napolitano: Minnesota.

Sen. Klobuchar: Very good.

Sec. Napolitano: Right across the river.

Sen. Klobuchar: Exactly. I'm actually going to mostly focus on the Secure Watch issue and some of the terrorist watch lists and the misidentifications on those lists but I wanted to start with one quick question about the Canadian baggage rescreening, and this is something that affects my state. We have a state-of-the-art airport and the requirement that checked luggage at appropriately-cleared Canadian airport facilities be rescreened before the transfer to a U.S.-based connecting flight it has frequently caused delayed connections for our passengers arriving (since?) Canada because their baggage has to be physically transported from the arrival. And I know that TSA has been working with Canadian authorities for well over a year to reach an agreement that could put in place new technologies for Canadian baggage screening that would meet our own United States security standards, and I wondered if you have any sense of when that agreement will be reached.

Sec. Napolitano: I know about the issue, I know about the discussions, and I don't know when they will come to a conclusion. But if, Senator, if you're asking me to see if I can prompt them to hurry up, I'll be happy to do so.

Sen. Klobuchar: That's a great answer. Thank you. The watch list redress problems -- one of my primary concerns -- and I get to know the TSA people very well at my airport and have had very good relations with them since I have a hip replacement so I talk to them every time I'm through the airport and they do a good job -- but my question was about the no-fly lists, and last year in response to reports that thousands of U.S. travelers experienced misidentifications each year I introduced legislation to require the Department of Homeland Security to establish a comprehensive cleared list for innocent (travels?). The implementation of the Secure Flight program has been underway for nearly a year now and TSA officials continue to stress that once the program is fully operational these misidentifications will be minimized, and you say in your testimony that 18 air carriers have successfully switch to Secure Flight and that testing is underway with an additional 27 air carriers. For the air carriers that have not fully switched to Secure Flight how are passengers being screened against the watch list? How do you think this is going? We're still, obviously, having some problems.

Sec. Napolitano: Well, Senator, if they're not in Secure Flight and, again, that is a successful program and I think it demonstrates how as our department matures but also as technology gets better and also as we get a better sense of what actually needs to be done and what's value added to security some of these things do get dealt with. But Secure Flight is going to cover the vast majority of passengers by the time of its full implementation. Right now, we're in that transitional status and those passengers that are not on a carrier that has moved over are still being measured the old-fashioned way

but we've also implemented some computer software, for example, that helps us segregate out often misidentified names, misspellings of names, and things of that nature, and we have also worked to speed up the and make easier the appeal process so --

Sen. Klobuchar: Mm-hmm.

Sec. Napolitano: -- people can get de-watch listed.

Sen. Klobuchar: Right, and -- but one issue that still remains the Department of Homeland Security inspector general recently reported that passengers who encounter misidentifications and seek to use the Traveler Redress Inquiry Program -- named TRIP -- to clear these problems they said generally do not benefit from their participation in TRIP. Their cases often languish for extended periods of time. The IG made 24 recommendations and one of the main problems highlighted was that the cleared list of travelers who have gone through the TRIP process is used by airlines only sparingly to rule out false positives on the watch list.

You have to understand in our state we have a kid that was going to Disneyland who couldn't go -- he was like two years old -- because his name was on the watch list. So we've had a lot of concerns. We -- I think we have a lot of common names in Minnesota. We have a lot of Johnsons and things like that. So we continue to be concerned. So do you know what's happening with the IG's recommendations on the TRIP program?

Sec. Napolitano: Senator, let me get back to you on that. I know that we constantly are working to make those sorts of things more consumer friendly, more passenger friendly. But I'll get back to you specifically on that.

Sen. Klobuchar: All right. Thank you very much, again, and thank you for your leadership. Yield back.

Sen. Rockefeller: Thank you, Senator. Senator Udall?

Sen. Tom Udall (D-NM): Thank you, Mr. Chairman, and thank you for holding this hearing. Good to see you here, Secretary Napolitano. We both share the Southwest as home and I think you're doing an excellent job with a very, very difficult department there to manage. I'd like in my time to hit a couple of areas -- one is Real ID and then the TSA approach to whole-body imaging.

As you know, more than 30 states incl uding New Mexico are unlikely to meet the December 31st deadline to become materially compliant with the Real ID Act of 2005.

While I understand the administration would prefer to enact Pass ID Act in lieu of granting an additional extension, the uncertainty surrounding what your department may or may not do if the legislation is not signed into law is creating confusion for people in the state that are not in compliance. This is -- and I'm sure you've heard a lot about this too -- this is causing a great deal of anxiety with the constituents who are seeing news reports they'll need a passport in order to travel on a commercial airline in the U.S. after the 1st of the year. I believe Senator Bingaman and I sent you a letter on this issue on Monday. Will you commit now to extending the deadline for compliance with Real ID if Congress has not addressed the issue by December 31st?

Sec. Napolitano: Well, Senator, thank you, and yes, I -- here is the problem. Congress passed Real ID as a footnote in an appropriations bill and that did not have the benefit of hearings nor consultation with the states, which caused vast revolt among the states of which Arizona was one, and so we went and worked with the governors on a bipartisan basis to fix Real ID and that gave birth to a piece of legislation known as Pass ID. It has been through committee. It's been marked up. It is ready for floor action. It deals with a lot of the issues that -- it solves the governors' problems with Real ID.

I would -- before I get to the question of extensions, one of the reasons we had Real ID and now Pass ID is because the 9/11 commission had a recommendation that we improve the security quality of driver's licenses, and because Real ID has been rejected by the states just by granting extension after extension after extension we're not getting to the pathway to have more secure driver's licenses. Pass ID helps us meet the 9/11 commission recommendations and at the same time addresses issues that were legitimately raised by the states. And so what I would prefer to urge the Senate to do and use the -- this hearing as an opportunity to really urge it to do is to move to floor action and move Pass ID through so we can get it over to the House. I think it could go very quickly over there and we could solve this issue, as opposed to extension after extension, which not only doesn't deal with the 9/11 commission recommendation but it's just another year of uncertainty.

Sen. Udall: Yeah. Well, as you are probably aware, the situation that we're in now -- we have health care on the floor -- where if tried to move to anything else I think it would make it much more difficult procedurally. So I think if -- I don't see us getting to Pass ID on the Senate floor between now and the end of the year. So I think it would be very helpful for

you to issue a statement -- you might use this as an opportunity to do it -- to assure people that after December 31st they will be able to travel with something other than a passport. I don't know if you want to do that at this point but if you decline that's fine.

Sec. Napolitano: I think I will not accept that invitation at this point in time.

Sen. Udall: Okay. Okay. Thank you. I probably don't have enough time to get you to answer the question but on whole-body imaging let me just lay it out a little bit here. You're -- TSA's greatly expanding its use of whole-body imaging for primary passenger screening at airports, and Albuquerque is one of the airports where it's doing that. And although TSA has voluntarily taken certain measures to protect passenger privacy, I believe several serious questions should be answered before TSA deploys these whole-body imaging machines more widely, and one of the issues really is if you decline the machine you get a full-body pat down, and as you can see, that could -- you either one of the other -- that could be very intrusive. So I -- I'm going to submit the questions to you because my time is up and I know the chairman may want to get to other senators here. But I hope that you'll give us a prompt response on that.

Sec. Napolitano: Right, and Senator, in the airports I've been at observing how that technology is used and there's been a -- that technology is much different than as portrayed in the press. But in any event, it hasn't been a pat down but you go through the standard magnetometer process. So -- but we'll be happy to answer the questions that you have.

Sen. Udall: We'll get you all that information. Thank you very much. Thanks for your service.

Sen. Rockefeller: Thank you, Senator Udall. Madame Secretary, I'm going to ask you a question, which you can't answer but you want to, desperately. But --

Sec. Napolitano: Okay.

Sen. Rockefeller: -- but you can't because OMB won't let you. Okay. I'll just -- I'd catch your attention by -- (inaudible) -- okay.

Sec. Napolitano: Yes, you have.

Sen. Rockefeller: The -- to me, one of the most enormous problems of your extraordinarily important agency -- I mean, the president spoke last night and he kept coming back to (what?) the economy I really want to build is my country's economy and he really had to do that -- and I (sort of ?) wanted him to say, and by the way, in protecting security we really need to do much more with the Department of Homeland Security, give it more resources. I think it's one of the great anomalies and, frankly, embarrassments to us in the Congress and to -- (inaudible) -- that they have underfunded you. I mean, everybody loves to pick on FEMA or whatever is going on, but often the reason is or they give you they say you got to have 100 percent container scanning, air cargo, maritime cargo, you know, and then 10,000 more rules and regulations have to pour out of your organization. And it's just -- it's an awful way and you are responsible in so many ways for our national security.

I mean, the intelligence people aren't; you are. They're meant to provide information, and you have your own intelligence folks.

But you need money -- and the question I want to ask you is how much money do you need? And what do you need it for to be able to do what you are required to do, and what you want to do? You'll never get another question so wonderful as that.

Sec. Napolitano: Thank you Mr. Chairman. Let me just address it in the following fashion, which is to say one of the things that I have set about to do as the secretary is to identify the major mission areas of the department, to align our budget request with those major mission areas. And to create a longer-term vision for the Department, through the Quadrennial Homeland Security Review process.

Congress asked us to complete that QHSR by December 31. We are on track to do so. But here's the -- the major mission areas of the 22 agencies that were combined really involve counterterrorism, securing the air, land and sea borders, immigration enforcement while we work for immigration reform; and preparation for, and the ability to respond to disasters of any type -- natural disasters.

And what we have been about doing is prioritizing under each of those and aligning our budget request accordingly. And I hope --

Sen. Rockefeller: Madame Secretary, I know what you're doing. I applaud you for it, but it's not helpful. I mean, you're laying out your priorities. And what I would say is that you're then applying totally inadequate resources to your

priorities because you don't have any choice. And you can't say much because OMB vets your testimony as they do with any cabinet secretary and way on down too. And most people don't know that, that you can't speak your mind.

Well, I don't want to get you fired. But I really do want Homeland Security to have the money it needs. And at some point, maybe we'll have -- maybe you can leave a private letter and stick it under my office door or something. But it counts to us; it counts so that we can put pressure on appropriators to be helpful to you. I'll just leave it there because you're in an impossible situation.

Sec. Napolitano: Thank you Mr. Chairman.

Sen. Rockefeller: I did not want to leave Senator Brownback's -- you know, if you do any regulation of general aviation, the business that will collapse. I just can't let that pass. General, I think you mentioned 90 percent of airports in Kansas or whatever it was were small airports. And therefore, the use of general aviation is convenient. Yes, it certainly is convenient, it's probably convenient to a lot of people who are running drugs and running guns, and all kinds of things. But we can't do anything to increase their screening.

Again, out at Dulles, the idea of walking through something which -- a machine that that lady I guess walked through, who crashed the White House party the other night. They don't even have them out there. They don't even have them. So at any given moment, two-thirds of the airplanes in the air are general aviation. They get all of this attention from air traffic control, just as much as any commercial air passenger.

And yes, Kansas makes a lot of general aviation aircraft. But there is also the question of national security of them -- you pointed that out. They could have fuel on them; they could have run into buildings. I'm pointing out that they could be running drugs, they could be running guns. And we don't know about it. And so, we can't touch them. They're untouchable because if you touch them, they call up all the senators and congressmen who ride on their general aviation things; and say don't you dare do anything with it. And that's exactly the way it works.

I mean, I tried to put a 25 cent per trip tax on them last year to help pay for our air traffic control system. That got four inches down the football field. The telephone calls just squashed it immediately. And at some point, this becomes just a little bit more than annoying when they become somehow sacred because they're fragile. They're not fragile, they're doing vey well.

Whether they're doing well or not, is secondary to the national security concerns that you would have; and that I certainly do have about them. And I just wondered if you would comment on that.

Sec. Napolitano: Well senator, as I suggested to Senator Brownback, the security issues involving GA, general aviation, need to be addressed. There was a proposed rule. It had a strong reaction from that community. We have worked with that community. We are in the process of finalizing that rule.

But I agree with you, that when I look at the overall kind of vulnerabilities and threats involving threats to the homeland; particularly with respect to the larger, general aviation aircraft there are security interests that must be protected. And we are moving to do just that.

Sen. Rockefeller: How do you do that? They resist that.

Sec. Napolitano: We do it by -- through the regulatory process, and we do it --

Sen. Rockefeller: Then, how come I don't see it?

Sec. Napolitano: Well, because we haven't finished the rule yet. But we will be doing it through a variety of mechanisms.

Sen. Rockefeller: I advise you to be bold. My time has run out.

Senator Hutchison.

Sen. Hutchison: Thank you.

I wanted to go back to the border wait times. This is something that I know you are familiar with as well, having been the governor of Arizona. And my question is how can you address the border wait times; because there are trucks backed up for miles, taking hours to get through? Because it does make a difference in commerce, and people being willing to come across. How are you going to address it keeping security in mind as well as efficiency of commerce on our land borders?

Sec. Napolitano: Well, a couple of things. First of all, between Fiscal Year '08 and Fiscal Year '09, we actually saw a reduction in wait times, according to the data I have, a 12.3 percent reduction. And the wait times for commercial trucks, and I think that's what you're focused on, Senator, went from in '08 10.6 minutes to 9.3 minutes on the U.S. side of the border.

Where the wait times can add up is on the Mexican side of the border. And so, working with Mexico, they are now establishing their own customs capacity on that side of the border, which I think will do a great deal to resist. Because as you know, when you go through a land port, you're actually going through two borders. You're going through the Mexican side and the U.S. side. So the U.S. side, the wait times have gone down; and I think will continue to go down with our greater use of technology.

Sen. Hutchison: I really am referring to the Mexican side, because that affects so many of our border retailers. And it's commercial, but it's also people who will shop --

Sec. Napolitano: In those areas, indeed. And so, Mexico is now developing its own customs agency and deploying them to the border, which they really had not had before. As well as, as we build out our ports on the northern side of the border, we are working with them to build their infrastructure to match our ports so that they're paired up appropriately.

Sen. Hutchison: So, we do have an ongoing effort to work, to coordinate better the Mexican side with our side. So that we can get some of those wait times down for commerce.

Sec. Napolitano: Yes.

Sen. Hutchison: Okay. It's a big deal on our border. It must have been in Arizona as well. Because border retailers on our side, get a lot of business from that land traffic. And if you have to wait an hour or two, or more sometimes, it's a problem.

Is there something we need to do to increase further customs and also coordination because there has been a complaint that's ongoing for a long time of coordination of just working hours between DEA, Customs and Border Patrol? So that sometimes, one group is off in a coffee break, while the other group is on, but you have to have all of them. And is there an effort in your department to address that kind of coordination to better utilize our resources?

Sec. Napolitano: Senator that coordination should already be occurring, under the direction of who ever is the manager of the port. If you have a specific instance or a specific port where you are getting reports that that is not happening, I hope you would let me know about it; and we will follow-up.

Sen. Hutchison: Okay. I will do that. Thank you very much.

Thank you Mr. Chairman.

Sen. Rockefeller: Thank you Senator Hutchison.

Senator Cantwell.

Sen. Cantwell: Thank you Mr. Chairman. Thank you for allowing me to ask a second round of questions.

And Secretary Napolitano, again thank you for your service and all your hard work. I'd like to submit a question if I could to you about semi-submersible vehicles that are being used in the drug trade. And my understanding is and growing in numbers.

I don't know if we've thought about that as it relates to security, since these are one-way vessels and they can be used for drugs; they could be used for other things. But I'm going to submit that for the record and maybe get an answer from you.

But I'd like to bring up two specific cases that have been really receiving national attention and see if I can get your help on that. The first is Ernesto Gamboa. He was an individual who served as a confidential informant, and for the past 14 years assisted law enforcement in the dismantling of large and dangerous drug operations.

He frequently put himself at risk. He worked with the Washington State Patrol, the Federal Bureau of Investigation, the DEA and INS, and with the Bureau of Immigration and Customs, ICE. So his cooperation was critical to the success of federal prosecutors in seizing hundreds of pounds of cocaine and methamphetamine, as well as large seizures of money and weapons.

During all the time that he was cooperating with law enforcement over that time period, he was promised that he would get help with his immigration status. But instead, in July he was detained by ICE and placed on removal, despite all of

the good work that he had been doing previously for these various agencies.

And so I'm expressing concern over this case because he's kind of in limbo. He can't work because he doesn't have paperwork, and he can't get -- if he is returned to El Salvador, I'm sure he will likely be killed. And so if we don't help the Gamboas, who have been the informants for us, how are we going to recruit other people to helping us with finding drug traffickers and criminals? And so I would, you know, ask for your help in this case in understanding what we should do with Mr. Gamboa.

Sec. Napolitano: I'll be happy to look into it. This goes to the intersection between the Department of Justice and the Department of Homeland Security, where the Department of Justice, DEA, doesn't have authority to make immigration representations. Sometimes that gets lost in the shuffle. DEA needs to bring ICE in, or vice versa sometimes. So I think that illustrates perhaps what is happening with Mr. Gamboa. I'll be happy to look into the situation.

Sen. Cantwell: Thank you.

The second one is a case, Alonso Chehade, who -- you know, we talked about this border issue in my first round of questioning, and Senator Murray and I have asked you for the removal of Alonso Chehade until the end of the 11th Congress. He is a case that would be -- if the DREAM Act was law, he would obviously have the relief of that legislation. But he's a 22-year-old Peruvian national who resides -- who's resided in the United States since childhood. And earlier this year, he literally took a wrong turn on I-5 and was detained when he accidentally crossed into Canada. And so now he faces deportation.

He graduated from high school with honors, attended Olympic Community College, earned his bachelor's degree from the University of Washington, and so it's generated a lot of media attention in our state. And so I'm hoping that we can defer action on his case until the 111th Congress to see if we can get the DREAM Act passed, and so maybe Mr. Chehade, who has come to the United States as a child, not of his own doing, but has now been through our whole education system, will, not because he took a wrong turn on a freeway, be able to stay in the United States.

Sec. Napolitano: I think his removal will be or has been deferred. I will double-check on that, Senator. But the situation you describe illustrates why President Obama is eager to have the Congress take up the whole issue of immigration and immigration reform. These situations happen in my department every day, day in and day out.

Sen. Cantwell: Well, I appreciate that, and I appreciate you looking into this further. I think he's gotten a temporary deferral, but I think that'll run out in January.

Sec. Napolitano: That may be right. I'll take a look.

Sen. Cantwell: If you could, thank you.

I thank you, Mr. Chairman.

Sen. Rockefeller: Thank you, Senator Cantwell.

Senator McCaskill may be on her way. In the meantime, I have one more question to ask.

Are you okay on time?

Sec. Napolitano: I'm fine.

Sen. Rockefeller: Okay. This is cybersecurity. And this doesn't appear to be a very important question, but it is to me. Again, I go back to George Bush's director of National Intelligence, Barack Obama's director of National Intelligence, citing the number one threat to this country is not al Qaeda. It's not dirty bombs. It is cybersecurity -- huge importance, more or less ignored by the press, a somewhat disinterested public in that because they can't wrap around those two words. And you have some responsibility for that. Now, my question is very specific, and you may not want to answer it, but I want to tell you how I feel about it. You all had a big conference and you decided that you'd get somebody who would report -- to be responsible for cybersecurity, but report to the National Security Council and to the National Economic Council, to which I say goodbye focus on cybersecurity. I mean, I've been through that trip before. I've seen what happens. It just -- you know, by the time the Pentagon takes their chunk, you know, it won't work.

Senator Snowe and I are working on legislation. We'd like to work with you on it. We say that there ought to be somebody who reports only to the president. Now, there's that part of this -- "Oh, there's another czar," to which I would say, "Well, if that's another czar, then that's the one you want to have," because that's the number one national-security threat to our country, and will remain so.

People have no idea what they can do. They read about it. It hasn't happened in their community, so they forget about it and go on and concentrate on al Qaeda and Taliban and, you know, all kinds of things, but not on cybersecurity, which is the main threat.

So I want to say to you that I feel very strongly that there ought to be somebody who reports directly to the president, has that responsibility, who doesn't try to mix the military, the intelligence and the National Economic Council, because he'll wander off into nothing being done or money not being spent.

I think when you have somebody who reports to the president, it's like the Office of Science & Technology. That's not an -- Dr. John Holdren is not an agency. He's a free floater. He can walk in and out of the Oval Office any time he wants. But he's doing science and technology, which just affects everything we do in our country, including cybersecurity.

Sec. Napolitano: Indeed.

Sen. Rockefeller: And I think that -- I think we ought to have somebody who reports to the president. I want to say that loudly and clearly to you. You don't have to respond if you don't want to that view. I think the idea of having a lesser (statute?) with a more diverse number of bosses is a very bad idea and that we won't make progress, because it's the one area of national security where the public really isn't there yet. The press isn't there. They're not interested.

It's yesterday's news story. Somebody hacks into something and then you get two or three days and it's gone. And it's a terrible threat, terrible thing to do to this nation. So I want to make that statement. If you'd care to respond to it, I'd be happy. But that's what our legislation is going to say.

Sec. Napolitano: Well, Mr. Chairman, I think I'd be happy to work with you on that legislation. I think your assessment of cybersecurity as a threat is an accurate one. I would be happy to brief you and your staff on the extensive efforts we have taken within DHS to deal with the civilian side of government and the protection of that, the .gov side, as well as our interaction with the private sector.

You know, 85 percent of the critical infrastructure in the country is in the hands of the private sector, and they're totally network-dependent. You think of utilities, water companies. And I could go on and on and on. I know you understand what I'm addressing.

And so we have been involved in a series of critical infrastructure meetings over the last two months, myself included, with the private sector with respect to their own network security and how we work together to improve that. So I couldn't agree with you more about the severity and nature of the threat, and I think it is going to be part of our ongoing threat environment.

Sen. Rockefeller: I think the private sector will be helpful, but I have to -- and this is not really quite fair of me, but about 10 years ago I was worried about that and generally about power plants and chemical plants that had backed up to the Ohio River. And if you go between Pittsburgh and the Allegheny River down to Cincinnati, that's about 200 miles, or maybe it's 300 miles; I have no idea, but it's a long way.

And there are hundreds and hundreds of power plants and chemical plants, and three Coast Guard cutters that have, you know, machine guns on the front, heavy machine guns -- three. They can't go 24 hours a day, so that means there's an average of one every eight hours to patrol all of the Ohio River. This is what I'm talking about when I say please ask me, do you need more money for that, because it obviously can't do the job.

Anyway, I got them together and I said, "You've got to improve your security. You're backed up against the water. That's exactly where the terrorists will come at you. If you're a power plant, you have these big cooling things. They can drop things into that." There's the way for chemical companies to be blown up. I mean, we've had incidents in West Virginia that had nothing to do with terrorism. They were just accidents. And they're just massively threatening.

And so they agreed to do something. And then they -- this is slightly cynically put, but it's the way they look at it -- they came back a year later and they said that they'd given everybody who admits people into the workspace -- that is, where their cars pass through -- a sidearm. Well, of course, that's the opposite side of the plant. The river is on the other side of the plant. It has nothing to do with what I'm talking about.

So to the extent that the private sector is willing to be helpful on something like cybersecurity or other forms of security, it always makes me just a little bit suspicious, because, as Senator Brownback said, it costs. And everybody's feeling very fragile and everybody is very fragile, but this is -- you know, this is the big one as far as the director of national intelligence says.

I don't know if you have any comments.

Sec. Napolitano: Our interactions on the cyber side with the private sector to date have been, I think, very productive. And perhaps it's because the economic costs of a major denial of service attack or a virus is substantial enough that there are incentives there for everyone to work together.

But this is an evolving field; it's an ever-changing threat environment. And again, it's something that I think we will be dealing with for months and years to come.

Sen. Rockefeller: Okay. Yeah. Well, it appears that Senator McCaskill will not be coming. So I will --

Sec. Napolitano: You want to --

Sen. Rockefeller: Use her time.

Sec. Napolitano: Okay.

Sen. Rockefeller: So bear with me one more time.

Can you please walk me through the challenges that you face as you attempt to implement 100 percent scanning requirement? And I have these photographs.

And you know, I'm talking now about maritime. Air -- I mean, water cargo containers. And some of them, you know, everybody in the House wants them scanned -- 100 percent. You're doing about 5 percent, I think. And some of them, there has to be more than that.

For example, just to pick out Home Depot. I mean, maybe every -- probably every Tuesday at about seven different ports around the country, massive cargo containers of lumber come in. And that's predictable -- totally predictable. Thinking somebody hides something inside -- a dirty bomb inside that -- and does that require scanning? Then you have -- things are wrapped in plastic and then they have wrapped in metal. And they have locks and people say, well, that's good, except you can blow up the locks. Well, to blow up the locks, I think, would probably be a fairly noticeable event. And so help me understand your view of what you can responsibly and should responsibly do and what you should not cost effectively and potentially responsibly do?

Sec. Napolitano: Thank you, Mr. Chairman.

Well, I'd begin by saying that we should not believe that 100 percent scanning equates to 100 percent security. And that is because, as I mentioned before, the 100 percent scanning rule only focuses on one method of delivery and in one place. And there are numerous methods of delivery in numerous places. And so that is why we really have to take a more nuanced -- nuanced is probably not the right word -- but a layered, risk-based approach to these issues.

But, for example, the technology really isn't currently available. To name just one problem: We have a high rate of false positives. The logistical challenges and costs of deploying --

Sen. Rockefeller: Is it because the technology's insufficient or because it reads and confuses?

Sec. Napolitano: It reads and -- it reads and confuses. You have a high level of false positives. The speed of the through-port is very slow. You have lack of adequate anomaly detection. You have -- even if you had a good technical system, recognize that you're dealing with 700 different ports around the world. Having an adequately trained work force and the maintenance of these systems is an issue.

You've got a trade issue. Most -- many countries around the world are very -- not just resistant to, but in some respects almost offended by the notion that we would install -- you know, require this at their port in their country. So you have to negotiate each of those agreements separately. So there's always the possibility of a retaliatory type of approach.

There's the additional cost to the shipping system. There was a study done recently in the EU that this could add as much as 10 percent to shipping cost, which in an era of a fragile global economy is a significant add-on.

So I hope that gives you some of the picture of the difficulty that we have implementing 100 percent scanning rule.

Sen. Rockefeller: It's very helpful. And I asked that question, actually, because it was so important that Senator McCaskill get there. Therefore, I had to tread water as best as I could. So she can now ask a couple of absolutely brilliant questions.

Sec. Napolitano: Well, I'm glad you asked it, because I studied my answer really hard.

Sen. Rockefeller: Senator McCaskill.

Sen. Claire McCaskill (D-MO): Thank you, Mr. Chairman.

I appreciate you holding the hearing open until I had a chance to get here. I was over in Armed Services as we were dealing with the president's speech on Afghanistan last night and it took awhile for me to get my questioning done there.

I wanted to briefly bring up with you, Secretary Napolitano, something that I have been working on for a number of years now and that is foreign repair stations as it relates to airline maintenance.

I know this is not necessarily in your lane, but in the long run, it needs to be on your radar -- pardon the pun --

Sec. Napolitano: Mm-hmm.

Sen. McCaskill: Because we have increasingly in this country turned to foreign repair stations for not just kicking the tires, but significant maintenance and repair work for our domestic airline industry.

FAA -- it is from the many different hearings in this room we have figured out we're not really sure we certify certain repair stations, that we allow non-certified repair stations to do the work. We're not really sure why we don't have the same kind of standards at foreign repair stations in terms of background checks, in terms of perimeter security.

And I bring it up to you, because I think this is something that we could benefit from you -- your people taking a look at this. We have foreign repair stations doing significant work on some of our airlines in countries that were on the State Department's terrorist watch list.

So meanwhile, I -- with a smile on my face -- get wanded every time I get on an airplane, because I have one artificial knee and they go through my mom's stuff, because she has two artificial knees. We have repair work -- significant repair work being done in places around the globe where I don't think the American people would be comfortable with the level of security and oversight that we're providing them.

And I wanted to bring it up to you, because it's something that I'd worked on and I know we haven't had a chance to visit about it before, but would like your reaction to that and whether or not you think that some of your obligation, as it relates to homeland security, could reach out to at least do an assessment, in your view, whether or not this is something we should be worried about.

Sec. Napolitano: Well, thank you, Senator. And the foreign repair issue really reveals something, which I say often, which is that homeland security does not begin at the borders of the United States. You really have to think of it in a global context and then bring it home, so to speak.

On November the 18th of this year -- so just a few weeks ago -- we issued an actual notice of proposed rulemaking on foreign repair stations. And it builds on the certification requirements that the FAA uses. But it would require such things as making -- requiring that they be open to audits by the Department of Homeland Security on a random and surprise basis. It requires certain types of recordkeeping. It requires certain types of -- other types of checks in the stations themselves.

The comment period on the notice, I think, closes -- I want to say the third week of January. So it is something that has occupied our attention and we're moving forward in that fashion.

Sen. McCaskill: That is terrific.

I know you've got to go and I appreciate you sticking around till I got here.

I also do want to bring up -- I am hopeful that you all are looking at the security Clearinghouse contracting issue as it relates to a re-compete. Those costs have gone up. I'm sure you're aware a security check has risen from $3 a head to $27 a head. For many of our airports that are struggling right now in this economy, it has gotten to be a very expensive proposition.

And I know you all -- TSA has not gone on record yet affirming that it will open the contract to competition, but I wanted to go on record as saying I'm hopeful that you all will move towards a competitive contract as quickly as possible. I think this has been a sole source for way too long and I think we're paying more than we need to pay.

Sec. Napolitano: Duly noted.

Sen. McCaskill: Thank you very much.

And thank you, Mr. Chairman.

Sen. Rockefeller: Thank you. Senator McCaskill.

And you have an appointment and a flight to catch. I totally thank you for being here. It's very important to us as a committee. We respect what you're doing and we want to be your partner.

Sec. Napolitano: Thank you, Mr. Chairman, for the opportunity to be here today.

Sen. Rockefeller: Thank you. The hearing is adjourned.

###

This page was last reviewed/modified on December 2, 2009.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds

- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

GAO

United States Government Accountability Office

Statement before the Committee on Commerce, Science and Transportation, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, December 2, 2009

HOMELAND SECURITY

DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity

Statement for the Record
Cathleen A. Berrick, Managing Director
Homeland Security and Justice

GAO
Accountability * Integrity * Reliability

December 2, 2009

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-10-106, Statement Before the Committee on Commerce, Science and Transportation, U.S. Senate

HOMELAND SECURITY

DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity

Why GAO Did This Study

Securing the nation's transportation and information systems is a primary responsibility of the Department of Homeland Security (DHS). Within DHS, the Transportation Security Administration (TSA) is responsible for securing all transportation modes; U.S. Customs and Border Protection (CBP) is responsible for cargo container security; the U.S. Coast Guard is responsible for protecting the maritime environment; and the National Protection and Programs Directorate is responsible for the cybersecurity of critical infrastructure. This statement focuses on the progress and challenges DHS faces in key areas of maritime, aviation, and cybersecurity. It is based on GAO products issued from June 2004 through November 2009, as well as ongoing work on air cargo security. GAO reviewed relevant documents; interviewed cognizant agency officials; and observed operations at 12 airports, chosen by size and other factors. The results are not generalizable to all airports.

What GAO Recommends

GAO is not making recommendations in this statement; however, GAO has made prior recommendations to DHS to, among other things, analyze the feasibility of scanning U.S.-bound cargo containers and more fully protect computer-reliant critical infrastructures. DHS generally agreed with these recommendations. DHS provided technical comments on this statement, which GAO incorporated as appropriate.

View GAO-10-106 or key components. For more information, contact Cathleen Berrick at (202) 512-8777 or berrickc@gao.gov.

What GAO Found

DHS has made progress in enhancing security in the maritime sector, but key challenges remain. For example, as part of a statutory requirement to scan 100 percent of U.S.-bound container cargo by July 2012, CBP has implemented the Secure Freight Initiative at select foreign ports. However, CBP does not have a plan for fully implementing the 100 percent scanning requirement by July 2012 because it questions the feasibility, although it has not performed a feasibility analysis of the requirement. Rather, CBP has planned two new initiatives to further strengthen the security of container cargo, but these initiatives will not achieve 100 percent scanning. Further, TSA, the Coast Guard, and the maritime industry took a number of steps to enroll over 93 percent of the estimated 1.2 million users in the Transportation Worker Identification Credential (TWIC) program (designed to help control access to maritime vessels and facilities) by the April 15, 2009 compliance deadline, but they experienced challenges resulting in delays and in ensuring the successful execution of the TWIC pilot. While DHS and the Coast Guard have developed a strategy and programs to reduce the risks posed by small vessels, they face ongoing resource and technology challenges in tracking small vessels and preventing attacks by such vessels.

In the aviation sector, TSA has made progress in meeting the statutory mandate to screen 100 percent of air cargo transported on passenger aircraft by August 2010 and in taking steps to strengthen airport security, but TSA continues to face challenges. TSA's efforts include developing a system to allow screening responsibilities to be shared across the domestic air cargo supply chain, among other steps. Despite these efforts, TSA and the industry face a number of challenges including the voluntary nature of the program, and ensuring that approved technologies are effective with air cargo. TSA also does not expect to meet the mandated 100 percent screening deadline as it applies to air cargo transported into the U.S., in part due to existing screening exemptions for this type of cargo and challenges in harmonizing security standards with other nations. GAO is reviewing these issues as part of its ongoing work and will issue a final report next year. In addition, TSA has taken a variety of actions to strengthen airport security by, among other things, implementing a worker screening program; however, TSA still faces challenges in this area.

DHS has made progress in strengthening cybersecurity, such as addressing some lessons learned from a cyber attack exercise, but further actions are warranted. Since 2005, GAO has reported that DHS has not fully satisfied its key responsibilities for protecting the nation's computer-reliant critical infrastructures and has made related recommendations to DHS, such as bolstering cyber analysis and warning capabilities and strengthening its capabilities to recover from Internet disruptions. DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but it has not fully implemented GAO's recommendations and, thus, more action is needed to address the risk to critical cybersecurity infrastructure.

AR 000891

Mr. Chairman and Members of the Committee:

I am pleased to submit this statement on the progress that the Department of Homeland Security (DHS) has made and the challenges it faces in key areas of maritime and aviation security, as well as in securing the nation against computer-based, or cyber attacks. The economic well being of the United States is dependent on the expeditious flow of people and goods through the U.S. transportation system, which moves millions of passengers and tons of freight each day. The extensiveness of the transportation system, as well as the sheer volume of passengers and freight moved, makes it both an attractive target and challenging to secure. Ports, waterways, and vessels are part of an economic engine handling more than $700 billion in merchandise annually, and an attack on this system could have a widespread impact on global shipping, international trade, and the global economy. Likewise, successful terrorist attacks and plots against the commercial aviation system in the past 8 years highlight the threats and vulnerabilities this system faces. Balancing security concerns with the need to facilitate the free flow of people and commerce remains an ongoing challenge for the public and private sectors alike. Likewise, pervasive and sustained cyber attacks against the United States and others continue to pose a potentially devastating impact to systems and operations and the critical infrastructures that they support.

Within DHS, numerous component agencies have responsibility for securing areas of transportation security and computer-reliant critical infrastructures, such as communications and electricity. The Transportation Security Administration (TSA) is the federal agency with primary responsibility for securing all modes of transportation and has developed and implemented a variety of programs and procedures to secure commercial aviation and surface modes of transportation. U.S. Customs and Border Protection (CBP) has a priority mission of keeping terrorists and their weapons out of the U.S., is responsible for securing and facilitating trade, and has primary responsibility for cargo container security. The Coast Guard has responsibility for protecting the public, the environment, and U.S. economic and security interests in any maritime region in which those interests may be at risk, including America's coasts, ports, and inland waterways. The National Protection and Programs Directorate is responsible for, among other things, assuring the security, resiliency, and reliability of the nation's computer-reliant critical infrastructures—a practice known as cyber critical infrastructure protection, or cyber CIP.

AR 000892

A number of laws have been enacted in recent years to strengthen maritime and aviation security, as well as cybersecurity. In response to provisions of the Aviation and Transportation Security Act (ATSA), TSA established the Transportation Worker Identification Credential (TWIC) program in December 2001.[1] The Security and Accountability For Every (SAFE) Port Act of 2006 directed the Secretary of Homeland Security to, among other things, implement the TWIC pilot project in the maritime sector.[2] To increase the security of container cargo bound for the United States, the SAFE Port Act further required CBP to establish a pilot program to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports.[3] Further, in August 2007 the Implementing Recommendations of the 9/11 Commission Act (9/11 Act) was enacted and provides, among other things, that by July 2012, a container loaded on a vessel in a foreign port shall not enter the United States unless that container is scanned before it is loaded onto the vessel.[4] The Act further requires that by August 2010, 100 percent of cargo—domestic and inbound—transported on passenger aircraft be physically screened.[5] To address the threats posed by cyber attacks, President Bush issued a 2003 national strategy and related policy directives aimed at improving cybersecurity nationwide, including both government systems and those

---

[1]See Pub. L. No. 107-71, 115 Stat. 597 (2001). TSA was transferred from the Department of Transportation to DHS pursuant to requirements in the Homeland Security Act of 2002. See Pub. L. No. 107-296, § 403(2), 116 Stat. 2135, 2178.

[2]See Pub. L. No. 109-347, 120 Stat. 1884.

[3]See id. § 231, 120 Stat. at 1915 (codified at 6 U.S.C. § 981).

[4]See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)). Both the SAFE Port Act and 9/11 Act define scanning to be an examination with both non-intrusive imaging equipment and radiation detection equipment. In addition, while the law states that cargo containers are not to enter the United States unless they were scanned at a foreign port, actual participation in the program by sovereign foreign governments and ports is voluntary.

[5]The 9/11 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. See Pub. L. No. 110-53, § 1602(a), 121 Stat. at 477-79 (codified at 49 U.S.C. § 44901(g)). 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. 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 inbound cargo refers to cargo transported by U.S. and foreign-based air carriers from a foreign location to the United States.

that support cyber critical infrastructures[6] owned and operated by the private sector.[7]

My statement today focuses on the progress that DHS and its component agencies have made to strengthen maritime, aviation, and cybersecurity, and the challenges that remain. In particular, my statement addresses (1) cargo container scanning, (2) efforts to enroll maritime workers in the TWIC program, (3) small vessel security,[8] (4) air cargo screening, (5) airport perimeter and access control security, and (6) cybersecurity for critical infrastructure.

My statement is based on related GAO reports and testimonies issued from June 2004 through November 2009,[9] as well as ongoing work that will be completed in early 2010 assessing the progress that DHS and its component agencies have made in addressing challenges related to air cargo screening. To conduct this work, we reviewed relevant documents related to the programs reviewed; interviewed cognizant DHS, TSA, Coast Guard, and CBP officials; and observed operations at a non-probability sample of 19 seaports—13 domestic and 6 foreign—and 12 airports, chosen by size, program participation, and other factors. Although the results of our site visits are not generalizable to all seaports, airports, or officials, we gained a critical understanding of the progress and challenges associated with implementing efforts to secure the transportation system and improve cyber CIP. We have conducted our ongoing work—covering the period October 2008 to date—as well as the prior audit work that serves as the basis for this statement, in accordance with generally

---

[6]Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

[7]The White House, The National Strategy to Secure Cyberspace (Washington, D.C.: February 2003); Homeland Security Presidential Directive 7 (Washington, D.C.: Dec. 17, 2003); and National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

[8]According to DHS's *Small Vessel Security Strategy*, "small vessels" are characterized as any watercraft—regardless of method of propulsion—less than 300 gross tons, and used for recreational or commercial purposes.

[9]See for example, GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 30, 2009) and *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

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.

In summary, DHS has made progress in enhancing security in the maritime sector, but key challenges remain. Among other things, CBP has begun working with foreign ports to scan U.S.-bound container cargo; TSA, Coast Guard, and the maritime industry enrolled over 93 percent of the estimated 1.2 million users in the TWIC program by the April 15, 2009 compliance deadline; and DHS and the Coast Guard have developed a strategy and programs to reduce the risks associated with small vessels. However, DHS and its component agencies face a number of management, technological, and resource challenges associated with these efforts. In our previous work, we made recommendations to help address these challenges. Specifically, in our October 2009 report on scanning of U.S.-bound cargo containers, we made recommendations to DHS and CBP to complete a feasibility analysis, cost estimates, and a cost-benefit analysis and provide the results to Congress to help strengthen container security. In our November 2009 report on TWIC, we made recommendations to TSA to, among other things, expedite the development of contingency and disaster recovery plans and system(s), and recommended to TSA and the Coast Guard that they develop a detailed evaluation plan to help ensure that needed information on biometrics readers will result from the pilot. DHS generally concurred and discussed actions to implement recommendations from both of these reports, but we believe that these actions will not fully address the intent of all of the recommendations. In the aviation sector, TSA has made progress in meeting the air cargo screening mandate of the 9/11 Act—including developing a program to share screening responsibilities across the supply chain, but the agency continues to face challenges related to planning and technology, among other things. In our September 2009 report on airport security, we made recommendations to TSA to, among other things, develop a national strategy to guide stakeholder efforts to strengthen airport perimeter and access control security, to which DHS concurred. Finally, regarding cyber CIP issues, DHS has developed and implemented certain capabilities to satisfy aspects of its cybersecurity responsibilities, such as addressing certain lessons learned from cyber attack exercises, but it has not fully satisfied our recommendations to, among other things, bolster cyber analysis and warning capabilities and strengthen its capabilities to recover from Internet disruptions. As a result, DHS needs to take further action to address these areas.

Background

Secure Freight Initiative (SFI)

In December 2006, in response to SAFE Port Act requirements, DHS, and the Department of Energy (DOE) jointly announced the formation of the Secure Freight Initiative (SFI) pilot program to test the feasibility of scanning 100 percent of U.S.-bound container cargo at three foreign ports (Puerto Cortes, Honduras; Qasim, Pakistan; and Southampton, United Kingdom). According to CBP officials, while initiating the SFI program at these ports satisfied the SAFE Port Act requirement, CBP also selected the ports of Busan, South Korea; Hong Kong; Salalah, Oman; and Singapore to more fully demonstrate the capability of the integrated scanning system at larger, more complex ports. As of October 2009, SFI has been operational at five of these initial seven seaports. According to CBP and DOE officials, the SFI program builds upon existing container security measures by enhancing the U.S. government's ability to have containers scanned for nuclear and radiological material overseas and, thus, better assess the risk of weapons of mass destruction (WMD) in inbound cargo containers.

Transportation Worker Identification Credential (TWIC)

Managed by TSA and the U.S. Coast Guard, the TWIC program aims to protect the nation's maritime transportation facilities and vessels by requiring maritime workers to complete background checks and obtain a biometric identification card in order to gain unescorted access to the secure areas of regulated facilities and vessels.[10] A federal regulation in January 2007 set a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker was required to hold a TWIC in order to obtain unescorted access to secure areas of regulated facilities

[10]Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements—for authentication purposes. According to Coast Guard guidance, a secure area is an area that has security measures in place for access control. For most maritime facilities, the secure area is generally any place inside the outer-most access control point. For a vessel or outer continental shelf facility, such as off-shore petroleum or gas production facilities, the secure area is generally the whole vessel or facility.

and vessels.[11] In addition, TSA has initiated a pilot to test the use of TWIC with related access control technologies.

Small Vessel Security

Concerns have grown about the security risks of small vessels and DHS has identified the four gravest risk scenarios involving the use of such vessels for terrorist attacks. Some of these risks have been shown to be real through attacks conducted outside U.S. waters, but to date, no small boat attacks have happened in the United States. These four scenarios include the use of a small vessel as (1) a waterborne improvised explosive device, (2) a means of smuggling weapons into the United States, (3) a means of smuggling humans into the United States, and (4) a platform for conducting a stand-off attack.

Air Cargo Security

Air cargo ranges in size from 1 pound to several tons, and 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 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.[12] TSA's responsibilities include, among other things, establishing security requirements governing domestic and foreign passenger air carriers that transport cargo, and domestic freight forwarders.

Perimeter and Access Control Security

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

[11]To implement the requirement for using a biometric credential for accessing select maritime facilities and vessels—as called for in the Maritime Transportation Security Act of 2002 (MTSA), as amended by the Security and Accountability For Every (SAFE) Port Act of 2006—the credential rule (72 Fed. Reg. 3492 (2007)) established that all maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities and vessels were expected to hold TWICs by September 25, 2008, but the final compliance date was extended to April 15, 2009, pursuant to 73 Fed. Reg. 25562 (2008).

[12]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.

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.[13] Airport workers may access sterile areas— areas of airports where passengers wait after screening to board departing aircraft— 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.

Cybersecurity

The federal government has developed a strategy to address cyber threats. Specifically, President Bush issued the 2003 National Strategy to Secure Cyberspace and related policy directives, such as Homeland Security Presidential Directive 7, that specify key elements of how the nation is to secure key computer-based systems, including both government systems and those that support critical infrastructures owned and operated by the private sector. The strategy and related policies also establish DHS as the focal point for cyber critical infrastructure protection and assigns DHS multiple leadership roles and responsibilities in this area, to include (1) developing a comprehensive national plan for critical infrastructure protection, including cybersecurity; (2) developing and enhancing national cyber analysis and warning capabilities; (3) providing and coordinating incident response and recovery planning, including conducting incident response exercises; (4) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems; and (5) strengthening international cyberspace security. More recently, in February 2009, President Obama directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States' cybersecurity-related policies and structures. The resulting May 2009

[13]See generally Pub. L. No. 107-71, 115 Stat. 597 (2001).

report made a number of recommendations to improve the nation's approach.[14]

Maritime Security

CBP Has Made Some Progress in Working with Foreign Ports to Scan U.S.-Bound Containers, but Challenges Remain in Expanding the Program to Larger Ports and Meeting the Statutory Target Date

In October 2009, we reported that CBP has made some progress in working with the initial SFI ports to scan U.S.-bound cargo containers; but because of challenges to expanding scanning operations, especially to larger ports, the feasibility of scanning 100 percent of U.S.-bound cargo containers at over 600 foreign seaports remains largely unproven.[15] CBP and DOE have been successful in integrating images of scanned containers onto a single computer screen that can be reviewed remotely from the United States and have also been able to use these initial ports as a test bed for new applications of existing technology, such as mobile radiation scanners. However, the SFI ports' level of participation, in some cases, has been limited in terms of duration or scope. While 54 to 86 percent of the U.S.-bound cargo containers, on average, were scanned at 3 comparatively low volume ports that are responsible for less than 3 percent of container shipments to the United States, CBP has not been able to achieve sustained scanning rates above 5 percent at 2 comparatively larger ports—the type of ports that ship most containers to the United States.[16] Scanning operations at the initial SFI ports have encountered a number of challenges, such as logistical problems with containers transferred from rail or other vessels, and CBP officials are concerned that they and the participating ports cannot overcome them.

CBP has developed two initiatives related to SFI for improving container security; however, challenges remain as neither initiative will enable CBP to fully achieve the 9/11 Act requirement to scan 100 percent of all U.S.-

[14]The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

[15]GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

[16]Scanning percentages at Port Qasim, Puerto Cortes, and the Port of Southampton reflect operations conducted from November 2007 through May 2009.Scanning percentages at the Port of Hong Kong reflect operations conducted from February 2008 through April 2009. Scanning percentages at the Port of Busan reflect operations conducted from April 2009 through May 2009.

bound cargo by July 2012. The first initiative, the "strategic trade corridor strategy," involves scanning 100 percent of U.S.-bound containers at selected foreign ports where CBP believes it will mitigate the greatest risk of weapons of mass destruction (WMD) entering the United States. The Secretary of Homeland Security approved this strategy and, according to CBP, is in negotiations with foreign governments to expand SFI to ports in those countries. The second initiative, known as "10+2", requires importers to provide 10 data elements and vessel carriers to provide 2 data elements on containers and their cargo to CBP, which provides further information to CBP, thus, improving its ability to identify containers that may pose a risk of containing WMD for additional scrutiny—such as scanning or physical inspection. Based on discussions with DHS and CBP officials, it is unclear whether DHS intends for the strategic trade corridor strategy and 10+2 to be implemented in lieu of the 100 percent scanning requirement or whether it is the first phase of implementation. While these initiatives may collectively improve container security, they will not enable CBP to fully achieve the 9/11 Act requirement to scan 100 percent of U.S.-bound containers by July 2012. According to CBP, it does not have a plan for fully implementing the scanning requirement by this date because it questions the feasibility; however, it has not performed a feasibility analysis of expanding 100 percent scanning, as required by the SAFE Port Act. To address this, in October 2009, we recommended that CBP conduct a feasibility analysis of implementing 100 percent scanning and provide the results, as well as alternatives to Congress, in order to determine the best path forward to strengthen container security.[17] CBP concurred with our recommendation. Further, senior DHS and CBP officials acknowledge that most, if not all foreign ports, will not be able to meet the July 2012 target date for scanning all U.S.-bound cargo. As a result, DHS has recently decided to grant a blanket extension to all foreign ports, thus extending the target date for compliance with this requirement by 2 years, to July 2014.

[17]GAO-10-12.

TSA and the Coast Guard Took Steps to Enroll Transportation Workers into the TWIC Program by the Mandated Deadline, but Challenges in Program Scheduling and Evaluation May Hinder the TWIC Reader Pilot's Usefulness

In November 2009 we reported that, based on lessons learned from its early experiences with enrollment and activation, TSA and its contractor took steps to prepare for a surge in TWIC enrollments and activations as local compliance dates approached.[18] For example, according to TSA and port facility representatives, TSA and its contractor increased enrollment center resources, such as increasing the number of enrollment and activation stations to meet projected TWIC user demands. Likewise, the Coast Guard employed strategies to help the maritime industry meet the TWIC national compliance date while not disrupting the flow of commerce. As a result of these efforts, TSA reported enrolling 1,121,461 workers in the TWIC program, or over 93 percent of the estimated 1.2 million users, by the April 15, 2009 deadline.

Although most workers received their TWICs, TSA data show that some workers experienced delays in receiving TWICs. Among the reasons for the delays was that a power failure occurred in October 2008 at the government facility that processes TWIC data that caused a hardware component failure in the TWIC enrollment and activation system for which no replacement component was on hand. In our November 2009 report on TWIC, we made recommendations to TSA to expedite the development of contingency and disaster recovery plans and system(s). DHS stated it is taking steps to address this recommendation and future potential TWIC system failures by developing a system to support disaster recovery by 2012. While DHS's efforts are a positive step, until they are complete, TWIC systems remain vulnerable to similar disasters.

In response to our 2006 recommendation and a SAFE Port Act requirement, TSA initiated a pilot in August 2008[19] known as the TWIC reader pilot, to test TWIC-related access control technologies.[20] The pilot is expected to test the viability of selected biometric card readers for use in reading TWICs within the maritime environment and test the technical aspects of connecting TWIC readers to access control systems. The results

[18]GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: Nov. 18, 2009).

[19]The pilot initiation date is based on the first date of testing identified in the TWIC pilot schedule. The SAFE Port Act required the pilot to commence no later than 180 days after the date of enactment of the SAFE Port Act (October 13, 2006).

[20]GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: Sept. 29, 2006).

of the pilot are expected to inform the development of the card reader rule requiring TWIC readers for use in controlling access at MTSA regulated vessels/facilities. Based on the August 2008 pilot initiation date, the card reader rule is to be issued no later than 24 months from the initiation of the pilot, or by August 2010.

Although TSA has made significant progress to incorporate best practices into TWIC's schedule for implementing the reader pilot program, weaknesses continue to exist that limit TSA's ability to use the schedule as a management tool to guide the pilot and accurately identify the pilot's completion date. In response to limitations that we identified, the program office developed a new TWIC pilot master schedule in March 2009, and updated it in April 2009, and again in May 2009. The pilot schedule went from not meeting any of the nine scheduling best practices in September 2008 to fully addressing one of the practices, addressing seven practices to varying degrees, and not addressing one practice.[21] While TSA has improved its technical application of program scheduling practices on the TWIC reader pilot program, as of May 2009, weaknesses remain that may adversely impact its usefulness as a management tool. For example, the schedule does not accurately reflect all key pilot activities or assign resources to those activities. To address these weaknesses, in our November 2009 report we recommended that TSA, in concert with pilot participants, fully incorporate best practices for program scheduling in the pilot. TSA concurred in part with our recommendation. In addition, shortfalls in TWIC pilot planning have presented a challenge for TSA and the Coast Guard in ensuring that the pilot is broadly representative of deployment conditions. This is in part because an evaluation plan that

[21]These best practices include (1) capturing all activities—defining in detail the work to be completed, including activities to be performed; (2) sequencing all activities—listing activities in the order in which they are to be carried out; (3) assigning resources to all activities—identifying the resources needed to complete the activities; (4) establishing the duration of all activities—determining how long each activity will take to execute; (5) integrating all activities horizontally and vertically—achieving aggregated products or outcomes by ensuring that products and outcomes associated with other sequenced activities are arranged in the right order, and dates for supporting tasks and subtasks are aligned; (6) establishing the critical path for all activities—identifying the path in the schedule with the longest duration through the sequenced list of key activities; (7) identifying float between activities—using information on the amount of time that a predecessor activity can slip before the delay affects successor activities; (8) conducting a schedule risk analysis—using statistical techniques to predict the level of confidence in meeting a project's completion date; and (9) updating the schedule using logic and durations to determine the dates for all activities—continuously updating the schedule to determine realistic start and completion dates for program activities based on current information.

fully identifies the scope of the pilot and the methodology for collecting and analyzing the information resulting from the pilot has not been developed. Agency officials told us that no such evaluation plan was developed because they believe that the existing pilot documentation coupled with subject matter expertise would be sufficient to guide the pilot. However, our review of the TWIC pilot highlights weaknesses that could be rectified by the development and use of an evaluation plan. To address this, in November 2009, we recommended that TSA and the Coast Guard develop an evaluation plan to help ensure that needed information on the use of biometrics readers will result from the pilot. DHS concurred and discussed actions to implement the recommendation, but it is too early to determine if the intended actions will fully address the intent of the recommendation.

DHS and Coast Guard Have a Strategy and Programs in Place, but Identifying and Preventing Small Vessel Attacks Remains a Challenge

While DHS and the Coast Guard have developed a strategy and programs to reduce the risks associated with small vessels, they face ongoing challenges in tracking small vessels and preventing attacks by such vessels.[22] In April 2008, DHS issued its Small Vessel Security Strategy and is now in the process of developing and reviewing a more detailed implementation plan. After review by the Coast Guard and CBP, the draft plan was forwarded to DHS on September 18, 2009 with a recommendation for approval, but DHS has not yet issued a final decision. As part of its effort to improve security in the maritime domain, the Coast Guard is also implementing two major unclassified systems to track a broad spectrum of vessels. While these systems use proven technologies, they depend on the compliance of vessel operators to carry equipment needed to interact with these systems and to make sure the systems are turned on and functioning properly. These systems, however, generally cannot track small vessels. The Coast Guard and other agencies have other systems, though—which can include cameras and radars—that can track small vessels within ports, but these systems are not installed at all ports, and do not always work in bad weather or at night. In addition, the Coast Guard and other agencies, such as the New Jersey State Police, have several programs in place to address risks from small vessels, such as outreach efforts to the boating community to share threat information. However, the Coast Guard program faces resource limitations. For

[22]For further information on the risks associated with small vessels, see GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

example, the Coast Guard's program to reach out to the boating community for their help in detecting suspicious activity, America's Waterway Watch, lost the funding it received through a Department of Defense readiness training program for military reservists in fiscal year 2008. Now it must depend on the activities of the Coast Guard Auxiliary, a voluntary organization, for most of its outreach efforts. Even with systems in place to track small vessels, there is widespread agreement among maritime stakeholders that it is very difficult to detect threatening activity by small vessels without prior knowledge of a planned attack.

Aviation Security

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

As we previously reported in March 2009, TSA has taken several key steps to meet the air cargo screening mandate of the 9/11 Act as it applies to domestic cargo.[23] TSA's approach involves multiple air cargo industry stakeholders sharing screening responsibilities across the air cargo supply chain. According to TSA officials, this decentralized approach is expected to minimize carrier delays, cargo backlogs, and potential increases in cargo transit time, which would likely result if screening were conducted primarily by air carriers at the airport. The specific steps that TSA has taken to address domestic air cargo screening include the following:

- **Revised air carrier security programs:** Effective October 1, 2008, TSA established a requirement for 100 percent screening of nonexempt cargo transported on narrow-body passenger aircraft.[24] Effective February 1, 2009, TSA also required air carriers to ensure the screening of 50 percent of all nonexempt air cargo transported on all passenger aircraft. Furthermore, effective February 2009, TSA revised or eliminated most of its screening exemptions for domestic cargo.[25]

[23]GAO, *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, D.C.: Mar.18, 2009).

[24]Narrow-body flights transport about 26 percent of all cargo on domestic passenger flights. According to TSA officials, narrow-body aircraft make up most domestic passenger flights, and transport most passengers traveling on domestic passenger flights.

[25]Effective September 2009, TSA revised or eliminated additional exemptions for domestic cargo.

- **Created the Certified Cargo Screening Program (CCSP):** TSA created 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. In this program, air cargo industry stakeholders—such as freight forwarders and shippers—voluntarily apply to become certified cargo screening facilities (CCSF). CCSFs in the program were required to begin screening cargo as of February 1, 2009.

- **Issued an interim final rule:** On September 16, 2009, TSA issued an interim final rule, effective November 16, 2009, that among other things, codifies the statutory air cargo screening requirements of the 9/11 Act and establishes requirements for entities participating in the CCSP.

- **Established the Air Cargo Screening Technology Pilot:** To operationally test explosives trace detection (ETD) and X-ray technology among CCSFs, TSA created the Air Cargo Screening Technology Pilot in January 2008, and selected some of the largest freight forwarders to use the technologies and report on their experiences.[26] This pilot is ongoing, with an anticipated end date of August 2010, and the results have not yet been finalized.

- **Expanded its explosives detection canine program:** To assist air carriers in screening cargo, TSA has taken steps to expand the use of TSA-certified explosives detection canine teams. TSA now has 120 allocated canine teams dedicated to air cargo screening at 20 major airports.

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 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. Attracting certified cargo screening facilities (CCSF) is important because much cargo is currently delivered to air carriers in a consolidated form and the requirement to screen individual pieces of cargo will necessitate screening earlier in the air cargo supply chain. However, there are concerns about potential

[26]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.

program costs, including acquiring expensive technology, hiring additional personnel, conducting additional training, and making facility improvements.

Second, while TSA has taken steps to test technologies for screening and securing air cargo, it has not yet completed assessments of the technologies it plans to allow air carriers and program participants to use in meeting the August 2010 screening mandate. According to TSA officials, the agency has conducted laboratory assessments and plans to complete operational testing of X-ray technologies by late 2009, and laboratory and operational testing of explosives trace detection technology by August 2010. However, these technologies, which have not yet been fully tested for effectiveness, are currently being used by industry participants to meet air cargo screening requirements.

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 carrier and freight forwarders, TSIs are to also perform compliance inspections of new regulated entities that voluntarily become CCSFs, as well as conduct additional CCSF inspections of existing freight forwarders. TSA officials have stated that there may not be enough TSIs to conduct compliance inspections of all the potential CCSFs once the program is fully implemented by August 2010. Until TSA completes its staffing study, TSA may not be able to 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.[27]

Finally, TSA has taken some steps to meet the screening mandate as it applies to inbound 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.[28] In addition, TSA continues to work with CBP to leverage an

[27]For additional information on TSA's staffing study, see GAO, *Aviation Security: Status of Transportation Security Inspector Workforce*, GAO-09-123R (Washington D.C.: Feb. 6, 2009).

[28]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.

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 existing inbound screening exemptions, which TSA has not reviewed or revised, and 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 ongoing review of TSA's air cargo security efforts, to be issued next year.

TSA Has Taken Actions to Strengthen Airport Security, but Faces Challenges in Assessing Risk, Evaluating Worker Screening Methods, Addressing Airport Technology Needs, and Developing a National Strategy for Airport Security

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.[29] For example, in March 2007, TSA implemented a random worker screening program—the Aviation Direct Access Screening Program (ADASP)—nationwide to enforce access procedures, such as ensuring that workers do not possess unauthorized items when entering secured areas. In addition, TSA has expanded requirements for background checks and the population of individuals who are subject to these checks, and has established a statutorily directed pilot program to assess airport security technology.[30] In 2004 TSA initiated the Airport Access Control Pilot Program to test, assess, and provide information on new and emerging technologies, including biometrics. TSA issued a final report on the pilots in December 2006.

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.[31] 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

[29]GAO-09-399.

[30]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)).

[31]GAO-09-399.

milestones for its completion, and evaluate whether the current approach to conducting vulnerability assessments appropriately assesses vulnerabilities. DHS concurred with these recommendations.

Further, 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 to help identify the potential costs and benefits of 100 percent worker screening and other worker screening methods.[32] 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.[33] However, the report also identified limitations in the design and evaluation of the program and in the estimation of 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.[34] 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

---

[32]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.

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

[34]The contractor TSA hired to assist with the pilot program identified design and evaluation limitations, such as the limited number of participating airports. The contractor also identified limitations regarding estimates of the costs and operational effects of implementing various worker screening methods nationwide. For example, the contractor noted that its cost estimates did not include costs associated with operational effects, such as longer wait times for workers, and potentially costly infrastructure modifications, such as construction of roads and shelters to accommodate vehicle screening.

these decisions into airports' existing systems.[35] 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.

Cybersecurity

DHS Has Made Progress in Strengthening Cybersecurity, but Further Actions are Warranted

Federal law and policy[36] establish DHS as the focal point for efforts to protect our nation's computer-reliant critical infrastructures. Since 2005, we have reported that DHS has not yet fully satisfied its key responsibilities for protecting these critical infrastructures and have made recommendations for DHS to address in key cyberscurity areas, to include the five key areas shown in table 1.

Table 1: Key Cybersecurity Areas Identified by GAO

1.	Bolstering cyber analysis and warning capabilities
2.	Completing actions identified during cyber exercises
3.	Improving cybersecurity of infrastructure control systems
4.	Strengthening DHS's ability to help recover from Internet disruptions
5.	Addressing cyber crime

Source: GAO.

[35]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)).

[36]These include The Homeland Security Act of 2002, Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace.*

DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but the department has not fully implemented our recommendations and, thus, further action needs to be taken to address these areas. For example, in July 2008, we reported[37] that DHS's United States Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities related to four key areas.[38] As a result, we recommended that the department address shortfalls in order to fully establish a national cyber analysis and warning capability. DHS agreed in large part with our recommendation. Similarly, in September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned from these efforts, but its actions to address the lessons had not been fully implemented.[39] Consequently, we recommended that DHS complete corrective activities to strengthen coordination between public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation and has made progress in completing some identified activities.

We also testified in March 2009 on needed improvements to the nation's cybersecurity strategy.[40] In preparing for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement.

The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by these experts are listed in table 2.

---

[37]GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

[38]The four key areas are: (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat.

[39]GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO-08-825 (Washington, D.C.: Sept. 9, 2008).

[40]GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar.10, 2009).

Table 2: Key Strategy Improvements Identified by Cybersecurity Experts

1.	Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2.	Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3.	Establish a governance structure for strategy implementation.
4.	Publicize and raise awareness about the seriousness of the cybersecurity problem.
5.	Create an accountable, operational cybersecurity organization.
6.	Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7.	Bolster public-private partnerships through an improved value proposition and use of incentives.
8.	Focus greater attention on addressing the global aspects of cyberspace.
9.	Improve law enforcement efforts to address malicious activities in cyberspace.
10.	Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11.	Increase the cadre of cybersecurity professionals.
12.	Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research in this area. Until they are addressed, our nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk to attack from our adversaries.

Mr. Chairman, this concludes my statement for the record.

GAO Contacts and Staff Acknowledgements

For questions about this statement, please contact Cathleen A. Berrick at 202-512-8777, or berrickc@gao.gov. For further information regarding maritime security issues, please contact Stephen L. Caldwell at 202-512-9610, or caldwells@gao.gov. For further information regarding aviation security issues, please contact Stephen M. Lord at 202-512-4379, or lords@gao.gov. For further information regarding cybersecurity issues, contact David A. Powner at 202-512-9286, or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Acknowledgments

In addition to the contacts named above, Christopher Conrad, Assistant Director, managed this review. Jonathan Bachman, Dave Bruno, Lisa Canini, Joseph Cruz, Michael Gilmore, Barbara Guffy, Lemuel Jackson,

Steve Morris, Robert Rivas, Yanina Golburt Samuels, and Rebecca Kuhlmann Taylor made significant contributions to the work. Frances Cook, Geoffrey Hamilton, Tom Lombardi, and Jan Montgomery provided legal support. Linda Miller provided assistance in testimony preparation.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper

U.S. Department of Homeland Security
Arlington, VA 20598-6016

Transportation Security Administration

DEC 24 2009

Mr. Ralph Nader
Post Office Box 19367
Washington, DC 20036

Dear Mr. Nader:

Thank you for your letter of October 23, 2009, to Secretary Janet Napolitano concerning the use of advanced imaging technology (AIT) machines (sometimes referred to as whole body imaging machines) to screen passengers for security purposes at our nation's airports. AIT is a key component of the Transportation Security Administration's (TSA) efforts to address existing and emerging security threats that are not adequately addressed by current technologies.

TSA uses a variety of resources – including our web site,[1] blog,[2] outreach to the media and other interested groups, and signage at airports – to explain to the public the deployment of AIT machines at airport checkpoints. We appreciate the opportunity to provide information on this important subject to you.

Why AIT Machines Are Needed: AIT machines improve the detection capability for non-metallic (as well as metallic) threats, including weapons, explosives, and other objects concealed under layers of clothing that cannot necessarily be detected by walk-through metal detectors. The AIT machines not only enhance security, but also have reduced the need for pat-down searches for passengers with joint replacements and other medical conditions that cause them to set off the alarms on walk-through metal detectors. The AIT machines thus improve passenger convenience and comfort while enhancing public safety and security.

The emphasis on developing new technologies to address transportation security is codified at 49 U.S.C. § 44925(a), which directs the Secretary of Homeland Security to "give a high priority to developing, testing, improving, and deploying, at airport screening checkpoints, equipment that detects nonmetallic, chemical, biological, and radiological weapons, and explosives, in all forms, on individuals and in their personal property." This equipment must detect, under realistic operating conditions, the types of weapons and explosives that terrorists would most likely attempt to smuggle onto an aircraft. The Secretary also is required under 49 U.S.C. §

[1] See, e.g., Imaging Technology, www.tsa.gov/approach/tech/imaging_technology.shtm; TSA Continues Millimeter Wave Passenger Imaging Technology Pilot, www.tsa.gov/press/happenings/mwave_continues.shtm; TSA to Begin Testing Imaging Technology at George Bush Intercontinental Airport, www.tsa.gov/press/releases/2009/0731.shtm; and TSA to Begin Testing Imaging Technology at Cleveland Hopkins International Airport, www.tsa.gov/press/releases/2009/0730.shtm.

[2] See, e.g., Imaging Technology: The Bigger Picture, www.tsa.gov/blog/2009/08/imaging-technology-bigger-picture.html; Safety & Privacy Concerns Regarding the Millimeter Wave Whole Body Imager, www.tsa.gov/blog/2008/04/safety-privacy-concerns-regarding.html; and Pilot Program Tests Millimeter Wave for Primary Passenger Screening, www.tsa.gov/blog/2009/02/pilot-program-tests-millimeter-wave-for.html.

44925(b) to develop a strategic plan for deploying explosive detection equipment, such as AIT machines, at airport screening checkpoints.

In regard to your statement regarding the applicability of the Administrative Procedure Act (APA), TSA is not required to initiate APA rulemaking procedures each time the agency develops and implements improved passenger screening procedures. Current regulations require passengers and others to comply with TSA's procedures before entering airport sterile areas and other secured portions of airports. 49 CFR 1540.105(a)(2) and 1540.107.

Health and Safety: One of TSA's top priorities in the deployment of the AIT machines is to ensure the products are safe and independently evaluated. TSA deploys AIT machines using x-ray or millimeter wave technology.

The AIT x-ray systems were evaluated for TSA by the Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH), the National Institute for Science and Technology (NIST), and the Johns Hopkins University Applied Physics Laboratory (APL). All results confirmed that the radiation doses for the individuals being screened, operators, and bystanders were well below the dose limits specified in the American National Standards Institute (ANSI)/Health Physics Society (HPS) N43.17-2002, "Radiation Safety for Personnel Security Screening Systems Using X-rays." For comparison purposes, the radiation dose received from one AIT x-ray screening is equivalent to the radiation dose received from natural background radiation in two minutes of airplane flight at altitude.

In addition, regarding systems that comply with N43.17-2002, NCRP Commentary no. 16, *Screening of Humans for Security Purposes Using Ionizing Radiation,* states that "[g]iven the low levels of effective dose involved per scan (and the resultant low levels of equivalent dose per scan to the embryo or fetus of a pregnant woman), no special precautions are required for the embryo or fetus of a pregnant woman, for infants, or for children."

Similarly, the energy projected by AIT millimeter wave technology screening systems is 10,000 times less than a cell phone transmission (.00000597 mW/cm2 for millimeter wave technology compared to 37.5 mW/cm2 for a cell phone), and far below the standards set by the Institute of Electrical and Electronics Engineers (IEEE) and the International Commission on Non-Ionizing Radiation Protection (ICNIRP).[3] TSA requires that millimeter wave AIT equipment be tested by independent, third-party labs to assure that the equipment meets the IEEE and ICNIRP standards for safety.

Passenger Privacy: While AIT provides significantly enhanced threat detection capabilities, TSA implemented both technology and process protections to ensure that passenger privacy and anonymity is maintained during screening. For example, TSA required AIT manufacturers to include software algorithms in AIT systems that enhance privacy by blurring the face or the image of the body. In addition, the AIT machines cannot store images of screened passengers. TSA separated the TSO who views the AIT image (image operator) from the TSO at the screening location to avoid a specific individual from being associated with the image. Further, AIT screening is voluntary. The passenger may choose whether to undergo screening by this

[3] See Institute of Electrical and Electronics Engineers (IEEE), C95.1 – 2005, Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz, revision of C95.1-1991 (Active), and International Commission on Non-Ionizing Radiation Protection (ICNIRP), Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields (Up to 300 GHz). Health Physics 74 (4): 494-522, April 1998.

technology or proceed through a WTMD followed by a pat down. Over 98 percent of passengers opt for AIT screening.

TSA provided notice of its use of these machines to the public in Privacy Impact Assessments (PIAs)[4] in accordance with Section 222 of the Homeland Security Act and in consultation with the DHS Privacy Office. In addition, when evaluating privacy protections to place on this technology, TSA also considered the Fair Information Practice Principles (FIPPs)[5] developed by DHS from the concepts underlying the Privacy Act of 1974. The application of the FIPPs to TSA's implementation of AIT screening is discussed extensively in the PIAs. TSA also provides information at each AIT station and continues to engage in public dialogue concerning the use of AIT.

We appreciate that you took the time to share your concerns, and we hope this information is helpful.

Sincerely yours,

Keith Hall

for Robin Kane
Assistant Administrator/CTO
Operational Process & Technology

[4] See Privacy Impact Assessment – http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf. The PIA was updated on July 23, 2009, see http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf.

[5] The Fair Information Practice Principles (FIPPs): Framework for Privacy Policy at the Department of Homeland Security, December 29, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. As noted in this policy guide, these principles include: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality & Integrity, Security, and Accountability & Auditing.

MY

SCANNED/RECEIVED
BY EXEC SEC

2009 OCT 30 PM 3:46

October 23, 2009

Secretary Janet Napolitano
Department of Homeland Security
U.S. Department of Homeland Security
Washington, DC 20528

Dear Secretary Napolitano:

I am writing to voice my concerns over the use of whole-body imaging machines to screen airport passengers for security purposes, and the Transportation Security Administration's (TSA) announced plan, as described in the April 7, 2009 New York Times, to replace metal detectors with such body imaging machines as the primary screening tool at US airports.

Last June, the House of Representatives, overwhelming voted to severely restrict TSA's use of these machines, such as the backscatter x-ray and millimeter wave machines, in airports. However, this past month, it was announced that the TSA will deploy an additional 150 whole-body imaging machines to screen passengers in airports across the country. The TSA should observe the spirit of the House's vote and restrict the deployment of these machines until the Congress has settled the question of their use as a screening device.

Moreover, with respect to any deployment of these machines in US airports, the TSA should adhere to the public rulemaking requirements of the Administrative Procedures Act. The TSA should not invoke national security as justification for dispensing with the APA's public procedure requirements. Specifically, the TSA should:

* Fully explain why whole-body imaging machines are needed and why current security procedures are inadequate to protect the traveling public.

* Present scientific and medical evidence that the x-rays emitted by the backscatter imaging machines do not pose a health risk to passengers going through the machines, as well as to TSA employees operating the machines and passengers queuing in line near the machines. The TSA has routinely downplayed the health risks associated with these imaging machines, but has not released any information about the specific amount of x-rays emitted by such machines, their frequency of calibration and maintenance.

TSA-091102-034

Frequent fliers, pregnant women, children, and people who carry defective genes that make them more susceptible to radiation will be exposed to x-rays that may cause potential health hazards, no matter how small the risk. Initially, the TSA planned to use these machines only as a secondary screening tool for those small number of passengers who set off the metal detectors. Now, every air traveler, regardless of suspicion, may be subjected to unnecessary x-ray exposure. In a August 11, 2008 Boston Globe article, David Brenner, director of the Center for Radiological Research at Columbia University Medical Center, commented on the suitability of subjecting every passenger to such machines: "If you're going to go from New York to Los Angeles, you don't really have a choice about flying," he said. "But perhaps you should have a choice about going through these x-ray machines or not."

* Present arguments why whole-body imaging machines do not invade passengers' privacy. The ACLU has described these machines as a "frontal assault on personal privacy, with virtual strip searches revealing private body parts and intimate medical details." The TSA will capture the naked pictures of traveling Americans suspected of no wrongdoing.

Sincerely,

Ralph Nader

P.O. Box 19367
Washington, DC 20036

R. Nader
Post Office Box 19367
Washington, D.C. 20036

WASHINGTON DC 200

23 OCT 2009 PM 67 L

Secretary Janet Napolitano
Department of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528

RECEIVED OCT 27 2009

SG
OCT 28 2009

#16

RECEIVED STAPLED

TRANSPORTATION SECURITY ADMINISTRATION

OSO Executive Summary Recap

★ ★ ★ 28 December 2009 ★ ★ ★

AR 000921

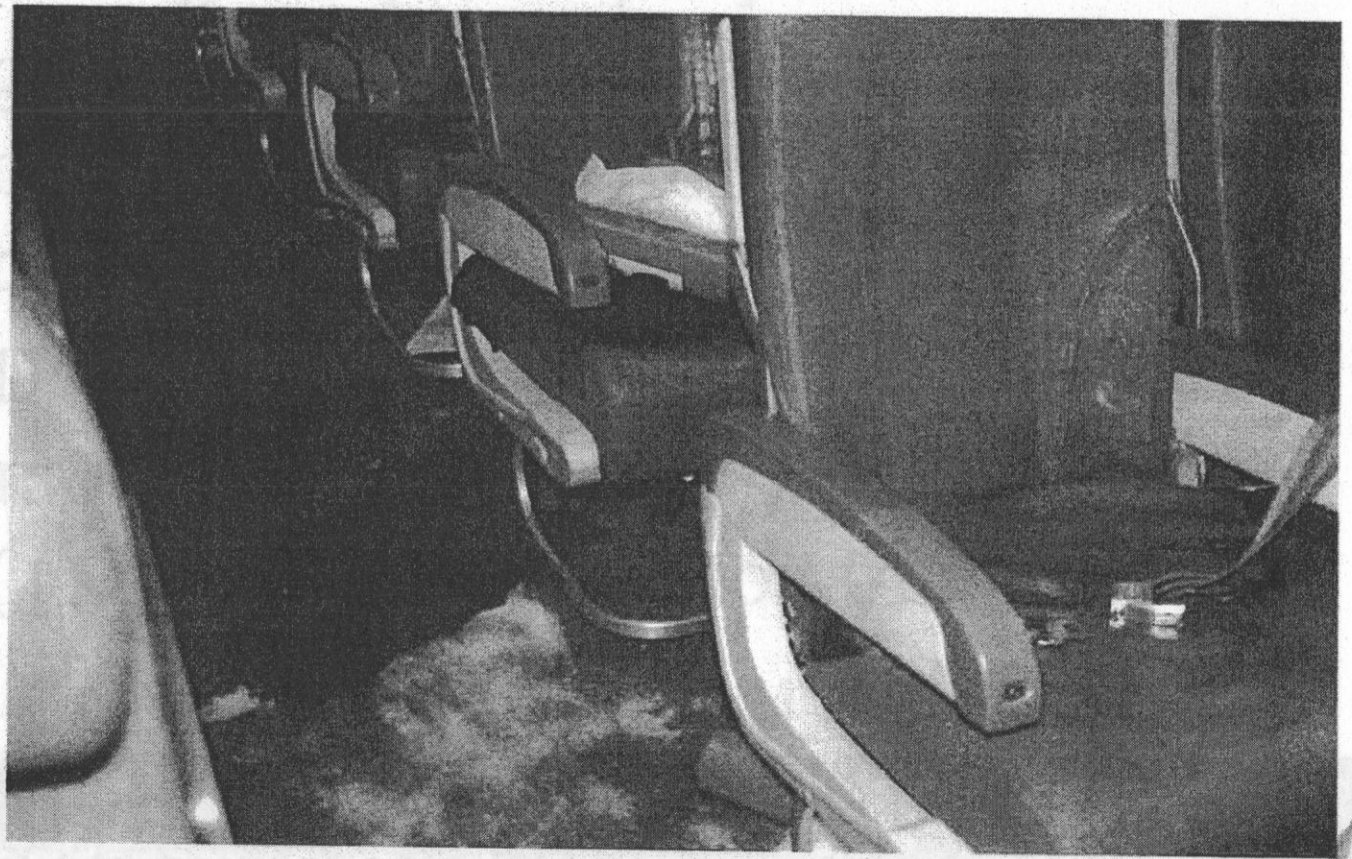
Disruptive Passenger on Flight to Detroit (DTW)

- (DTW) PIC of Northwest 253 (Amsterdam-Detroit) reported a fire indicator warning light
- PIC reported popping sounds in aircraft after landing
- Delta Security reported Pax ABDULMUTALLAB attempted to ignite a firecracker while in-flight
- Surrounding Pax tackled and restrained ABDULMUTALLAB
- Pax sustained burn injuries transported to hospital under CBP custody
- Pax stated there was a bomb on the aircraft as he was escorted off
- Pax told CBP that he got explosive device in Yemen and was supposed to detonate over US airspace and he had ties to Al Qaeda
- ICE reported device was a syringe filled with liquid that led into a bag of white powder taped to Pax's leg / powder would explode when liquid was injected into powder
- FBI is conducting all investigation

AR 000922

Derived: TSA-12-11860-09

Disruptive Passenger on Flight to Detroit (DTW)



AR 000923

Passenger Arrested after Artfully Concealed Contraband Detected by WBI at (TPA)

- (TPA) Item observed on American 1295 Pax ALLEN on (WBI)
- During private screening, marijuana discovered - Pax arrested on a charge of Possession of a Controlled Substance
- Pax allowed to re-book

AR 000924

TRANSPORTATION SECURITY ADMINISTRATION

OPS Executive Summary Recap

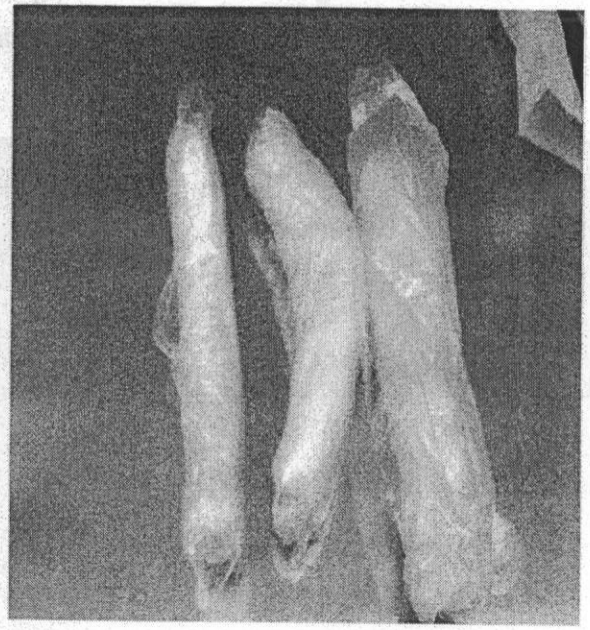
★ ★ ★ ★ ★ ★

Whole Body Imagery
Drug Detections

AR 000925

Passengers Arrested After Contraband Discovered during Checkpoint Screening at (LAX) (06/03/09)

- (LAX) Anomalies detected in WBI on Pax JOHNSON
- JOHNSON referred to secondary screening
- One pound of Methamphetamine discovered in JOHNSON's groin area
- LEO's responded and discovered upon further investigation 2 other Pax's in possession of 2 additional pounds of Methamphetamine
- All three Pax's arrested



AR 000926

Passenger Arrested after Controlled Substance Discovered during Checkpoint Screening at (SFO) (07/07/09)

- (SFO) Whole Body Imagery detected anomaly on Pax SHAFFER
- During secondary screening SHAFFER stated he was concealing contraband in crotch area
- LEO's responded – confiscated syringe – tested positive for cocaine
- SHAFFER placed under arrest
- EIR was not initiated against SHAFFER

AR 000927

Passenger Arrested during Checkpoint Screening at (PHX) (09/16/09)

- (PHX) Pax GRUBBS alarmed WTMD – referred to WBI for additional screening
- Anomaly detected in GRUBBS pocket during WBI screening
- During secondary screening – razor blade – bag containing white powder substance discovered.
- LEO's responded – interviewed GRUBBS – admitted substance to be Methamphetamines
- LEO's arrested GRUBBS
- EIR is pending against GRUBBS

AR 000928

Passenger Arrested after Contraband Detected during Checkpoint Screening at (TPA) (12/09/09)

- (TPA) During Whole Body Imagery an anomaly was detected in rear pocket of Pax WALLACE
- During additional screening WALLACE removed contraband from his pocket.
- LEO's responded – interviewed WALLACE who claimed he got the substance from his brother
- LEO's tested substance – positive for cocaine
- LEO's arrested Wallace
- EIR was not initiated against WALLACE

AR 000929

Passenger Arrested after Contraband Detected during Checkpoint Screening at (TPA) (11/24/09)

- (TPA) During Whole Body Imagery screening an anomaly was detected on Pax VOGEN
- VOGEN was subjected to secondary screening – revealed a bag containing a green leafy substance
- LEO's responded – tested – positive for Marijuana - less than 20 grams
- LEO's arrested VOGEN
- EIR was not initiated against VOGEN

AR 000930

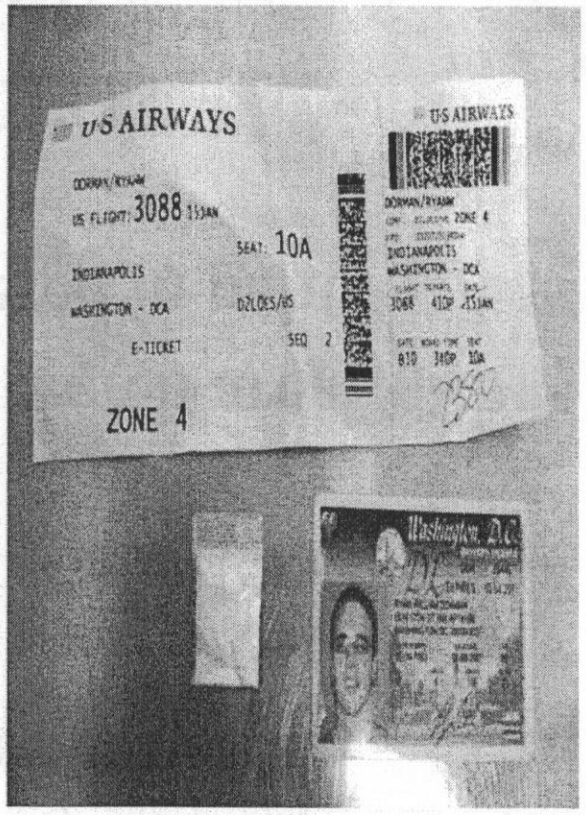
Suspicious Behavior during WBI Screening at (BWI) (12/30/09)

- (BWI)(12/29/09) Pax ALSHERI (traveling w/ Pax ALANAZI) carry-on bag selected for search – laptop in bag
- ALSHERI disclosed had cash in pockets – directed to Whole Body Imagery for screening
- Whole Body Imager alarmed – anomaly in crotch area
- Private screening – eight $100 bills discovered in pants
- LEO's responded – interviewed – cleared
- 12/30/09 FSD gathered information from TSO's – convinced Pax's conducting probes on security procedures

AR 000931

Suspicious Behavior during WBI Screening at (BWI) (01/15/2010)

- (IND) Whole Body Imagery detected anomaly on Pax DORMAN
- DORMAN divested small bag of white powdery substance during secondary screening
- LEO's responded – confiscated substance – Interview DORMAN who admitted having cocaine –arrested
- EIR was not initiated against DORMAN



AR 000932

Homeland Security

Secretary Napolitano Outlines Five Recommendations To Enhance Aviation Security

Release Date: January 7, 2010

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Department of Homeland Security (DHS) Secretary Janet Napolitano today joined White House Press Secretary Robert Gibbs and Assistant to the President for Counterterrorism and Homeland Security John Brennan to announce several recommendations DHS has made to the President for improving the technology and procedures used to protect air travel from acts of terrorism. Secretary Napolitano outlined five recommendations DHS will pursue to enhance the safety of the traveling public—developed as a result of the security reviews ordered by President Obama following the attempted terrorist attack on Dec. 25, 2009.

"The attempted attack on Christmas Day is a powerful illustration that terrorists will go to great lengths to try to defeat the security measures that have been put in place since Sept. 11, 2001," said Secretary Napolitano. "These recommendations will strengthen aviation security—at home and abroad—through new partnerships, technology and law enforcement efforts."

Secretary Napolitano outlined the following five recommendations:

- Re-evaluate and modify the criteria and process used to create terrorist watch lists—including adjusting the process by which names are added to the "No-Fly" and "Selectee" lists.
- Establish a partnership on aviation security between DHS and the Department of Energy 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.
- Accelerate deployment of advanced imaging technology to provide greater explosives detection capabilities—and encourage foreign aviation security authorities to do the same—in order to identify materials such as those used in the attempted Dec. 25 attack. The Transportation Security Administration currently has 40 machines deployed throughout the United States, and plans to deploy at least 300 additional units in 2010.
- Strengthen the presence and capacity of aviation law enforcement—by deploying law enforcement officers from across DHS to serve as Federal Air Marshals to increase security aboard U.S.-bound flights.
- Work with international partners to strengthen international security measures and standards for aviation security.

Secretary Napolitano will travel to Spain later this month to meet with her international counterparts in the first of a series of global meetings intended to bring about broad consensus on new international aviation security standards and procedures.

Deputy Secretary Jane Holl Lute, Assistant Secretary for Policy David Heyman and other senior Department officials already have embarked on a broad international outreach effort to meet with leaders from major international airports in Africa, Asia, Europe, the Middle East and South America to review security procedures and technology being used to screen passengers on U.S.-bound flights and work on ways to collectively bolster tactics for defeating terrorists.

Secretary Napolitano's recommendations come in addition to the Department's immediate actions following the attempted attack on Dec. 25, 2009—including enhanced security measures at domestic airports and new international security directives that mandate enhanced screening of every individual flying into the United States from or through nations that are State Sponsors of Terrorism or other countries of interest and the majority of all passengers traveling on U.S.-bound flights.

###

This page was last reviewed/modified on January 7, 2010.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

January 11, 2010

In U.S., Air Travelers Take Body Scans in Stride

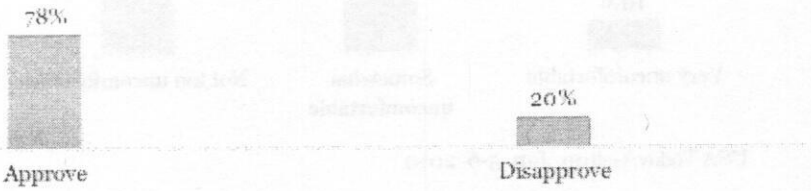
Seventy-eight percent approve of U.S. airports' using full body scans on passengers

by Jeffrey M. Jones

PRINCETON, NJ -- In the midst of renewed discussion of heightened security measures to thwart terrorist attacks like the Christmas Day attempt to blow up an airplane over Detroit, 78% of U.S. air travelers approve of U.S. airports' using full body scan imaging on airline passengers.

Approve/Disapprove of Full Body Scan Security Measures at Airports

One method of airport security that is expected to be used more widely at U.S. airports is a full body scan of passengers as they go through the security checkpoint. The full body scan would show a graphic image of a person's body underneath his or her clothes. The image would be viewed only by federal screeners in a separate, private room. Do you approve or disapprove of U.S. airports using the full body scan on airline passengers?



USA Today/Gallup, Jan. 5-6, 2010
Asked of air travelers
GALLUP

These results are based on a *USA Today*/Gallup poll conducted Jan. 5-6, including interviews with 542 regular air travelers, defined as those who have taken two or more air trips in the past 12 months.

The poll finds 29% of air travelers saying they are now more concerned about the safety of air travel than they were before Nigerian Umar Farouk Abdulmutallab allegedly attempted to detonate explosives hidden in his underwear. Current airport security measures, such as metal detectors, would not detect the type of explosives involved in the Detroit incident, but a body scan image would have. Thus, there are plans to expand the use of such machines at U.S. airports.

> "The majority, 67%, say they would not personally be uncomfortable in undergoing such a scan, with close to half (48%) saying they would not be uncomfortable at all."

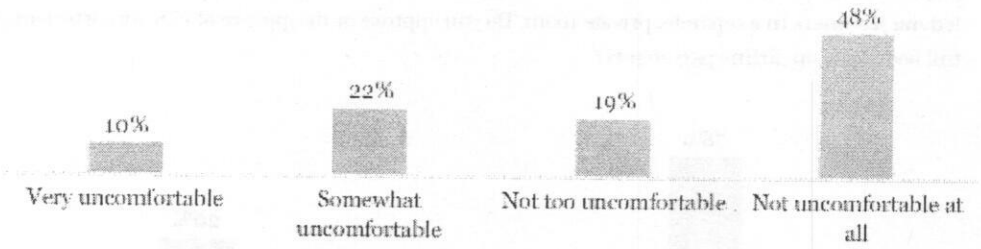
AR 000935

While some have expressed concerns about the implications of full body scans for passenger privacy, given the clarity of the images they would produce, airline passengers themselves do not seem fazed. Seventy-eight percent approve of the procedure, which was described to them as showing a "graphic image of a person's body underneath his or her clothes" that would be "viewed only by federal screeners in a separate, private room."

Additionally, the majority, 67%, say they would not personally be uncomfortable in undergoing such a scan, with close to half (48%) saying they would not be uncomfortable at all. Ten percent say they would be very uncomfortable if subjected to such a search.

How uncomfortable would you, personally, be with undergoing a full body scan at an airport security checkpoint -- very uncomfortable, somewhat uncomfortable, not too uncomfortable, or not uncomfortable at all?

Asked of air travelers



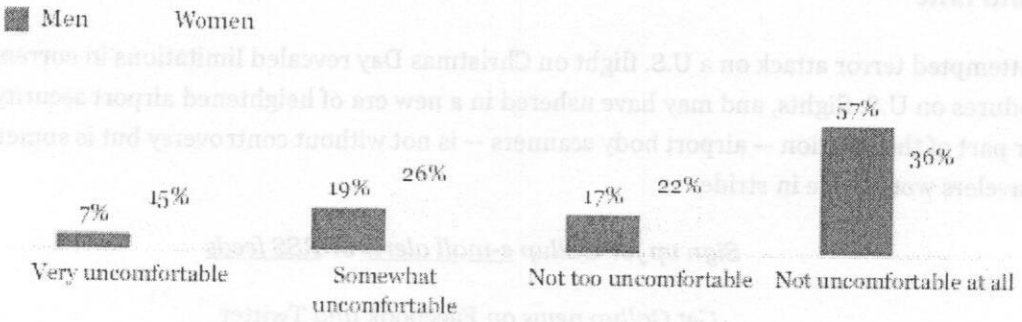
USA Today/Gallup, Jan. 5-6, 2010

GALLUP

There is a gender difference in the assumed level of discomfort, with female air travelers more likely than male travelers to express discomfort (41% to 26%). A majority of male air travelers say they would not be uncomfortable at all.

How Uncomfortable Undergoing a Full Body Scan at an Airport Security Checkpoint, by Gender

Asked of air travelers



USA Today/Gallup, Jan. 3-6, 2010

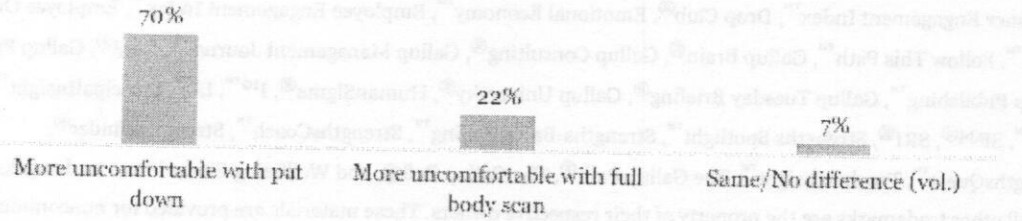
GALLUP

Perhaps as a result, men are also slightly more likely than women to approve of the use of body scan images (81% to 74%).

Air travelers would most likely not be required to undergo body scans at airports; they could instead opt to be searched or "patted down" by an airport security agent. Among air travelers, the choice is clearly in favor of body scans -- 70% say they would be more uncomfortable with being patted down, while 22% would be more uncomfortable in undergoing a body scan.

More Uncomfortable Security Procedure

As you may know, an alternative to a full body scan would be to have an airport security agent pat passengers down, that is to touch their bodies or clothing to search for hidden objects. Which method would make you more uncomfortable -- [ROTATED: having an airport security agent pat you down (or) undergoing a full body scan at the security checkpoint]?



USA Today/Gallup, Jan. 3-6, 2010
Asked of air travelers
(vol.) = Volunteered response

GALLUP

One reason air travelers generally approve of using full body scans may be because they believe scans will be effective at preventing terrorists from smuggling explosives or other dangerous objects onto

airplanes. Eighty-four percent say scans would be effective in this regard, including 38% who say they would be very effective. Thus, air travelers have a compelling reason to potentially counter any personal modesty issues they have related to body scans.

Bottom Line

The attempted terror attack on a U.S. flight on Christmas Day revealed limitations in current security procedures on U.S. flights, and may have ushered in a new era of heightened airport security. One major part of the solution -- airport body scanners -- is not without controversy but is something most air travelers would take in stride.

Sign up for Gallup e-mail alerts or RSS feeds

Get Gallup news on Facebook and Twitter

Survey Methods

Results are based on telephone interviews with 2,017 national adults, aged 18 and older, conducted Jan. 5-6, 2010. For results based on the total sample of national adults, one can say with 95% confidence that the maximum margin of error is ±3 percentage points.

For results based on the sample of 542 adults who have taken two or more air trips in the past year, the maximum margin of error is ±5 percentage points.

Interviews are conducted with respondents on land-line telephones and cellular phones

In addition to sampling error, question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of public opinion polls.

Copyright © 2010 Gallup, Inc. All rights reserved.
Gallup®, A^{8}™, Business Impact Analysis™, CE^{11}®, Clifton StrengthsFinder®, the 34 Clifton StrengthsFinder theme names, Customer Engagement Index™, Drop Club®, Emotional Economy™, Employee Engagement Index™, Employee Outlook Index™, Follow This Path™, Gallup Brain®, Gallup Consulting®, Gallup Management Journal®, GMJ®, Gallup Press®, Gallup Publishing™, Gallup Tuesday Briefing®, Gallup University®, HumanSigma®, I^{10}™, L^{3}™, PrincipalInsight™, Q^{12}®, SE^{25}™, SF^{34}®, SRI®, Strengths Spotlight™, Strengths-Based Selling™, StrengthsCoach™, StrengthsFinder®, StrengthsQuest™, TeacherInsight™, The Gallup Path®, The Gallup Poll®, and Wellbeing Finder™ are trademarks of Gallup, Inc. All other trademarks are the property of their respective owners. These materials are provided for noncommercial, personal use only. Reproduction prohibited without the express permission of Gallup, Inc.

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

January 19, 2010

The Honorable Dianne Feinstein
United States Senate
Washington, DC 20510

Dear Senator Feinstein:

Thank you for your December 29, 2009 letter regarding the attempted detonation of an explosive device on Northwest Airlines Flight 253 on Christmas Day. This incident is a powerful illustration that terrorists will go to great lengths to try to defeat the evolving security measures put in place since September 11, 2001.

On January 7, 2010, President Obama spoke to the American public regarding the findings of the reviews that he ordered into our terrorist watch list system and air travel screening. The President simultaneously issued a directive for multiple Federal departments and agencies, ordering corrective actions with respect to intelligence, screening, technologies, and watchlisting systems and programs.

The Department of Homeland Security (DHS) is assessing its own security processes at domestic airports and the requirements at foreign airports that serve as last points of departure to the United States. DHS's Transportation Security Administration (TSA) does not conduct the screening at foreign airports. Accordingly, I dispatched Deputy Secretary Jane Holl Lute, Assistant Secretary for Policy David Heyman, and other senior Department officials to review the security procedures and technology used to screen passengers on flights bound for the United States with aviation security leaders in Africa, Asia, Europe, the Middle East, and South America. Deputy Secretary Lute and Assistant Secretary Heyman have just returned and will continue the dialogue with our international partners to strengthen our tactics for defeating terrorists. I will follow up on these efforts in ministerial-level meetings within the next few weeks.

Regarding checkpoint screening technologies, TSA is accelerating its efforts to acquire and deploy Advanced Imaging Technologies (AIT), such as the Backscatter X-ray and Millimeter Wave systems, to increase the probability of detecting explosives and other threats concealed on passengers. This technology will form one layer of a multi-layered system. TSA bought 150 AIT systems using *American Recovery and Reinvestment Act of 2009* funding and will acquire an additional 300 in upcoming weeks. TSA will also expand the use of Explosives Trace Detectors in multiple scenarios to test passengers for the presence of particles that may

indicate contact with explosive material. I am also establishing a partnership with the Department of Energy to leverage fully the National Laboratories in spurring technology innovation that will help keep us ahead of evolving threats.

Thank you again for your letter. I greatly appreciate and share your concerns over the events surrounding the attempted terrorist attack. I hope to continue to foster a close working relationship with you on this and other homeland security matters. Should you need additional assistance, please do not hesitate to contact me at (202) 282-8203.

Yours very truly,

Janet Napolitano

DEC. 29. 2009 5:23PM NO. 0837 P. 1

FAX from . . .

Senator Dianne Feinstein

of California

331 Hart Senate Office Building
Washington, DC 20510
(202) 224-3841

DATE: 12-29-09

TIME: _____

TO: Secretary Napolitano
c/o Ms. Chani Wiggins

FROM: David Grannis : office of
Senator Dianne Feinstein

COMMENTS:

2009 DEC 31 10:15

Received

DEC 30 2009

Office of Legislative Affairs

TOTAL NUMBER OF PAGES (INCLUDING COVER SHEET): 2

NOTE: The information contained in this facsimile is confidential. If you receive this transmission in error, please notify the sender immediately.

TSA-091231-001

DIANNE FEINSTEIN
CALIFORNIA

SELECT COMMITTEE ON INTELLIGENCE - CHAIRMAN
COMMITTEE ON APPROPRIATIONS
COMMITTEE ON THE JUDICIARY
COMMITTEE ON RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510-0504
http://feinstein.senate.gov

December 29, 2009

2009 DEC 31 P 05:15

The Honorable Janet Napolitano
Secretary of Homeland Security
Washington, DC 20528

Dear Secretary Napolitano,

I am very concerned that the nation's means of detecting explosives, especially by the Transportation Security Administration at U.S. and international airports, are not keeping up with the nature and sophistication of the terrorist threat.

The recent case of Umar Farouk Abdulmutallab demonstrates how terrorists with no more than moderate training have been able to bypass standard security checks. Another case in point is the attempted assassination attempt on Saudi Prince Muhammad bin Nayef, in which the placement of the explosive (as opposed to the nature of the explosive used) was able to evade detection.

I understand that more advanced detection technologies, including backscatter x-ray machines, have been deployed to some U.S. airports, but their use is still not widespread and may face difficulties in scaling up to full usage. I therefore ask how the Department, and the TSA in particular, intends to implement the changes necessary to ensure that would-be terrorists won't be able to bring explosives or other prohibited weapons onto airplanes or other restricted areas.

Finally, let me share with you what I have also communicated to the Intelligence Community – that individuals coming to the attention of the U.S. Government through warnings by family members concerned about radicalization should be immediately placed on the selectee or no-fly lists to prevent potential terrorist attacks.

Please have the relevant officials in your Department contact Dan Wessel in my office with any questions or to provide a response to my request for additional information.

Sincerely,

Dianne Feinstein

Question#:	1
Topic:	role
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), the National Counterterrorism Center (NCTC) serves as the primary organization in the U.S. Government for integrating and analyzing all intelligence pertaining to counterterrorism (except for information pertaining exclusively to domestic terrorism [which is the responsibility of the Federal Bureau of Investigation]). However, the Homeland Security Act of 2002, assigns the intelligence component of DHS with the responsibility to receive, analyze, and integrate law enforcement and intelligence information in order to "(A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities to the homeland."

What role does DHS have under law and in practice for evaluating threat streams and warning of possible terrorist attacks?

Response: The Homeland Security Act of 2002 assigns DHS the primary mission to "prevent terrorist attacks within the United States" and "reduce the vulnerability of the United States to terrorism." Pursuant to section 201(d) of the Act, DHS satisfies these requirements by analyzing all-source intelligence and information from DHS Component organizations, other Federal, state and local government agencies—including intelligence and law enforcement partners—and the private sector. This analysis is used to identify potential threats and to provide warnings of possible terrorist attacks, and indicators of terrorist tactics, techniques, and procedures.

DHS has the specific responsibility in 201(d)(9) "to disseminate" information it analyzes "… in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States." Pursuant to sec. 203 of the Act, DHS also "administer(s) the Homeland Security Advisory System…to provide advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland." In fulfilling these responsibilities, DHS consults with the DNI, the Intelligence Community, law enforcement, and other elements of the Federal government to establish collection priorities and strategies for information relating to terrorist threats [201(d)(9)], and with state and local governments and private sector entities to ensure information relating to terrorist threats is appropriately exchanged [201(d)(9)].

To this end, DHS produces a variety of analytical products for distribution to various customer sets, including intelligence assessments, Roll Call Releases, joint bulletins on

Question#:	1
Topic:	role
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

time-sensitive events, reference aids, daily summaries, and tailored responses to inquiries. The Department also provides weekly, tailored briefings to its state and local customers, and ad hoc briefings to all its customers, as warranted.

Question: Specifically, regarding the intelligence that the President's summary states was available prior to the attempted bombing of NW-253, did DHS have access to that intelligence? That is, was the intelligence disseminated to DHS or was it available in databases to which DHS personnel had access? If so, what did DHS do with that information, or with the database access?

Response: Intelligence information relating to Umar Farouk Abdulmutallab was available to DHS and the entire Intelligence Community prior to December 25, 2009. Mr. Abdulmutallab was entered into the Terrorist Identities Datamart Environment (TIDE), maintained by the National Counterterrorism Center. However, the derogatory information associated with that record, based on the policy in place at that time, was insufficient for him to be watchlisted through the Terrorist Screening Database (TSDB, the U.S. Government's consolidated terrorist watchlist). It was also insufficient to have him placed on the No Fly list which would have prevented him from boarding, or subjected him to additional screening prior to boarding Northwest Flight 253. At the time of his travel, a Consolidated Lookout and Support System (CLASS) notice had been posted for Mr. Abdulmutallab, but these records did not meet the criteria for referral to IAP officers in Amsterdam prior to boarding. Since this incident, CBP has added CLASS lookouts with terrorism-related indicators to the pre-departure vetting criteria.

While in flight, U.S. Customs and Border Protection (CBP) officers in Detroit conducted a screening of inbound flights against a consolidated system that included the State Department's CLASS database. Mr. Abdulmutallab was identified as a match to the record and CBP officers were awaiting his arrival to conduct an in-depth interview.

Question#:	2
Topic:	NCTC
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: What presence does DHS have at NCTC and what functions do DHS analysts perform there?

How do DHS analysts at NCTC interact with their counterparts at the DHS Office of Intelligence and Analysis and with the intelligence staffs of the DHS components? Are DHS personnel at NCTC permitted to share what they learn, or have access to, at NCTC with DHS officials in DHS's operational components? If not, why not? Should this be corrected?

Response: DHS currently has 17 analysts assigned to the National Counterterrorism Center (NCTC), as broken out below:

- Office of Intelligence and Analysis (I&A) – 11
- National Protection and Programs Directorate – 1
- United States Citizenship and Immigration Services – 1
- United States Coast Guard - 4

In general, analysts detailed to NCTC operate as NCTC employees, not as DHS liaisons, and they are fully integrated into NCTC's analytic management structure. While these analysts maintain reach-back capabilities and apply their expertise and experiences in Homeland intelligence analysis to the intelligence topics they are assigned, their roles are determined by NCTC management. The analysts have individual analytic accounts for which they are responsible, and have full access to intelligence available to other analysts in NCTC.

DHS analysts assigned to NCTC share intelligence and coordinate with DHS under NCTC's guidelines, as appropriate with the parameters of the clearance levels and need-to-know of counterpart DHS analysts. Coordination is generally accomplished through I&A, with I&A performing any onward coordination with the Intelligence Enterprise within those same parameters.

Among I&A's contribution to NCTC are two detailees to the Interagency Threat Assessment and Coordination Group (ITACG), as well as three individuals from state, local, and tribal organizations, who are "federalized" as I&A employees and detailed to NCTC. Rather than being integrated into an NCTC work unit, one I&A detailee leads the ITACG under NCTC's management, and the second serves as a senior analyst supporting the ITACG mission. The federalized detailees from state, local, and tribal organizations

Question#:	2
Topic:	NCTC
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

serve as the ITACG's core, providing crucial advice and insights into state, local, and tribal needs and interests. Each of these detailees has access to NCTC systems, but his work focuses on reviewing finished production, rather than original intelligence analysis. Each works with all agencies that support intelligence collection and dissemination from within the NCTC analytical offices to ensure that relevant information is shared with state and local customers.

Under NCTC's information sharing guidelines, because NCTC has direct access to many sensitive compartmented systems from across the federal government, NCTC employees – including DHS detailees – are necessarily constrained from sharing information derived from those sources, pursuant to arrangements with the agencies that own them. NCTC's guidelines in this regard raise issues for DHS under the following circumstances:

- When DHS analysts co-author or provide significant input to an NCTC product based on unique Homeland equities, lack of access to all relevant materials can skew otherwise valuable and relevant input we can provide.
- When DHS analysts are assigned to specialized projects at NCTC, as opposed to a routine detail to an NCTC analytic team, we believe that these guidelines should be reconsidered so that the analyst has the authority to maximize reachback to contribute Homeland inputs.

A direct line of communication and information exchange in a 24/7 basis must be created between the NCTC and the DHS National Operations Center (NOC). NOC employees must be fully integrated within the Intelligence Community (IC) and able to contact and exchange intelligence information with the NCTC independently from DHS I&A.

In addition to this a Congressional study must analyze which counterterrorism functions currently under the FBI National Security Branch must be better placed under DHS I&A and DHS NOC. Those functions must be transitioned to DHS within a period 6 months from the date of the study.

Question#:	3
Topic:	ATS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: CBP uses the Automated Targeting System (ATS) at its National Targeting Center to identify high risk passengers and cargo shipments. The passenger component of ATS processes traveler information against other information available to ATS and applies threat-based scenarios comprised of risk-based rules to assist CBP officers in identifying individuals who require additional screening or in determining whether individuals should be allowed entry into the United States. It was reported that CBP officers learned of Abdulmutallab's possible extremist links while NW-253 was airborne on December 25 as a result of cross-checking his name with the State Department's CLASS database. As a result, CBP officers intended to question him when he landed.

Was the determination to question Abdulmutallab upon landing based on the risk-based rules within the ATS system or purely on the CLASS entry or other intelligence information?

Response: Based on the Department of State (DOS) record, Abdulmutallab would have been referred to secondary inspection upon his arrival in Detroit. The risk-based rules in the ATS passenger module are designed to identify higher-risk travelers whose travel parameters match threat-based scenarios, but who do not have pre-existing lookout records.

Question: Why was the CBP security assessment of passengers for NW-253 not completed prior to departure of the flight?

Response: CBP assessments are an on-going process that generally start 72 hours prior to a flight's departure when Passenger Name Record (PNR) information from the airlines reservation system is transmitted to CBP and processed in the Automated Targeting System – Passenger (ATS-P) to the passenger's arrival at a U.S. airport. Beginning at 72 hours CBP can identify potential watchlist matches and patterns of illicit activity through the analysis of PNR. PNR data can be carrier reservation data and so is not standardized. As a result, a given PNR record may not always have full information on a traveler. For example, travel document information or method of payment may not be present. Once Advance Passenger Information (API) is received from the airline, prior to the flight's departure (API contains complete biographic information taken from the passenger's travel document at check-in) the passenger manifest is processed through the risk-based rule scenarios in ATS-P and additional lookouts may be found or possible lookouts may be confirmed. In the NW 253 case there were no records available to ATS-P that would have warranted CBP intervention to prevent Abdulmutallab from boarding the flight

Question#:	3
Topic:	ATS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

because the State Department record present did not rise to the level of pre-departure vetting. In particular, the failure of the USG to watchlist Abdullmutallib hampered CBP's ability to take action prior to departure.

Question: Is it standard practice to cross-check passenger lists as soon as they are received (e.g., up to 72 hours in advance of departure) against the entire TSDB and the NCTC TIDE database? Was that done in this case? Should this be standard procedure?

Response: CBP utilizes the Advance Passenger Information System to screen passenger manifest data against the TSDB, including the No Fly and Selectee lists, but not TIDE. CBP automated checks also include (the U.S. Government's consolidated terrorist watchlist), as well as visa revocation records, Electronic System for Travel Authorization (ESTA) denials, lost/stolen passport records, public health records, and other information. As a result of gaps identified from the NW 253 incident, Department of State records related to terrorism are now also included in the initial security screenings prioritized for action by the ATS-P Hot List. The TIDE database is a classified repository that contains the underlying derogatory information on persons who are watchlisted in the TSDB. Subjects in the TIDE are included in the TSDB when they meet the interagency defined and agreed to criteria for terrorist watchlisting.

Question: If the CBP security assessment of passengers had been completed prior to departure, would Abdulmutallab still have been allowed to board?

Response: If CBP had conducted a pre-departure screening which included vetting against the Department of State's records related to terrorism it is possible that Abdulmutallab would still have been permitted to board the aircraft, because there were no significant lookouts in the systems, e.g. no visa revocation by Department of State and neither TSDB nor No Fly/Selectee record.

Question: Would he have been subjected to additional screening or questioning?

Response: At the time the Advance Passenger Information data was provided to CBP, the record in TECS for Abdulmutallab that had been received from State was not coded as a TSDB or terrorist related record, and CBP's Automated Targeting System did not flag him as requiring additional screening by CBP IAP officers at Amsterdam-Schiphol International Airport. Since December 25, CBP has modified its automated screening procedures to identify State Department records pertaining to terrorism which results in additional screening.

Question: Were there DHS personnel at the departing airport?

Question#:	3
Topic:	ATS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Response: Yes, Abdulmutallab would have received additional screening prior to departure from Amsterdam and upon arrival at the port of entry.

Question: Had the security assessment been completed on the basis of the passenger list provided 72 hours in advance, could DHS personnel have traveled to Amsterdam to interview Abdulmutallab if they were not already there?

Response: IAP officers were on-site at Amsterdam. At the time the Passenger Name Record data was provided to CBP, the record in TECS for Abdulmutallab that had been received from State was not coded as a TSDB or terrorist related record, and CBP's Automated Targeting System did not flag him as requiring additional screening by CBP IAP officers at Amsterdam-Schiphol International Airport.

Since this time, CBP has changed its procedures so that it now focuses on identifying high-risk passengers and other inadmissible aliens prior to travel in an effort to prevent their departure prior to boarding commercial carriers bound for the United States from non-IAP overseas locations. CBP does this for IAP and non-IAP locations, by identifying all passengers who are possible matches to Terrorist Screening Database (TSDB including No Fly List records), Electronic System for Travel Authorization (ESTA) denials, Visa Revocation, Public Health, Lost or Stolen Passports (non-US) hits and all Department of State TECS records with terrorism related exclusion.

The CBP National Targeting Center-Passenger (NTC-P) coordinates with IAP offices, Immigration Customs Enforcement (ICE) Attachés, CBP Attachés, and the Regional Carrier Liaison Group (RCLG) to assist with notifying specific airlines and that these identified subjects do not board an aircraft destined to the United States.

Question#:	4
Topic:	CAPPS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Were the passengers on NW-253 screened through the Transportation Security Administration's Computerized Passenger Pre-Screening System (CAPPS) or other DHS computer-assisted risk analysis capabilities? If not why not?

Response: The passengers aboard NW 253 were screened against CBP's Automated Targeting System-Passenger.

Question#:	5
Topic:	criteria
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Does the Computer-Assisted Passenger Prescreening System (CAPPS) or other Department of Homeland Security (DHS) computer-based analysis system's screening algorithms include any current intelligence information, or is it based solely on criteria such as a passenger's nationality, ticketing, itinerary, frequent flyer status, etc.? Do the DHS organizations that operate these risk-analysis tools have access to intelligence databases, or are there intelligence agency personnel detailed there who can search the intelligence holdings of their home agencies? If not, why not? Why not conduct risk analysis against all the data at the government's disposal?

Response: The Department of Homeland Security (DHS) has computer-based algorithms in place that are informed by intelligence and operational information. These algorithms utilize available passenger data. The DHS organizations that operate these algorithms – which include Intelligence and Analysis (I&A), the Transportation Security Administration, and the U.S. Coast Guard – have direct access to intelligence databases as well as Intelligence Community (IC) agencies. DHS also has personnel detailed to IC agencies under various agreements and understandings. DHS conducts terrorism risk analysis by leveraging the most relevant data available, including all source intelligence information.

Question#:	6
Topic:	VSP - 1
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: As you know, Immigration and Customs Enforcement's (ICE's) Visa Security Program deploys special agents to high-risk visa activity posts to conduct in-depth reviews of individual visa applicants. In 2005, the Government Accountability Office observed that these agents would benefit from greater language proficiency for interviewing applicants and reviewing files. Likewise, a 2008 Department of Homeland Security (DHS) Inspector General report stated that language skills appear to be very important at some posts.

Since these reports were issued, has DHS made any changes to the language training and proficiency requirements for ICE's Visa Security Officers? If so, please describe these changes. If not, please discuss whether DHS plans to review the requirements and any anticipated changes to them.

Response: DHS has participated in language training as recommended by the DHS IG report. For example, Special Agents assigned to Jakarta, Indonesia attended language training at the Department of State's Foreign Service Institute prior to deploying to post. In some instances, DHS has been able to assign agents proficient in a language to a particular post. This was the case in both Manila and Frankfurt. ICE has recently made language training available through a contract with Rosetta Stone. This training is available to Special Agents both before and during their overseas deployments. Additionally, all ICE offices with Visa Security responsibilities hire locally engaged staff who are proficient in the local language and who are available to assist in interviewing applicants and reviewing files.

Question#:	7
Topic:	resources
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The Transportation Security Administration's (TSA) Office of Global Strategies develops and promotes effective transportation security processes worldwide. It relies on its overseas TSA representatives to align security between the U.S. and foreign governments and to assess foreign airports and air carriers. Since the Christmas Day attempt, what is DHS doing to ensure TSA has adequate staff and resources to reduce aviation security risks before they reach our shores?

Response: The President's budget proposal for fiscal year (FY) 2011 reflects an increase of $38.8 million for TSA's Office of Global Strategies (OGS) to support international outreach efforts, conduct assessments of international airports and inspections of foreign and domestic air carriers with flights to and from the United States, provide necessary security training to foreign governments, and evaluate the data identified through the assessment process in order to develop more robust systems and processes to better analyze the risk and institute appropriate security measures to prevent and deter terrorist acts. The requested resources will enable TSA to increase staffing levels by an additional 34 Transportation Security Specialists, 10 International Industry Representatives, 20 desk officers/analysts to support field operations, trend and risk analysis, and provide overall program support, and 10 personnel for Aviation Security Sustainable International Standards Teams and Rapid Response Teams. TSA will fund an additional three (3) Transportation Security Administration Representatives from existing resources.

Question#:	8
Topic:	scanning
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: There were recent media reports that whole body imaging and related scanning technology may not detect small amounts of explosives. Please discuss the extent to which these concerns are valid. If needed, please provide any classified information to my staff through Senate Security.

Response: Advanced Imaging Technology (AIT) systems provide TSA with added capability to address explosives (bulk, liquids, and powders), as well as both metallic and nonmetallic weapons and prohibited items, based on the Transportation Security Officer's (TSO) visual interpretations of passenger imagery. The detection capabilities of TSA's AIT and related scanning technologies is sensitive information and can be provided to the Committee in the appropriate forum.

Question#:	9
Topic:	WBI
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: In President Obama's January 7, 2010, memo about the attempted attack on Christmas Day, he assigned you with the task of "aggressively pursuing enhanced screening technology consistent with privacy and civil liberties." As you know, some privacy groups have argued that current whole body imaging technology may be too invasive.

Are DHS and TSA looking into whole body imaging equipment that may be less invasive but just as effective, such as passive millimeter wave technology?

Some small businesses may not have the capital to produce additional units of promising whole body imaging technology to support DHS and TSA testing and evaluation requirements. How are DHS and TSA handling this issue, and are they providing any funding to support the testing and evaluation of promising technology developed by small businesses?

Response: The Transportation Security Administration (TSA) continues to evaluate different Advanced Imaging Technologies (AIT), including passive millimeter wave units, as part of the ongoing acquisition process for these systems. During this process TSA continues to seek effective technologies that protect travelers' privacy and civil rights and civil liberties. Currently, Transportation Security Officers (TSOs) view AIT images from a remote location and have no contact with the passenger. Further, the AIT images are partially obscured by installed privacy algorithms and images are not stored. TSA is working with the Department of Homeland Security's Science and Technology Directorate (DHS S&T), the security industry, and international government partners to develop an automated threat detection capability. The objective of Automated Target Recognition detection algorithms is to provide effective detection performance without the need for TSOs to interpret the passenger imagery to identify potential threat items. Instead, the technology would flag anomalies for further TSO screening on a representative image of the human body.

In order to adequately evaluate the system performance of any technology, TSA requires a certain quantity of systems from vendors for test and evaluation. This is especially important during the operational testing of technologies, where technologies must be tested at a variety of airports with different operators, travel characteristics (type of baggage, passenger clothing, etc.) and physical environments (altitude, humidity, temperature, etc.). While TSA tries to limit the number of systems requested from vendors for testing, the aggressive acquisition, budgeting, and deployment schedules that

Question#:	9
Topic:	WBI
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

are required to ensure a timely rollout of security technologies often require simultaneous testing at multiple laboratories and airports. Additionally, as pertains to funding for testing, the DHS S&T conducts all research and development for the TSA, including providing funding for the development and testing of emerging technologies.

Question#:	10
Topic:	database
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: The initial error in failing to accurately determine whether Abdulmutallab had a valid visa was caused by a slight misspelling. This error is similar to the mistakes made by Customs and Border Protection in failing to identify a Mexican national with a multiple-drug-resistant form of Tuberculosis who was able to enter the U.S. twenty-one times, even after DHS had his last name and date of birth.

With the Mexican national, DHS acknowledged that its border screening database was antiquated and lacked sophisticated search functions. After this Committee's hearing and investigation into that incident in 2007, I understand that these technological limitations were addressed.

Secretary Napolitano, the Department of Homeland Security has access to the Consolidated Consular Database that holds U.S. visa records. Do you know if this database has been enhanced to provide matches for searches with near, but not exact, name matches to accommodate for misspellings?

Response: TECS and Automated Targeting System algorithms are established to provide appropriate levels of matching for advance passenger information, primary, and secondary passenger screening.

CBP continuously evaluates and enhances matching algorithms to ensure levels of flexibility and sensitivity to provide users with appropriate matches. In particular, CBP's TECS Modernization effort is looking at options for new and enhanced matching algorithms.

Question#:	11
Topic:	VSP - 2
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: At the hearing, I questioned you about delays in obtaining final DHS approval for the expansion of ICE's Visa Security Program to three State Department consular posts overseas. In response to my questions, you stated that you were unsure how long the requests for deployment to these posts had been waiting for your approval. When did the Secretary's Office receive each of the requests? And when did you approve them?

Response: The below chart indicates the dates on which ICE submitted five NSDD-38 applications to DHS for approval, and the corresponding dates on which DHS approved the respective applications.

ICE Attaché Office - VSP	NSDD-38 Sent to DHS for Approval	DHS Approval Date
Sana'a, Yemen	**9/8/2008**	**1/14/10**
Frankfurt, Germany	**9/25/2009**	**1/14/10**
Amman, Jordan	**9/25/2009**	**1/14/10**
Tel Aviv, Israel	**9/25/2009**	**1/15/10**
Jerusalem	**9/25/2009**	**1/15/10**

Question#:	12
Topic:	GAO
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In October, The Government Accountability Office (GAO) released a report on the Transportation Security Administration's (TSA) airport passenger screening technology. In the report, GAO recommends that the TSA "ensure that technologies have completed operational tests and evaluations before they are deployed."

What is the process for testing airport screening technology before it is deployed?

Do all airport screening technologies go through this process?

Please describe how long and what type of operation scenarios do you recreate to test this machines.

Response: The Transportation Security Administration (TSA) implements a robust Testing and Evaluation (T&E) program in accordance with Department of Homeland Security (DHS) policy and management directives to ensure that the operational effectiveness and suitability of candidate security technology systems are evaluated in both a laboratory and field environment prior to deployment. This process leverages data from multiple developmental and operational testing sources, accredited vendor data, modeling and simulation, and other special analyses (as required), in accordance with T&E and systems engineering principles and best practices. Security technologies undergo laboratory testing to verify conformance with technical standards and requirements, which includes requirements for probability of detection, false alarms rates, screening/decision time, health and safety, privacy, human factors engineering, etc. Laboratory testing is conducted primarily at the DHS Science and Technology Directorate's Transportation Security Laboratory in Atlantic City, NJ, but may also take place at a variety of other facilities, such as the Department of Defense laboratories or the Department of Energy National Laboratories. Depending on the technology, the TSA may also utilize the TSA Systems Integration Facility (TSIF, located in Arlington, VA) to conduct additional operational scenario and Concept of Operations testing on security technologies before they are fielded. Operational testing and evaluation (OT&E) is typically conducted within the intended field environment (typically, multiple aviation facility checkpoints) for a period of 30-60 days, with representative Transportation Security Officers (TSOs) operating under the intended concept of operations. OT&E testbed sites are chosen based on their ability to reflect the anticipated utilization rates, operational tempos, and mix of passengers and carry-on items representative of the intended deployment. In addition, threat surrogates are employed to the extent practical as part of the OT&E effort, to gauge system performance in a more realistic environment.

Question#:	12
Topic:	GAO
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Testing results are then compiled and analyzed. A determination is then made as to the overall operational effectiveness and suitability. These results are briefed to TSA leadership, the DHS Director of Operational Test and Evaluation (for oversight programs), and the relevant Acquisition Review Board.

Question#:	13
Topic:	puffer
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Which versions of the explosive trace portal devices, also known as "puffer machines" have operational testing and which ones did not? Were they operationally tested and for how long? Did TSA have problems with the machines during operational testing? If they were not tested was there an official reason for that?

Response: Both fielded versions/vendors of the Explosives Trace Portal (ETP) were tested in an operational setting prior to full scale deployment. The Transportation Security Administration (TSA) proceeded with airport operational assessments by fielding five (5) commercial General Electric (GE) Entry Scan ETP systems in 2004. TSA proceeded with another round of operational assessments at multiple airports from April to May 2005 on both the GE and Smiths Sentinel II ETP to further validate operational suitability. Field test results demonstrated satisfactory performance, indicating the equipment was ready for full scale deployment. In April 2006 TSA began deploying ETPs to airports.

In 2006, TSA initiated another round of laboratory testing of the ETP to evaluate its effectiveness in detecting live explosives. During April and May of 2006, Idaho National Engineering and Environmental Laboratory conducted testing on both vendor submissions, which revealed a significant deficiency in the GE ETP's ability to detect certain explosive compounds. Once these test results were received, along with exhibited reliability, maintainability, and availability issues with the fielded units, TSA formally notified the ETP vendor in June of 2006 that TSA would not deploy any additional ETPs until the detection capabilities and reliability issues were addressed. Remaining delivery units were diverted to the TSA warehouse until improvements could be completed and verified.

Question#:	14
Topic:	plans
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: I am concerned that our screening efforts may be chasing the last threat rather than the next one. In the Wall Street Journal, put it succinctly when he said, "to inspect all shoes after the shoe bomber almost succeeded, or to pat down passengers after the underwear bomber almost succeeded, provides no defense against the next techniques that could be tried at any time." Has TSA developed a comprehensive airport passenger screening plan that not only looks at present day threats but also looks down the road at newer threats?

Response: The Transportation Security Administration (TSA) considers this question to be central to its mission. Terrorist adversaries are highly adaptive and have shown they are capable of exploiting vulnerabilities in the aviation system. TSA employs a layered risked based security strategy to counter specific and general threats.

The use of intelligence informs TSA on the development of countermeasures to mitigate future threats. Over the past year, TSA has developed two inter-related processes increasing the likelihood that deployed countermeasures will mitigate both current and emerging threats. TSA has developed a risk analysis capability to assist resource allocation. In addition, TSA has developed a risk-based "capability-gap" process to identify the gaps between current capabilities and those needed to mitigate a portfolio of threat scenarios, including emerging threats. Through both risk analysis and the capability-gap process, TSA deploys "threat-agnostic" countermeasures capable of addressing a broader set of threats because their security design does not rely on assumptions about what form the threat might take. For example, Behavior Detection Officers (BDO) look for anomalous behaviors rather than a particular explosive or weapon. As a result, BDOs have a broader range of threat coverage and are less dependent on an assumption of which weapon terrorists will use in order to provide effective security.

In addition, TSA works with the Department of Homeland Security's Science and Technology Directorate and industry to advance the detection capabilities and operational suitability of a wide variety of screening technologies. TSA continues to support the development of emerging technologies that offer advanced screening capabilities while minimizing impact to the traveling public.

Question#:	15
Topic:	testing
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: TSA is currently deploying whole body imagers in airports. Have the whole body imagers that TSA plans to purchase in 2010 been operationally tested and for how long?

Response: The Transportation Security Administration (TSA) has been testing and evaluating Advanced Imaging Technology (AIT) for almost three years. Through covert testing, ongoing airports assessments, developmental testing in a laboratory environment, and operational testing in the field environment, AIT has proven itself as an effective tool to assist TSOs with the detection of metallic and nonmetallic threats in the laboratory and in the field. Initial product demonstrations and laboratory testing were conducted at the Transportation Security Laboratory from February to May 2007. Operational testing of AIT included:

- Initial product demonstrations and laboratory testing at the Transportation Security Laboratory from February to May 2007;
- Operational utility evaluations (OUEs) at multiple airports from August 2007 to July 2008
    a. Sept 2007 – TSA awarded contracts for a limited number of systems to millimeter wave (MMW) and backscatter manufacturers for preliminary deployments to support extended surveillance
    b. MMW OUEs and field trials from November to December 2007 at Phoenix Sky Harbor International Airport (PHX); May to June 2007 at Los Angeles International Airport (LAX) and John F. Kennedy International Airport (JFK)
    c. Backscatter field trials OUEs from February to April 2008 at PHX; June 2008 at LAX; and July 2008 at JFK.
- Summer 2009 – Conducted Operational Testing and Evaluation (OT&E) and field trials of next-generation (AIT-2) MMW at George Bush Intercontinental Airport (IAH), Cleveland Hopkins International Airport (CLE), and Burbank-Glendale-Pasadena Airport (BUR); AIT-2 backscatter systems at IAH, CLE, and Greater Rochester International Airport (ROC) which provided the basis for recent procurement decisions.

TSA continues to evaluate other vendors' AIT proposals.

Question#:	16
Topic:	devices
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Are all the airport screening devices purchased under the American Recovery and Reinvestment Act being operationally tested?

Response: Yes, all airport screening devices purchased under the American Recovery and Reinvestment Act undergo laboratory (developmental) testing as well as operational testing and evaluation in the field. They also meet the Transportation Security Administration's established requirements for each specific technology.

Question#:	17
Topic:	health
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: As a doctor, I am concerned with the possible health effects associated with whole body imagers. Have the whole body imagers that TSA plans to purchase been tested for possible exposure to unhealthy levels of radiation or other health hazards?

Response: In its solicitation, the Transportation Security Administration references nationally recognized applicable safety standards for various forms of Advanced Imaging Technology (AIT). Vendors are required to demonstrate compliance to these standards prior to entering laboratory trials. Backscatter imaging results in exposures of less than 10 microREM. This is equivalent to the exposure each person receives in about 2 minutes of airplane flight at altitude or every 15 minutes from naturally occurring background radiation. The technology meets the American National Standards Institute standard for personnel security screening systems using X-rays. Millimeter wave AIT systems are also safe, utilizing energy frequency levels that are 10,000 times less than what is permitted for a cell phone. The average exposure time for a passenger being scanned by a millimeter wave AIT system is far less than the time that the average citizen is exposed to higher frequency cell phone transmissions throughout the day.

Question#:	18
Topic:	decision
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that domestic flights in the air on Christmas night were not made aware of the emergency security directive. What was the reasoning for only alerting inbound transatlantic flights of the new directive? Who ultimately makes that decision?

Response: After being made aware of the incident onboard Northwest Flight 253, the Transportation Security Administration (TSA) convened a Senior Leadership Team Conference Bridge to evaluate the incident and order appropriate action. Based upon our understanding of the incident and related intelligence at the time and advice from the Federal Aviation Administration on the number of flights in-bound, the Acting Assistant Secretary ordered that flights to the United States from European locations be apprised of the incident. As we continue to evaluate our response to the NW 253 incident, we are reviewing our protocols to notify aircraft in the air.

In addition, TSA ordered additional security measures on these flights as well. As our response to the incident progressed, TSA expanded additional security measures to all international flights to the United States. Within five hours of issuing a Security Directive and Emergency Amendment ordering these measures, approximately 95 percent of our partners reported being in full compliance.

Question#:	19
Topic:	directive
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: On January 4, TSA issued a new security directive to focus on more extensive screening of passengers flying from certain countries of interest. Was this decision made based on intel gathered from the Christmas Day terrorist himself or from other outside intelligence?

Response: The countries of interest listed in the Transportation Security Administration's Security Directive issued subsequent to the December 25, 2009, incident were selected based on information contained in Chapters Three (State Sponsors of Terrorism) and Five (Terrorist Safe Havens) of the State Department 2008 Country Reports on Terrorism, as well as information provided in Department of Defense country threat assessments. Additionally, two countries were identified based on a number of threat and aviation security factors. The list was coordinated with the U.S. State Department.

Question#:	20
Topic:	briefing
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that White House counterterrorism advisor John Brennan was briefed in October on an assassination attempt by Al Qaeda that may have used the same underwear bombing technique used on Christmas Day.

Question: Were you made aware of this briefing?

Response: Yes.

Question: What actions did DHS take in light of this new potential threat?

Response: DHS acts quickly in response to the identification of new and emerging threats, coordinating with the Intelligence Community, and across the DHS components, on products designed to inform and educate our state, local, and private sector partners. DHS continues to analyze this and other terrorist tactics, techniques, and procedures, and shares information via briefings, teleconferences, and the generation of products at the classified and unclassified levels.

In response to the attempted assassination briefed to John Brennan in October, DHS drafted a classified assessment for situational awareness, and an unclassified note that described the incident and subsequent extremist chatter encouraging the use of the device which the extremists lauded as an internally packed device. In response to the extremist chatter and initial press reporting, the Department undertook studies to determine the attenuation effects of the human body on an explosive detonation, and to determine the potential for TSA deployed technologies to detect such a device.

DHS has established research and development programs to address emerging threats and continues to invest in the development of advanced screening technologies. DHS has also 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 Christmas Day bombing attempt. While DHS has always worked in close collaboration with the DOE National Laboratories, the Department has 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.

Question#:	21
Topic:	IG
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: Last year, the DHS Inspector General issued a report and indicated that TSA's limited use of the No Fly and Selectee lists is appropriate in identifying individuals who pose threats to aviation security. Do you agree with the IG's assessment?

Response: The Transportation Security Administration (TSA) provided input to the Department of Homeland Security Office of Inspector General's assessment and TSA agreed that the use of the No-Fly and Selectee lists was appropriate in identifying individuals who posed threats to aviation security under normal circumstances.

DHS is collaborating with our interagency partners to assess corrective actions to protocols and procedures for watchlisting, as directed by the President, to ensure that gaps identified from this incident are addressed.

Question#:	22
Topic:	DOS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: In November, the State Department provided intel to the National Counterterrorism Center (NCTC) about information provided by the terrorist's father who expressed concerns with son's possible "extremist views". This information, however, did not state that Abdulmuttalab had a U.S. visa.

Do you feel that the State Department should have provided this information?

Response: We are confident all members of the Intelligence Community will build upon the lessons learned from the failed Abdulmutallab attack. Recent events highlight the need to regularly assess all aspects of the intelligence—planning, collection, processing, analysis, and dissemination—to fix process and procedures that fail and to bolster process and procedures that work.

Question: Do you believe that the State Department is the right entity to be issuing visas given the security issues?

Response: DHS notes the Department of State has served as the visa issuing authority for the U.S. Government with distinction. They have the infrastructure, resources, processes, and procedures to continue to do so.

Question#:	23
Topic:	VSP - 3
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: The DHS Visa Security Program sends agents to posts overseas to review visa applications. I understand that in order to have the units deployed overseas, you must receive approval from the Department of State.

Has the Department of State ever turned any of your requests down?

If so, which countries have you been turned down for and what was their reasoning?

Response: At posts where ICE Visa Security Program (VSP) operations have been established, Department of State (DOS) and DHS personnel have established strong and productive partnerships that enhance the security of the visa process. In 2008, ICE VSP and DOS collaborated on VSP's site selection methodology and presented the joint findings to the Homeland Security Council. Additionally, DOS and ICE VSP released a 2008 cable to all posts highlighting the joint accomplishments of DOS and ICE VSP efforts overseas.

While ICE VSP's cooperation with DOS has been largely successful, ICE VSP has occasionally faced resistance from individual Chiefs or Deputy Chiefs of Mission towards the establishment of new Visa Security Units in certain locations. ICE VSP continues to coordinate site selections and visits to posts under consideration for ICE VSP deployment to explain the program's value.

Question#:	24
Topic:	AIT
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: I know that the Department is looking to acquire Advanced Imaging Technologies. What is the Department doing to address the low-tech methods possibly being used by terrorists (i.e. placing explosives within their own body cavity)?

Response: The Transportation Security Administration (TSA) mitigates this threat through the expanded use of explosives trace detectors, allowing TSA to detect minute quantities of explosive trace particles present on the bodies of individuals who have handled or carry explosive materials. TSA works closely with the Department of Homeland Security's Science and Technology Directorate, as well as the National Laboratories under the Department of Energy, to develop new detection technologies.

Statement of Janet A. Napolitano
Secretary

U.S. Department of Homeland Security

before

United States Senate
Committee on Commerce, Science and Transportation

on

The State of Aviation Security – Is Our Current System Capable of Meeting the Threat?

Wednesday, January 20, 2010

106 Dirksen Senate Office Building
Washington DC

Chairman Rockefeller, Senator Hutchison, and members of the Committee: Thank you for this opportunity to testify on the attempted terrorist attack on Northwest Flight 253.

The attempted attack on December 25 was a powerful illustration that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. This Administration is determined to thwart those plans and disrupt, dismantle and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just DHS, but many other federal agencies and the international community as well.

As our part in this effort, DHS is a consumer of the U.S. Government's consolidated terrorist watchlist, which we use to help keep potential terrorists off flights within, over or bound for the United States and to identify travelers that require additional screening. We work with foreign governments, Interpol, and air carriers to strengthen global air travel security by advising them on security measures and on which passengers may prove a threat. We also work with air carriers and airport authorities to perform physical screening at TSA checkpoints and to provide security measures in flight.

Immediately following the December 25 attack, DHS took swift action at airports across the country and around the world. These steps included enhancing screening for individuals flying to the United States; increasing the presence of law enforcement and explosives detection canine teams at air ports, and of air marshals in flight; and directing the FAA to notify the 128 flights already inbound from Europe about the situation. Nonetheless, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with the explosive

PETN on his person. As President Obama has made clear, this Administration is determined to find and fix the vulnerabilities in our systems that allowed this breach to occur.

Agencies across the federal government have worked quickly to address what went wrong in the Abdulmutallab case. The effort to solve these problems is well underway, with cooperation among DHS, the Department of State, the Department of Justice, the Intelligence Community, and our international allies, among others. As a consumer of terrorist watchlist information, the Department of Homeland Security welcomes the opportunity to contribute to the dialogue on improving the federal government's ability to connect and assimilate intelligence. We are also focused on improving aviation screening and expanding our international partnerships to guard against a similar type of attack occurring again. To those ends, today I want to describe the role that DHS currently performs in aviation security, how DHS responded in the immediate aftermath of the attempted Christmas Day attack, and how we are moving forward to further bolster aviation security.

DHS' Role in Multiple Layers of Defense

Since 9/11, the U.S. government has employed multiple layers of defense across several departments to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities, while other countries and the private sector – especially the air carriers themselves – also have important roles to play.

DHS oversees several programs to prevent individuals with terrorist ties from boarding flights that are headed to, within, or traveling over the United States or, in appropriate cases, to identify them for additional screening. Specifically, DHS uses information held in the Terrorist Screening Database (TSDB), a resource managed by the Terrorist Screening Center (TSC), as

well as other information provided through the Intelligence Community to screen individuals; operates the travel authorization program for people who are traveling to the United States under the Visa Waiver Program (VWP)[1]; and works with foreign governments, international and regional organizations, and airlines to design and implement improved security standards worldwide. This includes routine checks against Interpol databases on wanted persons and lost or stolen passports on all international travelers arriving in the United States. The Department also performs checkpoint screenings at airports in the United States.

To provide a sense of the scale of our operations, every day, U.S. Customs and Border Protection (CBP) processes 1.2 million travelers seeking to enter the United States by land, air or sea; the Transportation Security Administration (TSA) screens 1.8 million travelers at domestic airports; and DHS receives advanced passenger information from carriers operating in 245 international airports that are the last point of departure for flights to the United States, accounting for about 1,600 to 1,800 flights per day. Ensuring that DHS employees and all relevant federal officials are armed with intelligence and information is critical to the success of these efforts.

Safeguards for Visas and Travel

One of the first layers of defense in securing air travel consists of safeguards to prevent dangerous people from obtaining visas, travel authorizations and boarding passes. To apply for entry to the United States prior to boarding flights bound for the U.S. or arriving at a U.S. port of

[1] The 35 countries in the Visa Waiver Program are: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, and the United Kingdom (for the U.K., only citizens with an unrestricted right of permanent abode in the U.K. are eligible for VWP travel authorizations).

entry, most foreign nationals need visas – issued by a U.S. embassy or consulate – or, if traveling under a Visa Waiver Program country, travel authorizations issued through the Electronic System for Travel Authorization (ESTA) .[2]

Issuing visas is the responsibility of the Department of State. At embassies and consulates where it is operational, the Visa Security Program positions personnel of U.S. Immigration and Customs Enforcement (ICE) to assist State Department personnel in identifying visa applicants who may present a security threat. For individuals traveling under the VWP, DHS operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. These systems examine an individual's information to assess whether he or she could pose a risk to the United States or its citizens, including possible links to terrorism. Without presenting a valid authorization to travel to the United States at the airport of departure, a foreign national is not able to board a U.S.-bound flight.

The Department also works with other federal agencies and our foreign partners to try to prevent possible terrorists from obtaining boarding passes. These include the application of the No-Fly List and the implementation of Secure Flight program, which I explain below.

Pre-departure screening

As another layer of defense, DHS conducts pre-departure passenger screening in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. DHS uses TSDB data, managed by the Terrorist Screening Center that is administered by the FBI, to determine who may board, who requires

[2] Exceptions would be citizens of countries under other visa waiver authority such as the Western Hemisphere Travel Initiative or the separate visa waiver program for Guam and the Commonwealth of the Northern Mariana Islands, or those granted individual waivers of the visa requirement under the immigration laws.

further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

Specifically, to help make these determinations, DHS uses the No-Fly List and the Selectee List, two important subsets within the TSDB. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, over, or within the United States. Individuals on the Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

Through the Secure Flight Program, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List, and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, DHS began to transfer this responsibility to TSA in 2009, and the transition is targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination.

As an additional layer of security, DHS also uses the Passenger Name Record (PNR), the Advanced Passenger Information System (APIS), and the Immigration Advisory Program (IAP) to assess a passenger's level of risk and, when necessary, flag them for further inspection. PNR data, obtained from the airline reservations systems, contains various elements, which may include optional information on itinerary, co-travelers, changes to the reservation, and payment information. PNR data is evaluated against "targeting rules" that are based on law enforcement data, intelligence and past case experience. APIS data, which carriers are required to provide to

DHS at least 30 minutes before a flight, contains important identifying information that may not be included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. DHS screens APIS information on international flights to or from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations. APIS is also connected to Interpol's lost and stolen passport database for routine queries on all inbound international travelers.

Another layer in the screening process is the Immigration Advisory Program (IAP). The CBP officers stationed overseas under the IAP program at nine airports in seven countries receive referrals from CBP screening against the TSDB, of which the No Fly list is a subset. IAP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

Checkpoint screenings and in-flight security

The third layer of defense for air travel in which DHS plays a role is the screening of passengers and their baggage. TSA screens passengers and baggage at airports in the United States, but not in other countries. When a traveler at a foreign airport is physically screened, that screening is conducted by the foreign government, air carriers, or the respective airport authority.

Domestically, TSA employs a layered approach to security, which includes measures both seen and unseen by travelers. The 48,000 Transportation Security Officers at hundreds of airports across the country screen passengers and their baggage using advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines,

vapor trace machines that detect liquid explosives, Advanced Imaging Technology, full-body pat-downs, explosives detection systems, Bomb Appraisal Officers, and Behavior Detection Officers – both at the checkpoint and throughout the airport. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security throughout the airport perimeter and in limited access areas of airports. The $1 billion in Recovery Act funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

In an effort to enhance international screening standards, TSA conducts security assessments in accordance with security standards established by the International Civil Aviation Organization (ICAO) at more than 300 foreign airports, which include foreign airports from which flights operate directly to the United States and all airports from which U.S. air carriers operate. If an airport does not meet these standards, TSA works with the host government to rectify the deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. In long-term circumstances of non-compliance with international standards, TSA may recommend suspension of flight service from these airports to the United States. In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level. If an airport is located within one of the 35 VWP countries, DHS conducts additional audits and inspections as part of the statutorily mandated VWP designation and review process.

In terms of in-flight security, Federal Air Marshals (FAM) are deployed on high-risk domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more volunteer pilots serve as armed, deputized Federal Flight Deck Officers. Additionally, armed law enforcement officers from federal, state, local, and tribal law enforcement agencies that have a need to fly armed provide a force multiplier on many flights.

DHS Response to the Christmas Day Attack

The facts of the Christmas Day attempted bombing are well established and were relayed in the report on the incident that the President released on January 7, 2010. On December 16, 2009, Umar Farouk Abdulmutallab, a Nigerian national, purchased a round-trip ticket from Lagos, Nigeria to Detroit. Abdulmutallab went through physical security screening conducted by foreign airport personnel at Murtala Muhammed International Airport in Lagos on December 24 prior to boarding a flight to Amsterdam Airport Schiphol. This physical screening included an x-ray of his carry-on luggage and his passing through a walk-through metal detector. Abdulmutallab went through additional physical screening, conducted by Dutch authorities, when transiting through Amsterdam to Northwest Flight 253 to Detroit, and presented a valid U.S. visa. Abdulmutallab was not on the No Fly or Selectee Lists. Accordingly, the carrier was not alerted to prevent him from boarding the flight or additional physical screening, nor did the IAP officer advise Dutch authorities of any concerns. As with all passengers traveling on that flight, and similar to all other international flights arriving in the United States, CBP evaluated Abdulmutallab's information while the flight was en route to conduct a preliminary assessment of his admissibility and to determine whether there were requirements for additional inspection.

During this assessment, CBP noted that there was a record that had been received from the Department of State, which indicated possible extremist ties. It did not indicate that he had been found to be a threat, or that his visa had been revoked. CBP officers in Detroit were prepared to meet Abdulmutallab upon his arrival for further interview and inspection. The attack on board the flight failed in no small part due to the brave actions of the crew and passengers aboard the plane.

Immediate DHS response

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. TSA directed the Federal Aviation Administration to apprise 128 U.S.-bound international flights from Europe of the attempted attack and to ask them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosive detection canine teams, state and local law enforcement, expanded presence of Behavior Detection Officers, and enhanced screening. That evening, DHS issued a security directive for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

From the first hours following the attempted attack, I worked closely with the President, Assistant to the President for Homeland Security and Counterterrorism John Brennan, senior Department leadership, and agencies across the federal government. I communicated with international partners, members of Congress, state and local leadership and the aviation industry and met with national security experts on counterterrorism and aviation security. The results of

these communications culminated in two reports to the President: one on New Year's Eve and the second on January 2, 2010.

One of our most important conclusions was that it is now clearer than ever that air travel security is an international responsibility. Indeed, passengers from 17 countries were aboard Flight 253. Accordingly, DHS has embarked upon an aggressive international program designed to raise international standards for airports and air safety. On January 3, 2010, I dispatched Deputy Secretary Jane Holl Lute and Assistant Secretary for Policy David Heyman to Africa, Asia, Europe, the Middle East, Australia, and South America to meet with international leadership on aviation security. In these meetings, they reviewed security procedures and technology being used to screen passengers on U.S.-bound flights and worked on ways to bolster our collective tactics for defeating terrorists. This afternoon, I am traveling to Spain to meet with my European Union counterparts in the first of a series of global meetings intended to bring about broad consensus on new, stronger, and more consistent international aviation security standards and procedures.

In addition to these efforts, the Department has been in close contact with Congress, our international partners, the aviation industry and state and local officials across the country since the afternoon of the attempted attack. On December 25, the Department issued a joint bulletin with the FBI to state and local law enforcement throughout the nation; conducted calls with major airlines and the Air Transport Association; distributed the FBI-DHS joint bulletin to all Homeland Security Advisors, regional fusion center directors and Major City Homeland Security Points of Contact in the country; and notified foreign air carriers with flights to and from the United States of the additional security requirements. DHS has maintained close contact with all of these partners since the attempted attack, and will continue to do so.

On January 3, TSA issued a new Security Directive, effective on January 4, which includes long-term, sustainable security measures developed in consultation with law enforcement officials and our domestic and international partners. Because effective aviation security must begin beyond our borders, this Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism[3] or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners.

Steps Forward to Improve Aviation Security

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. On January 7, I joined Assistant to the President for Counterterrorism and Homeland Security John Brennan to announce five recommendations DHS made to the President as a result of the security reviews ordered by President Obama. At the President's direction, DHS will pursue these five objectives to enhance the protection of air travel from acts of terrorism.

First, DHS will work with our interagency partners to re-evaluate and modify the criteria and process used to create terrorist watchlist, including adjusting the process by which names are added to the No-Fly and Selectee Lists. The Department's ability to prevent terrorists from boarding flights to the United States depends upon these lists and the criteria used to create them.

[3] The State Department currently lists Cuba, Iran, Sudan, and Syria as state sponsors of terrorism.

As an entity that is primarily a consumer of this intelligence and the operator of programs that rely on these lists, the Department will work closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watchlist system.

Second, DHS will establish a partnership on aviation security with the Department of Energy and its National Laboratories in order to use their expertise to bolster our security. This new partnership will work to develop new and more effective technologies that deter and disrupt known threats, as well as anticipate and protect against new ways that terrorists could seek to board an aircraft with dangerous materials.

Third, DHS will accelerate deployment of Advanced Imaging Technology to provide capabilities to identify materials such as those used in the attempted December 25 attack, and we will encourage foreign aviation security authorities to do the same. TSA currently has 40 machines deployed at nineteen airports throughout the United States, and plans to deploy at least 450 additional units in 2010. DHS will also seek to increase our assets in the area of explosives-trained canines, explosives detection equipment, and other security personnel.

Fourth, DHS will strengthen the presence and capacity of aviation law enforcement. As an interim measure, we will deploy law enforcement officers from across DHS to serve as Federal Air Marshals to increase security aboard U.S.-flag carriers' international flights. At the same time, we will maintain the current tempo of operations to support high-risk domestic flights, as we look to longer-term solutions to enhance the training and workforce of the Federal Air Marshal Service.

Fifth, as mentioned earlier, DHS will work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in

foreign airports and the commitments of our foreign partners to enhance security – not just for Americans, but also for their nationals traveling to this country.

In all of these action areas to bolster aviation security, we are moving forward with a dedication to safeguard the privacy and rights of travelers.

Conclusion

The attempted attack on Christmas Day serves as a stark reminder that terrorists motivated by violent extremist beliefs are determined to attack the United States. President Obama has made clear that we will be unrelenting in using every element of our national power in our efforts around the world to disrupt, dismantle, and defeat al-Qaeda and other violent extremists.

While we address the circumstances behind this specific incident, we must also recognize the evolving threats posed by terrorists, and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities in all sectors. President Obama has clearly communicated the urgency of this task, and the American people rightfully expect swift action. DHS and our federal partners are moving quickly to provide just that.

I wish I could close by giving you a 100 percent guarantee that no terrorist, ever, will try to take down a plane or attack us in some other fashion. I cannot give you such a guarantee; that is not the nature of the world we live in, nor of the threats that we face. What I can give you, however, is the 100 percent commitment of myself, DHS leadership, and the entire DHS enterprise to do everything we can to minimize the risk of terrorist attacks.

Chairman Rockefeller, Senator Hutchison and members of the Committee: Thank you for this opportunity to testify. I can now answer your questions.

CQ CONGRESSIONAL TRANSCRIPTS
Congressional Hearings
Jan. 20, 2010

Senate Commerce, Science and Transportation Committee Holds Hearing on the Northwest Flight 253 Bombing Attempt

---

ROCKEFELLER:
This hearing will come to order. I want to thank our witnesses for coming today. There are other hearings on this matter. And I'm really glad of it.

Some of you are going to have to do a lot of traveling to a lot of committees. But I'm really glad of that too. People need to hear from you. And, in fact, you look a long way off.

Secretary Napolitano, I welcome you back to the committee. I think that you have one of the hardest jobs in America, maybe second or third hardest. The president wins on that. You and Mike can fight out who's second and who's third.

I think you are doing a terrific job, that I think you're -- you personally are underappreciated. I think your department is underfunded. And I think this incident may help us solve that underfunding problem. Your problem doesn't have to be solved, as I told you before, as the hearing just a few moments ago started. As far as I'm concerned, you wear -- you wear four stars on each shoulder.

Director Leiter, this is the first time circumstances have combined to have you be testifying before the Commerce Committee. You're a very lucky man. As chairman of the Intelligence Committee, I have the pleasure of working with you on -- on matters relating to intelligence reform. And, as you know, I expressed my feelings then how impressed I was at the job that you were doing then and you are doing now.

We've had a very serious problem. There's the question of accountability. That's a hard thing to solve. It's also sometimes not a wise thing to solve in the first few minutes in public. Sometimes it's good to know what you're talking about before you get into that.

And I know my colleagues will recognize your tremendous, profound expertise in understanding what it takes to meet our responsibilities. So, I am very grateful that you are here for our committee, and that you serve as you do.

I know that you've been working around the clock. I've been a governor. But I -- I don't think even that comes even close to the pressure that both of you, a Cabinet secretary, NCTC, et cetera, that -- what -- what that amounts to in the way of -- of pressure, sleeplessness, trying to find out how we can do better. That's the purpose of this hearing.

We're going to stay on this subject most of this year. We're going to get it right. It is a very serious thing that happened. The fact that nobody was killed and nobody was particularly injured, except for perhaps the perpetrator, and one or two others in a minor way, belies the fact that, had things gone according to the way they were meant to, 252 people who have died 20 minutes outside of Detroit.

I tend to think of it in terms of what I just said, as opposed to the fact that nothing happened. And I think that's the way you look at it too.

Lee Hamilton and Tom Kean, you are welcome anywhere at any time. And you're an -- you're an asset to the nation, both of you. Maybe you're just one person. I don't know.

But you have brought more wisdom and challenged us in more ways. I asked each of you to be tough on us in your questioning, answer -- answer to questions, or matters that you want to raise, because this is the time for us to hear clearly from those who have watched wisely from the outside, but really on the inside. Thank you again for coming.

OK, so the Christmas terror attack told us that we need to further harden our defenses and evaluate if we're doing everything we can to meet an evolving Al Qaida terrorist threat or perhaps non-Al Qaida terrorist threats, domestic problems, discontent, all of the instability that rules throughout our -- our -- our country, fear throughout the world, the fear, the hopelessness.

All of this combines to produce exactly the wrong kind of people doing exactly the wrong kinds of things. But they think it's for the right reason. And if they seek martyrdom, it's pretty hard to argue and win them over.

The threat to America is real and we have to get it absolutely right. And our problem, of course, is that we have to get it right 100 percent of the time. Their problem is they have to get it right once. And -- and it's not fair. But that's the world we live in. And that's what we need to deal with on this committee as well as other committees.

A man with a bomb was able to board a plane headed for America. So, it's obvious and clear our system failed; cannot be disputed. I know that every day countless unsung American heroes are working in your agencies, working 17-hour days seven days a week, and going through every scrap of information.

People have no idea. Actually, it's classified. People have no idea of the amount of information that comes in each day to the various intelligence agencies. You -- you get the brunt of it, Director Leiter.

So, the question is how do you pick one thing from another? And the answer is that it seems to be impossible. And that can't be the answer. The answer is we've got to get it right.

How come this guy got a visa? How did he get a visa? How come it was his -- what he said, what his father told to the American embassy was not considered a clarion call? Potential answer

AR 000989

-- all those things come in all the time. Other potential answer is we should have harkened to that, and responded to that, and made sure that he never got on an airplane.

So, I tremendously value -- I'm still on the Intelligence Committee, and I still do -- that people that work so hard to try to get it right, seven men and women of the CIA recently killed in Afghanistan. They don't make it home.

So while we have a responsibility to be frank about where we've fallen short, we must also honor their service. I want that to be very, very clear. We can do that by building on the progress that we've made since the 9/11 attacks, with an eye towards making smart and specific improvements that keep us safe; easy to say, hard to do.

Nine years ago, our intelligence agencies did not even share information, largely because they could not, by law. First bill that we passed: Yes, CIA and FBI, you can talk to each other. Stunning, less than a decade ago. And their information systems weren't interoperable. Part of that's true still today.

And because they would not, agencies too often preferred to stovepipe information rather than share it. That was the past. How much is that of the present, we will talk.

Since then, as Mr. Leiter will testify, we have made enormous strides. Today, our systems and practices are far superior than those that were -- allowed 19 men to execute the global plan to commit the horrific acts of 9/11. But we're not failsafe. We haven't gotten there yet.

And yet, just weeks ago our systems still allowed a terrorist to board Flight 5 -- 253 with sophisticated explosives. This was a grave and multi-layered failure. The intelligence community did not piece together clues about this man's connections to terrorism, clues that were available, including from his father.

It's my -- it is my general impression it's -- it doesn't fall within the habit of Islamic behavior for a father to go in and, in a sense, give up his son, or even more for us, then, to ignore it; that being such a unique and -- and stunning thing for a father to do.

The State Department and the Department of Homeland Security allowed this man to board the airplane with a valid U.S. visa. The Brits hadn't given him one a couple years before. We gave him one that lasts for two years. And the international airport screening that we depend on did not detect that this man was carrying a potentially devastating explosive device.

One of my questions, Madam Secretary, is going to be about the meeting that you take off for tomorrow, the 21st and the 22nd with Europeans. How -- how do we, in this tiny, tiny little world, how can somebody just pass through Amsterdam without any American eyes alighting upon him or her or what their situation might be?

So, we have a responsibility to be brutally honest about where we have fallen short. We have to do better. And the basic fact that will drive much of this committee's work in the year ahead is trying to make it all better. I promise you that. I promise my colleagues that.

AR 000990

We have to do better at protecting our families, safeguarding our communities, securing our nation. Nobody was injured. Nobody was killed -- not in my head. Malfunction, 252 would have died.

So, this is at the top of our agenda for this year: bringing the attention, and the resources, and the leadership needed to provide an improvement in our -- in our citizens' safety and security. This committee intends to continue asking the tough questions, to shape the policies that guide transportation security in all of its modes. And by that, I mean our port security, our chemical security, our cybersecurity. And the list goes on.

We have oversight of that here. Have we exercised it sufficiently? Perhaps not.

Today's hearing on aviation security represents an opportunity to bring to the table key issues that demand all of our attention. And I want to invite my colleagues to bring their new ideas, as we work together to develop concrete solutions that advance our security efforts and make us safer.

Let me end with five suggestions. Some key solutions I believe we can and must seriously consider: requiring US-bound aircraft and international airports to meet more rigorous security requirements, and not letting our cumbersome international negotiating process slow us down. Is that possible? According to international protocol, it is not. It has to be possible. We cannot talk this thing to death. We are a tiny, little globe, interlocked.

Two, engaging a major new effort to develop and deploy advanced imaging technologies, which means more money, more accuracy, and getting serious about stopping any programs that do not work. So then, we have the question of civil liberties versus national security -- for -- for -- forever a problem, forever rightly a problem. But we cannot tread lightly on what we do on national security.

Three, improving and, in some cases, mandating better information sharing among TSA, intelligence agencies and even commercial airlines. I invited an airline to be at this hearing today. They declined. They declined. I was not happy.

I don't know what that tells us. But it tells us that we're all in this together. And everybody has to do their part. And nobody has a safe haven. We need to do more to establish the partnership between government and the private sector when it comes to security.

Four, making the watchlist more accurate on the one hand, and more dynamic on the other, expanding the universe of people who receive secondary screening. I'm a believer in that. Re-evaluating our screening criteria, and then doing something called educating the public in advance about what may become more stringent scrutiny at airports.

Our public understands this very well. They've been through the beginning of TSA. They're been through shoe bomber and taking off the shoes. Have they liked it? No. Have they complied

with it? Yes, because they understand what the stakes are. So, we need partnership with the flying public also.

And finally, number five, requiring coordination between the valuable resources we have at our embassies, especially our regional security offices and the TSA, to identify threats emanating from overseas airports. Believe it or not, this is not always happening today. And it did not happen in this case.

This is not an exhaustive list. But it's something to start with. All of this, obviously, is going to require raising new revenues. That's always a problem in the United States Senate. But doing nothing is not an option.

I don't know how you improve security. I don't know how you put in better machinery. I don't know how you get to the WBIs -- not just 40, but the 900 you want by 2014 -- without more money, more training for our -- our security people.

So, the need is clear and transparent. The way is hard and difficult. But it is our obligation. I look forward to our witnesses' testimony as we work together and make our transportation system as safe as possible.

Just, Madam Vice Chair, if I can just say that I'm sure that our colleagues all know that Erroll Struthers (sic) withdrew his name for head of TSA today. And our national security system has lost a skilled law enforcement officer who had needed expertise and leadership qualities because of, I would call it political gains. But I'm not going to -- I'll just scratch that from the record.

Anyway, it's a real shame. It's a real shame. So, now we've got to go out and find another one, and vet them in the -- in the -- in the way that Americans can, which takes a long time. We don't have a long time. I'm confident that the president will quickly -- very quickly nominate a new candidate to run TSA. And I'm committed to seeing that that person gets through the process.

I thank you. And I thank my colleagues for their patience. And I turn now to Senator Hutchison for her opening statement.

HUTCHISON:
Thank you, Mr. Chairman.

Mr. Chairman, I would just say that I believe there were legitimate concerns about Mr. Southers. And I think those concerns deserve to be investigated. So, I hope that we can move forward with a new nominee, because we certainly need an experienced person in that position. But it also needs to be a person who would assure the respect of the people in the agency, to have the authority to assure that the agency is doing its job.

I do think that every one of you have done a lot to try to put America in a place where we can be more secure. I think the members of the 9/11 Commission certainly have given many volunteer hours to give advice early on after 9/11. And I think the members of our administration

AR 000992

as well are working very hard. And no one disputes that you are doing everything that -- that you know to do.

But I think now, we need to look at what has happened and learn from that. And we need to go forward in a constructive way.

The plot that unfolded on Christmas day just shows that the defense of our homeland from terrorists is dependent on information collection and sharing, intelligence analysis and the vigilance of our security personnel; and that none of these can be effective without the other.

And if there's anything that we have learned from my experience that happened in my home state of Fort Hood, and then this one on its heels, it's that we're not sharing enough. And what the chairman said about, after 9/11, saying, oh yes, our intelligence agencies can actually talk to each other, that is a very small first step. And we need to perfect that and quickly.

The president's own initial review has concluded that, if our intelligence analysts had pieced together the information at their disposal about the attempted bomber, there would have been sufficient grounds to place him on the terrorist watchlist, perhaps averting what happened.

Going forward, I think that we need to look at several things. We need to look at expanding the number of known or suspected terrorists and their associates who are placed on screening lists, even though, in the short term, this may result in more mistaken matches.

Number two, I think we need to expedite the adoption of programs that will aid the process, such as the complete implementation of the Secure Flight program, which will take the ultimate screening responsibility away from air carriers and place it completely within the security agency. It has more access to intelligence than a private airline could have, making our screening efforts more effective. Progress on that program has been positive of late. But we need to move faster, if we can.

And number three, I think it is very important that we better synthesize intelligence data, especially in relation to associates of known terrorists or those who may be connected to potential terrorist threats.

Since 9/11, we have been in a new era of conflict. However, recently, we have seen a series of disturbing changes in our fundamental mission of how we deal with terrorists and terrorist threats, most starkly in the decision to bring the perpetrators of the 9/11 attacks to New York for civil trials in our courts and the closing of Guantanamo Bay.

Mr. Chairman, this country and its leaders need to remember that we are at war with terrorists and extremists who mean us harm. This is not a war of traditional means and should not be dealt with through the civil process. We should have an approach that is committed to more vigilance and flexibility and enables our intelligence and security personnel to utilize all the tools at their disposal for the purposes of eliminating the threat to this nation.

So, this is not a blame game. But it is, I hope, an opportunity for us to talk to you, or you to talk to us, and for us to come to the conclusion that we must be more vigilant in pursuing the people who wish to do us harm. And even in today's paper, they are talking about recruiting more Americans for these terrorist activities in Yemen. And they are focusing on blond hair and blue eyes, so that it is not someone who would raise flags.

So, we've got a problem that we need to go through together. And I hope that we can learn from our hearing, from the hearing you had this morning, and that we can have the confidence that we're all going on the same track.

Thank you, Mr. Chairman.

ROCKEFELLER:
Thank you, Madam Vice Chairman.

And I just say to our members that I want the following senators who I've spoken to to make statements, each five minutes or less. And I hope that others will understand. These are the people who are chairman and ranking on -- on the -- the relevant subcommittees.

So, I want to start with Senator Dorgan. And then I want Senator DeMint. Then I want Senator Lautenberg. And then I want Senator Thune to make statements.

So, we'll start with Senator Dorgan. And I hope others will understand.

DORGAN:
Mr. Chairman, thank you. I'll try to be very brief. You know, this is one of those very important issues in which failure is not an option. And we had, on Christmas day, something that was near tragic for a lot of passengers on the -- that airline. And fortunately, the terrorist attack that day failed to achieve the objective.

But what I want to understand is a couple things. Number one, I think there was a screening failure. The question is what do we do to -- what do we need to do to better screen passengers, balancing it with privacy and so on? And the second is the intelligence failures. What has caused the intelligence failures, especially inasmuch as we put together a DNI to end stove-piping and so on. And clearly that didn't happen here.

Harry Truman famously had the sign, the buck stops here. The question with all of this for me is where does the buck stop with respect to these failures? And I want to just hypothecate.

If we were thinking forward here, and it's today, and we have some information about a couple of weeks from now. And it's a father of a young Nigerian that comes through our intelligence community overseas and says, look, my son is engaged with some bad people. I'm worried about what he might or might not do.

AR 000994

He's then put on a watchlist, but not on a no-fly list. Nobody checks to see that he has an open visa and cancels the visa. So, here's someone who's father thinks apparently he's a potential terrorist or something of that nature. And he's put on a watchlist, but again, not on a no-fly list and continues an open visa.

And there are three intercepts in the next few weeks or so. Two of the -- one of them is that a man with the first two names of this person has volunteered for some coming operation. That was an intelligence intercept I understand. Another intercept would be a Nigerian man being groomed for an operation. And the first intercept actually used the first two names of this young man.

The third intercept in December mentions some type of operation on December 25th. And then a young man shows up and -- and pays cash for an airline ticket to go from Ghana to, as I understand it, to Amsterdam to Detroit, and then shows up and boards the plane with no luggage.

So, this isn't looking for a needle in a haystack. This is looking for a big old needle right in the middle of our hand. And the question is would we see it next time, because we didn't see it this time. And that is, in my judgment, an unbelievable failure.

So, the question is where does the buck stop? Who's accountable for that, because that -- it is one thing to say the system failed. But we're not talking just about systems. We're talking about people who manage and operate the systems and who have to be accountable for making sure the systems work, because failure is not an option.

And we have -- we have constantly, as all of us know, dealt with the last issue: the last issue of the box cutter, the last issue of the shoe bomb, the last issue of liquid containers, the last issue of sewing plastic explosives in the underwear. It is constantly the last issue.

But much more important than that in this case is the question of how did we miss so many circumstances where you actually have a name and a father describing a son, and a circumstance with three intercepts that talk about a day and the name, and no-fly lists that aren't -- that aren't coordinated with -- with watchlists, and visa -- open visas that aren't coordinated with the watchlists.

You know, something just doesn't add up at all. And I -- my hope is that, through this hearing, we can understand what doesn't add up? Why doesn't it add up? And where does the buck stop? That's what's important.

So, two issues: how do we better screen? What kind of screening is necessary? What does it cost? How intrusive is it? All of those issues are things we have to talk about. And then second, what about this unbelievable, to me, issue of intelligence?

I say all of that without denigrating you all. This is a tough job. But still, I -- I think you and us need to understand what failed, and who failed and who's accountable.

ROCKEFELLER:
Thank you, Senator Dorgan.

Senator DeMint.

DEMINT:
Thank you, Mr. Chairman.

And I want to thank Chairman Dorgan for his work in airline safety. You've been a real proponent for many months, long before Christmas, to improve airline safety. And your expertise will -- will be missed.

I want to make a couple of points. I appreciate all the witnesses being here today. And first, I'd like to talk about TSA.

Anytime we implement any change in homeland security, TSA, anything related to that, the first question need to be how will it improve security? And I've been very concerned, as the secretary knows, that the administration has a priority of subjecting our TSA security officers to a collective bargaining regime.

No one is yet to give any reason, any security reason, why collective bargaining should be adopted. Employees are not mistreated. We will not add any flexibility or any benefit. It's clearly a political agenda.

And frankly, for me, even though I appreciate what the president has lately been saying and what has come out of homeland security -- those things have been encouraging -- it's hard for me to take commitments to security seriously as long as forcing TSA into collective bargaining is a priority, because it makes no sense.

Last month, I asked the secretary how collective bargaining at TSA will improve security. Her answer was that the two weren't mutually exclusive. Her answer was not that it would improve security. And I think anytime when the secretary of homeland security can't tell us how a change in homeland security is going to improve security, it should stop us all in our tracks.

Our security agents now are free to join a union. And the union can advocate on their behalf. But we all know that collective bargaining is very different. It creates a third party structure that our security system has to answer to. Collective bargaining will impose a 19th century industrial personnel management model to a 21st century information-age threat.

The threat we see in the aviation sector is a creative and nimble threat. And these are words the president has used. And our response needs to be nimble and creative. We need to continually improve what we do at TSA.

The men and women who protect the aviation sector need to be able to respond quickly to change -- to change in the counterterrorism tactics, so that we can thwart the tactics of our

AR 000996

adversaries and protect passengers. And they need to be able to do it without having to get sign-off from the labor unions. The Secret Service, Coast Guard, the military, the FBI, they realized this long ago. And they prohibit collective bargaining.

And let's not be fooled by some of the arguments that we hear that collective bargaining works in other areas of homeland security. The most immediate past director of customs and border protection is on record saying that collective bargaining made it much more difficult for him to do his job. He had to negotiate staffing policy with labor unions and had to discuss security policy with the unions that was better kept internal.

Quite simply, our security policy needs to be focused on improving security. It can't be subjected to a union middleman. The only concern career professionals at TSA should have when responding to a terrorist threat is what best meets the threat, not what best meets the needs of a labor union.

Let me shift the focus just a minute to talk about a couple of other things. One is behavioral targeting. In addition to not going backwards with this idea of collective bargaining for TSA, where it's been prohibited, we need a more modern approach to screening. The behavioral screening approach used by the Israelis provides a good model. And it's something that we should take a closer look at.

TSA continues to focus on keeping bad things off of airplanes. The Israelis, for example, focus on keeping bad people off of airplanes. Terrorists will always find a weapon, whether it be in a bottle of alcohol purchased at a duty-free store or two strategically placed laptop batteries. If we focus on things instead of terrorists, we're going to lose this war.

To be clear, I'm referring to assessing an individual's behavior to separate the terrorist from the traveler. Additional random screening will never be as successful as targeting the bad guys. Behavioral profiling is a vital and common-sense tool to increase security that we could use more effectively. And I hope we can talk a little bit about that today.

Just one other point, Mr. Chairman, on -- on visas. The Christmas bomber highlighted the need for across-the-board reform of the viva -- visa process. We need to make it faster and easier to revoke visas. Traveling to the United States is a privilege. It's not a right.

Currently, unless the applicant comes from a country designated as a sponsor of terrorism, the information threshold required for denying a visa may be too high. This issue needs to be addressed quickly, for both immigrant and non-immigrant visas.

America can be a safe and welcoming nation at the same time. We do not have to sacrifice security for expediency.

I am also concerned that, when security advisory opinions have been requested, some types of visas have actually been issued before all of the relevant intelligence agencies have had an opportunity to respond. Security has to be a priority, and policies that discourage information sharing and weaken security must be changed.

If we want to enhance security, we have to collect, analyze and quickly act on that information. The American people deserve to know why this terrorist was not added to the no-fly list, and what we intend to do to keep terrorists, not only from getting visas, but from gaining access to our country altogether.

Thank you, Mr. Chairman.

ROCKEFELLER:
Thank you.

And Senator Lautenberg.

LAUTENBERG:
Thanks, Mr. Chairman. If I might just take a moment to say that we have an outstanding group of witnesses that are at the table. But I am particularly pleased to see former Governor Kean from New Jersey and Lee Hamilton, who co-chaired the 9/11 Commission report, and it was a major piece of work in response to the worst attack ever on our country. We're glad to see -- see them here.

During -- the incident over Detroit wasn't the only urgent wake- up call about a major lapse in our national aviation security network that has been recently revealed. During what was supposedly a period of heightened aviation security, at an airport, Newark Liberty Airport, that lies within the two-mile stretch deemed to be the most at-risk place for terrorism -- that's by the FBI -- a man was able to break through security by walking unchallenged into Terminal C of Newark Airport.

This breach of security was intentional and shockingly easy. The inexcusable breach occurred when a TSA guard turned his back for a moment, and a watching individual took the opportunity to dash under a security tape into the airport, completely unchecked and unscreened. Without a vigilant traveler's alert to the TSA, we would never have known that the breach occurred.

And even after TSA was alerted, it took two hours for them to alert law enforcement people, the police there, to verify the breach on videotape and to take action -- two hours, when a potential terrorist could have been conspiring, with a plan or a weapon, to bring down an airplane; two hours when a potential terrorist could have been bird-dogging for a bigger plot.

And while the motives of the man behind the Newark breach may seem benign, this incident was not just, as it was portrayed, a playful reunion. The result was a major security breach that shut down an entire terminal of a major airport for more than six hours and delaying more than 16,000 people from getting to their families, friends or final destinations. It caused over 100 flight delays and 27 flight cancellations.

AR 000998

And since 2002, DHS has spent $1 billion on technology to screen passengers coming into an airport terminal. But all of that screening technology is useless if someone can just walk in through an exit without being noticed.

This exit at Newark Airport had security cameras operated by TSA. But the -- but the principal camera had been broken for almost a week. TSA knew about the broken camera and failed to report it.

The cameras weren't the only things that broke down. There was a complete communications breakdown between TSA and its partners on the ground, the Port Authority and Continental Airlines. Fortunately, the Continental Airlines camera nearby was effectively recording.

During this time, TSA still failed to notify the Port Authority Police of this breach. And we can be sure that terrorists are -- observe actively the kind -- this kind of a -- a free passage for plans that they may have.

A security breach of this nature is a matter of national security and needs to be treated that way. And that's why I'm taking action today to introduce legislation to close the dangerously -- the dangerous security gaps exposed by the breach at Newark Airport.

My legislation mandates that all airport terminal checkpoints and exits have working security cameras. It will require sufficient personnel at secure area exits. If someone purposely breaches airport security, under my bill, they will face serious consequences, not as is suggested a $500 fine, which is nothing more than a tap on the wrist that makes a joke out of the security structure.

I'm going to be working with DOJ and DHS to make sure the federal government gets involved in enforcing the law and handling major aviation security breaches instead of ceding this responsibility to state or local authorities.

The incidents at Newark and Detroit exposed fundamental weaknesses in our aviation security system. And if we learn from these events and treat them with the seriousness they deserve, I'm confident that we can say to all Americans who want to fly, you're safe as safe can be made.

And with that, I thank the Mr. Chairman.

ROCKEFELLER:
Thank you, Senator Lautenberg.

Senator Thune.

THUNE:
Thank you, Mr. Chairman.

AR 000999

I want to thank you and Senator Hutchison for holding this very important hearing, and also thank our panelists for being here today, and would echo what's been said about Congressman Hamilton and Governor Kean and your good work. And we appreciate the many contributions that you have made in looking carefully at this in great detail, and making recommendations about how to do a better job.

I do have to say that I think the initial reaction to this, that the system worked, could not have been more wrong. And it seems to me, at least, that there were significant breakdowns and failures in the system. And those need to be corrected, or this is going to happen again.

And I -- I guess I -- I think the people on Flight 253 and the crew can be very thankful that the -- the explosive failed to detonate. But that doesn't for a minute suggest that there aren't going to be other efforts made by those who would want to kill Americans to somehow get into our system and have access to Americans and -- and airplanes, and -- and other forms of transportation that -- that they can do to -- to try and -- and -- and kill and disrupt and -- and damage America and our interest.

So, we -- we need to get this fixed. And I think one of the things that I appreciate both Congressman Hamilton and Governor Kean have had to say is that we -- we do have to, I think, recognize that one of the greatest threats that we face in this country when it comes to air travel is public complacency, particularly following the stepped-up security protocols following 9/11. And I -- I appreciate that you recognize that in your testimony.

I think we all have to figure out where the intelligence and other human errors occur that failed to stop Mr. Abdulmutallab from entering the United States. And it's pretty clear that there was failure when it comes to sharing intelligence, a failure when it comes to analyzing intelligence. And I would share the observation of the senator from South Carolina that the focus of this effort really needs to be on terrorists.

And I'm interested in hearing Secretary Napolitano, from you, and from Mr. Leiter about what's being done to adjust the process by which names are added to the -- to the no-fly and selectee lists, and explaining what, if any, technological barriers exist when it comes to subject -- subjecting airline flights to the larger subset of the TIDE database, the -- the 550,000 names; because clearly there's got to be a better job when it comes to screening and -- and identifying people who are already on the list and making sure that they're not getting this kind of access.

And the other issue I'd be interested in hearing about is how often, how many times (inaudible) there have been suspended (inaudible) United States due to insufficient security standards that are employed by foreign countries. And I know we have TSA people that are looking at those, that are auditing those. But it seems to me, at least, that that was also something where there were serious breakdowns in the process this time around.

So, I appreciate the hearing, Mr. Chairman. I'm anxious to -- to hear from our witnesses. This is a critically important issue. And -- and we need to do everything we can to double down our efforts to make sure that these types of incidents don't happen again in the future. Thank you.

AR 001000

ROCKEFELLER:
Thank you, Senator Thune.

I want to both explain and apologize to our witnesses. We do this, and -- and there are a number of people in addition to those who've spoken here on the dais who want to say things. We can't. What we would traditionally do is we have the relevant subcommittee chair and ranking members say a word. You, in turn, have to listen to that. But on the other hand, they made some pretty good points.

So, I would now call on Secretary Napolitano. We welcome your -- your statement.

NAPOLITANO:
Well, thank you. Thank you, Chairman Rockefeller, Senator Hutchins (sic), members of the committee, for the opportunity to testify on the terrorist attack aboard Northwest Flight 253 on Christmas. I am pleased to be here today with Director Leiter, with Governor Kean and with Representative Hamilton.

Now, as President Obama has made clear, this administration is determined to find and to fix the vulnerabilities in our systems that allowed this attack to occur on Christmas day. Our country's efforts against terrorism include the actions of the Department of Homeland Security and many other agencies, as well as those of our international allies. So, I'd like to focus my statement, Mr. Chairman, on the DHS role within these larger efforts.

First, by and large, DHS is a consumer of the United States government's consolidated terrorist watchlist, which we use to help keep potential terrorists from boarding flights and to identify travelers who should undergo additional screening.

Within the United States, DHS performs physical screening at airport checkpoints and provides further in-flight security measures. Outside of the United States, we must work with foreign governments and airlines to advise them on which passengers may prove a threat and required security measures for flights bound for the United States. As you know, TSA does not screen people or baggage at international airports.

Now, regarding the Christmas day attack, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with explosives on his person. The interagency process to fix these vulnerabilities highlighted by this attack is well underway. And as a consumer of terrorist watchlist information, DHS welcomes the opportunity offered by this process to contribute to improving our federal government's ability to connect and assimilate intelligence. And we are working with the NCTC, with the ODNI and others to do that.

We're also focused on improving aviation screening and expanding international partnerships to guard against a similar type of attack. I believe several of the members have -- have made inquiry about that. So, I have submitted a longer written statement describing these various programs that work to keep terrorists from boarding planes and ask that it be put in the record.

In terms of the DH role -- DHS role in this case, the bottom line is this. He was not on the no-fly list, which would have flagged him to be prevented from boarding. Nor was he on the selectee list, which would have flagged him for secondary screening in Amsterdam by the Dutch. Furthermore, the physical screening performed by foreign authorities at airports in air -- at airports in Nigeria and in the Netherlands failed to detect the explosives on his body.

Now, immediately after the attack, DHS responded quickly. And -- and let me pause here a moment, Senator Thune. I -- I think you have quoted my words back to me exactly. The situation worked an unfortunate phrase that was inaccurate and for which I apologize.

But I'd like for your understanding in context, because, while it was a failure that he was allowed to get on this plane, it was a failure that we did not know that he had these intentions, once this incident occurred, the following operational activities took place, conducted through the leadership of the TSA.

First, we directed the FAA to alert all 128 flights from Europe bound for the United States of the situation. We increased security measures at domestic airports. We implemented enhanced screening at all -- for all international flights coming to the United States. And we reached out to state and local law enforcement air carriers international partners and relevant agencies to provide -- provide them with the information they needed on the ground.

Now, we have outlined in our report to the president five areas of action that correspond very well with what the members have commented on and their -- in their statements.

First, as this incident underscores, aviation security is increasingly an international responsibility. That's why I dispatched Deputy Secretary Lute and other top DHS officials on a multi-continent tour to meet with our international counterparts on these measures.

Tonight, I will travel to Spain to meet with my European counterparts tomorrow to work on strengthening international security and standards for aviation, including information sharing between countries, technology and other issues.

Third -- or second, excuse me, DHS has created a partnership with the Department of Energy and its national labs to use their scientific expertise to improve screening technology at domestic airports.

And it goes to a point you were making, Senator Dorgan.

Third, DHS will move forward in deploying enhanced screening technologies, like advanced imaging technologies and explosive trace detection machines to improve our ability to detect the kind of explosives used in the Christmas day attack. We currently have 40 of these machines deployed in the United States. We intend to deploy at least 450 more this year.

Fourth, we will strengthen -- the strengthen the capacity of aviation law enforcement, including the Federal Air Marshal Service. I would include here as well that we intend to

AR 001002

increase other law enforcement techniques as well, including behavior detection officers at our airports.

And finally, DHS will work with our interagency partners to re- evaluate and modify the way the terrorist watchlist is created, including how names are added to the no-fly and selectee lists.

I am very glad to be working with my colleague, Director Leiter; Admiral Blair, with whom I was with this morning; in addition to the members of this committee, who have done so much to improve our national intelligence and commerce apparatus, as these -- as we deal with these issues.

And I'm also very grateful to the men and women of the Department of Homeland Security. They work hard every day, every week, to keep this country safe against terrorist attacks. And that is work that is ongoing.

And that, while I cannot ever guarantee, and I will not to this committee or any committee, that we will never have another attack by someone like an Umar Farouk Abdulmutallab, I can tell you this -- that our department is working every day in every way we can think of to keep the American people safe.

ROCKEFELLER:
Thank you, Madam -- thank you, Madam Secretary.

And now, Director Leiter.

LEITER:
Mr. Chairman, Senator Hutchison, members of the committee, thank you. Needless to say, I -- I wish that my introduction to this committee were under a very different set of circumstances then they are today.

I'm honored to appear also with Secretary Napolitano, Governor Kean, Congressman Hamilton. But I also want to say that I am honored to appear.

I know in our audience today, in the gallery, are members of the families of the victims of 9/11. And I want to make a personal pledge to them on behalf of myself and also the members of NCTC and the counterterrorism community to continue to do all that we can to honor their family member's memory by trying to keep the scourge of terrorism from touching others.

I want to start with an assertion which I hope is as crystal- clear as Secretary Napolitano's was. Umar Farouk Abdulmutallab should not have stepped on a plane on Christmas day. The system failed. The counterterrorism system failed. And I, along with other leaders, have told the president that.

I'm here to tell you that. And I'm here to tell the American people that. And I think most importantly, that we are determined to do better.

The director of national intelligence and I have both been tasked by the president to look at how we can improve those elements of analysis, of collection, of information sharing and watchlisting that obviously need to be repaired.

I'd like to quickly run down some of the events that led to the Christmas day attack. And although I can't go into great depth in an open session, I -- I think it's important to make some points; because frankly, there are no shortage of inaccuracies in the media that have been reported.

But I want to start first by debunking what has become conventional wisdom among some -- that this is the same failure that occurred on 9/11. It is not And that is not to suggest that it is not potentially tragic; but it is to highlight, because, unlike 9/11 where there was a failure to share information the U.S. government had, that is not what occurred in this case. And obviously, any prescription for repairing the failings has to know what caused the failings in the first place.

I would open also by saying this is all the more frustrating to me, because the intelligence community and NCTC did identify many of the things that led up to this attack. But we very much failed in the last tactical mile of associating some of the plotting that we saw with this individual, Umar Farouk.

Throughout 2009, in the fall, in front of other members of Congress, we spoke to the growing danger posed by Al Qaida in the Arabian Peninsula, and in particular the danger posed by European and Western recruits that they might have for plotting against the homeland.

And although we didn't know it at the time, we were concerned about operations on Christmas. But again, we did not connect that with Abdulmutallab. And we also warned about the type of explosive that Abdulmutallab used and the ways in which it might prove a challenge to screening, which of course manifested itself on Christmas day.

But again, despite these pieces that we did connect, we simply did not make the final connections. And we failed in doing so the last tactical mile linking this individual to this plot.

We did, in fact, have the information from his father about his concern he expressed with his son going to Yemen, and that he had come under the influence of religious extremists, and that he was not returning home. And we had other streams of information from other intelligence channels. So, we ended up with a partial name, an indication of a Nigerian. But no piece of intelligence brought that together. Nor did my analysts, or my organization or I bring that together.

As a result, although Mr. Abdulmutallab was, in fact, entered as a known and suspected terrorist into what is known as the Terrorist Identities Datamart Environment, that list of 550,000 I believe Senator Thune referred to, he was not watchlisted, because this information was not connected to him. And hence, he also was not placed on the no-fly or selectee lists.

Had all of the information that was available to the U.S. been linked together to this one individual, he would have undoubtedly been watchlist. And therefore, he would have been on the visa screening list and the border inspection list.

And I want to read this verbatim, because it's a -- it's an important point. Whether he would have been placed on either the no- fly or selectee list, again based on the existing standards of 2008 and 2009, would have been determined by the strength of the analytic judgment about exactly who he was and what he was doing.

And, as I'd like to note quite clearly, one of the lessons that we have learned and the president has tasked us to do, is to review these watchlisting standards in a way that they are as flexible and as nimble as the enemy we face.

Finally, and I hope I have made clear that I do not wish to make excused for what we didn't do right. We didn't do things right. And we didn't do things well. I do want to note the context for some of these failings.

Each day, NCTC receives and reviews literally thousands of pieces of counterterrorism intelligence. Although the exact number is classified, it is well over 5,000 pieces of terrorism data, with more than 5,000 names each day. We put on the watchlist more than 350 individuals a day. And we look at more than 30 or 40 specific plots every day.

So, although I undoubtedly admit we must do better, the multi- dimensional and varied nature of this threat means that even intelligence is not a silver bullet. It is one part of a multilayer set of defenses, including technology, international cooperation and screening that we must combine.

Briefly, and of course I'll -- I'm happy to take more questions on this, we are trying to improve this situation as quickly as we can pursuant to the president's directive of January 7. In line with the president's conclusions and his direction, we're moving in really five broad areas.

First, as a number of you have noted, we're examining the no-fly list standards. Frankly, the pressure over the past eight years has never been to put more people on the no-fly list. It has been just the opposite.

We have to look at what those standards are and ensure that we are, again, flexible enough to have individuals, either selectees or no-flys, regardless of whether or not we have specific intelligence about their involvement in operations.

Second, although we saw the growing threat in Yemen, we, and I include myself in that -- in that we, and the DNI did not adequately move resources to address that threat. We were simply more focused on the threats that we saw within Yemen. And the threat outside was not addressed quickly enough with additional resources. We need to do that. And that has already been done to some extent.

AR 001005

Third, we have to move away a bit from a names-based system of tracking threats. It's fairly easy, and I think we're quite good as proved in many cases in 2009, to tracking threats when we know a name, and we know what the plot is. But it's much, much harder, and we have to do a better job of pursuing small, discrete pieces of data that don't automatically add up to a threat. That is our challenge. And we are trying to do that now.

Fourth, we are making sure that we assigned priority for tracking of threats as they come in. And we have done that quite well, again, when the threat is of a high profile and something we understand fully. We have to assign that same level of responsibility when we also are not sure what the threat is.

And finally, we have to make sure, again, that the records within our watchlists are enhanced to the extent they can. This is certainly a matter of technology. And technology applies to all of the areas I've already discussed. But it is also simply a matter of having enough people to put their eyes on these records and make the connections that will help keep the nation safe.

Although I would strongly echo what Secretary Napolitano noted: that none of this will guarantee security. But it must be used to perfect the system to the greatest extent possible. Thank you, and I look forward to working with the committee.

ROCKEFELLER:

Thank you, Director Leiter.

Now, the Honorable Lee Hamilton.

HAMILTON:

Chairman Rockefeller, Senator Hutchison, members of the committee, Secretary Napolitano and Director Leiter, Tom and I of course are delighted to be with you.

And I think we are eternally grateful to the members of the United States Senate for the way in which they have followed up the implementation of the recommendations of the 9/11 Commission. The actions of the Senate over a period of several years now have just been exceedingly good from our standpoint.

My remarks will be, I hope, very brief and on target. They will be directed principally to the questions of intelligence and not so much to commerce.

I was gratified to hear from a number of you, as you spoke, about the necessity of the recognizing that the threat is real. And we have to reject complacency and recognize that that threat is genuine. I think many of you emphasized that in your remarks.

Tom and I appear here -- here today as members of the National Security Preparedness Group, which is a successor to the 9/11 Commission. It's made up of a number of people, evenly divided

between Republicans and Democrats. I think their names are familiar to you. They're in the written testimony.

In the years since the passage of the Intelligence Reform and Terrorism Prevention Act, which created the director of national intelligence and the National Counterterrorism Center, it is our view that the United States government has made significant positive strides to correct the shortfalls that were obvious on September 11. But obviously, we've seen from the incidents at Fort Hood and the skies above Detroit, there's a lot of work to be done.

The DNI has been hobbled by disputes over its size, its mission and its authority. Nonetheless, the determination of the terrorists who attack the homeland remains unabated, demonstrated by these events and, from our point of view, understands the critical importance for creating and supporting the DNI and the NCTC. It is imperative that the DNI and the NCTC be successful in their vital and very complex missions that they have been asked to undertake for the country.

We note with approval, as Director Leiter said a moment ago, while other failures did occur, apparently the Christmas attack was not a repeat of the failures to share information that were evident on 9/11. That suggests to us that progress has certainly been made, and that agencies and analysts are sharing critical information.

In an age when we are collecting more information than ever before, the real challenge, it seems to us, is how do you understand, manage and integrate vast amounts of information?

It's really a problem of data management. We need better management of the data. And, of course, we have to look to the state- of-the-art technology to help us better sort through massive amounts of information to ensure the right people are seeing it in time to make a difference.

The greatest single challenge that arises from this incident, in our view, is the urgent need to strengthen the analytic process. We are pleased that the president has asked the DNI to look at this issue. And he is certainly properly situated in the community to assume a leadership role in that respect.

Another lesson that emerged from the Christmas attack reminded us of 9/11. We repeatedly said that one of the problems there that was no one was in charge. Well, in a sense, that's what's happened here. The intelligence community is designated as in charge of running down all the leads associated with a particular threat.

We welcome redoubled efforts to assure that responsibility for investigation leads on potential threats are assigned, pursued and acted upon immediately and aggressively. We need to do a better job of judging the sources of potential attacks. We are seriously behind the curve when, as the director said a moment ago, we were not sufficiently aware of a possible attack on the United States from Yemen.

The final point I want to make is that one of the things that has always concerned me about intelligence is that, though I think the intelligence community does a very good job, I don't think they do as good a job as they should on longer-term threats.

That's quite understandable that they should concentrate on the near term. But I think this is -- this incident is an example of it -- so heavily concentrated on Iraq and Afghanistan and Pakistan for reasons that are obvious to all of us, that we kind of did not see, or at least did not see sufficiently, the kind of attack that could come to us from Yemen -- a longer-term perspective.

And I think the intelligence community must learn, not only to focus on the immediate threats, but also threats that are developing, as they were in Yemen. I turn to Governor Kean.

KEAN:
Thank you, Lee.

And thank -- thank you Chairman Rockefeller. I'm sorry. Vice Chair -- it's on now? Thank you.

ROCKEFELLER:
Thank you for being here.

KEAN:
Well, thank you, Mr. Chairman. And I thank you...

ROCKEFELLER:
I tend to think of you two as founding fathers.

KEAN:
Well, thank you. But the -- I would -- I would mention to the committee, by the way, something that Mr. Leiter also said that it seems remarkable to me we have, here in the room with us today, again members of the people representing the families of 9/11.

It is remarkable to me that all these years after they suffered that tragedy, that they're here, hearing after hearing, that I talk to them on the phone all the time, that they have never flagged one minute in their efforts to make sure that that never, ever happens to families again. They're a remarkable group of people. And I just want to commend them to you today.

HUTCHISON:
That's very impressive. That is.

KEAN:

Yes. The -- I'd like to say just a word about the effectiveness, again, of the DNI. We're frequently asked, Lee and I, both of us, how is it working? You know, how's it working? And so, we've been trying in our new group to conduct a review of Intelligence Reform and Terrorism Prevention Act and see just how effective the DNI is. And we began our work to try and answer that question.

We have a lot more work to do, obviously. But what we can see already is that the DNI has achieved a meaningful measure of success in its first year. It has made it probably, hopefully, worthwhile the inevitable turmoil.

But it's a work in progress. And it's probably closer to beginning of reform than the end. Some of the successes of the last five years include progress and information sharing, a joint duty program, and despite the failures evident in this attack we've been talking about on Christmas, the National Counterterrorism Center.

Since September 11, 2001, the NCTC and other government agencies have repeatedly connected the dots. And they have, in the past, shared the information necessary to prevent terrorist attacks. Improvements have clearly been made. Although that sharing is not as prompt, nor as seamless as we would like it to be.

But what the DNI and the NCTC need most of all, in our opinion, is the unyielding support of the president and the Congress, if those organizations are going to achieve their role in integrating the intelligence community and preventing these attacks.

You know, we all gave the DNI a very, very difficult job, and a gargantuan to-do list. And the DNI was given substantial authorities to accomplish those missions. We are concerned about the expanding growth and bureaucracy of the DNI. And we urge vigorous re- evaluations of all its functions to assure that it's lean and efficient.

The DNI's authorities must be exercised with discretion and consideration of the priorities and sensitivities of the other intelligence agencies that it works with.

However, to be sure, there are still ambiguities -- ambiguities, excuse me, in the law that you passed. These ambiguities can (inaudible) to mission confusion and sometimes a lack of clarity, perhaps, in the lanes in the road. But the burden is on the president to be clear on who is in charge of the intelligence community and where final authority lies on budget and on personnel matters.

Absolutely crucial here is the president's leadership, or we run the risk of mission confusion and a decrease in the prospect of long and lasting reform that was recommended after September 11, 2001.

Let me say just a couple of other matters here before I close. The chairman mentioned in his opening remarks the problems and the balance that always has to occur between civil liberties and the need to keep ourselves safe. This will always be part of the struggle against terrorism.

We'll face these decisions all the time. And we can't sacrifice one for the other. We have to keep both. We have -- we're in the business of protecting freedom and liberty as well as fighting terrorism.

Now, we have recommended a board. This board has been dominant for a couple of years. And the Congress passed that legislation. With a massive capacity to develop data on individuals, this board, Civil Liberties Board, has to be champion of the seeing that the collection capabilities do not include, and do not intrude unnecessarily into privacy and civil liberties.

We continue to believe that that board, that we recommended and the Congress put into being, has critical functions and should be established. It doesn't now exist. The president has not yet appointed the members. So, we urge President Obama to reconstitute it, quickly appoint its members and to allow them full access to the information and the authority to form -- to perform and do this essential function.

Now, you are doing exactly what is required here in this room today. Nothing probably is as important in this whole intelligence area than your oversight, congressional oversight. And we placed a tremendous amount of importance to that in our report.

I know our recommendations, the creation of the House Homeland Security Committee and the Senate Homeland Security Committee, and Governmental Affairs Committee. However, there is enduring, fractured and overlapping committee jurisdictions. And that's true on both sides of the hill. And this has left congressional oversight, in our opinion, not yet in a satisfactory place.

DHS entities still report to dozens of separate committees, hundreds of times per year. And that takes, as every secretary has told us, a tremendous drain on their time and resources for their most senior officials. Furthermore, the additional melee among scores of congressional committees has led to conflicting and contradictory tasks and mandates for DHS.

Now, we worry that, unless we work to fix this system, its unworkable, and it could make this country less safe.

We also called congressional oversight over intelligence dysfunctional at the time of our report. We made recommendations to strengthen the oversight committees, which were not accepted by the Congress, although undoubtedly some progress has been made.

Today, we'd just like to emphasize the tremendous, enormous importance we attach to rigorous oversight of the intelligence community. Congressional oversight can help ensure the intelligence community is operating effectively and help resolve disputes about conflicting roles and missions, when they occur.

We urge you all, Congress, to take action to strengthen the oversight capabilities of the intelligence committees, because we think if you don't oversight (inaudible) intelligence, nobody does. And we would commend you -- commend that task to you. Thank you.

AR 001010

ROCKEFELLER:
Thank you, Governor, very much.

I -- there's no way that I can agree with you more about the need for oversight. It's really the only instrument that the -- that the Legislative Branch has. And it -- because of its classified nature, it's reserve really to two -- for the most part, to two committees, one in each house.

And I -- I do know that -- that, over the last number of years, what -- what the basic changes that have been made are, in fact, to take the Intelligence Committee, which was a so-called B committee, to make it an A committee more -- more budget -- excuse me.

And secondly, it was term-limited. It was term-limited to six years or eight years. I forget which it was. We got rid of that. So now, members are on permanently at the discretion of their respective leaders in their respective parties in both houses.

A great deal of the experience of the Iraq and Afghan war were, in fact, trying to bludgeon, you know -- all kinds of words I could use for it -- to try and pry out from the administrations -- both administrations, Republican and Democrat -- who hold on.

People think that -- that the intelligence committee is only intelligence. They have the intelligence. They don't. They only get what the administration's willing to give them. And so, sometimes you have to use strong-arm tactics.

Somebody says, "I need a deputy." I said, "I need full information." I used that tactic once, and it worked. A DNI got a deputy director, because he agreed that he would brief, not just the gang of six, the gang of four, the gang of eight, and all of that nonsense of earlier years, but the entire committee.

And so, that's the -- that doesn't say that we're getting what we should be, or that we're doing what we should be with what we get. But it does mean at least the process is headed in the right direction. And all of the folks involved in that feel very strongly about that.

Let me just -- I've already used a lot of time. I'm -- I'm just fascinated, Secretary Napolitano, with this concept of -- of screening watchlists. We've got the TIDE database. We've got the terrorist screening database. We've got the selectee. That's the first. It's 550. The second is 430 individuals. And then we go to the selectee, 14,000, and the no-fly, 3,400.

My -- my question and my frustration is -- and I -- and Director Leiter, I think that you said that there was -- there was movement to restrict even further the no-fly list. I think -- I think you said that.

LEITER:
Prior to December 25...

ROCKEFELLER:
Yes.

LEITER:
... we...

(CROSSTALK)

ROCKEFELLER:
But see, that's -- that's so wrong. I don't understand why, for example, with this Farouk Abdulmudalla (sic), why -- why is it that he can get on a list, which comes back from the State Department and goes to -- it's classified. But I know where it is. And so it's not possible to say that there is not some cause for doubt about him as a person.

But he doesn't end up on any list that means anything. So, he just cruises right on through, gets his two-year visa, Lagos, Amsterdam, Detroit, no problem, two-year visa. I don't understand.

The -- the question I want to ask is, do you think that there is -- Secretary Napolitano particularly, both of you -- that there is -- that -- that there's a false sort of division of databases and groups? That you move from one to another.

My instinct, just as a -- as an individual citizen, is the no-fly list ought to be a whole lot larger. Why -- why do we make the assumption that, because somebody's on the -- you know, the terrorist screening database list, et cetera, that that doesn't -- that's, you know -- and they're determined -- NCTC and the conjunction with the FBI, they determined they're known or reasonably suspected terrorists, but they can still fly?

And they're not even on the selectee list, much less the no-fly list. I don't understand those divisions. Should they be rethought in view of what happened on Christmas? Or do you think, I'm overreacting?

NAPOLITANO:
Mr. Chairman, first of all, that is an integral part of the -- the review and the actions that the president has directed, that that entire set of processes and -- and protocols that were set up to move from the -- the larger to the more specific in terms of the databases be relooked at in light of what happened on December 25, and in light of what could happen in the future. So, it should just be reactive, but also proactive.

As I -- as I said before, the CBP looks at the -- and these are protocols that have been in existence for a number of years. But they look at the no-fly list...

ROCKEFELLER:
You better explain CBP to us.

NAPOLITANO:
Customs and Border Protection. They look at the -- the no-fly list and the selectee list in terms of what happens internationally. That, too, is something that may need to be re- examined.

But I think you're -- you're -- the -- the -- the real heart of your questions goes to the watchlist, their systems, their creation overall. And let me defer to Director Leiter on that.

LEITER:
Mr. Chairman, the basic question, should the distinctions and differences be re-evaluated? The simple answer is absolutely, yes. And that's what the president's directed. And we want to.

I will say there is an enormous variation between different people on those watchlists. It ranges from the person who's associated with the financier to the operative.

Now, the standards that have evolved since 9/11, and again were promulgated in 2008 and 2009, made us make distinctions, which are readily apparent after 12/25, are distinctions that I believe the Congress and the American people are very uncomfortable with. And I believe they would make much more sense in light of the reaction we have seen to have many more people on the no-fly list or the selectee lists than we do today.

My only point about the pressure was, I will tell you, prior to December 25 of this year, the pressure had been, in fact, in the exact opposite direction. The pressure was to remove and scrub those no-fly and selectee lists and the watchlists, to inconvenience as few people as possible and reduce the number of false positives. That was the pressure under which we existed.

And I am more than happy, and as the president's directed us to do, we are going to re-evaluate that based on the events.

ROCKEFELLER:
Good. I'm going to call on, obviously, Senator Kay Bailey Hutchison. And after that will be Senator Dorgan, followed by Senator Begich, who appears to be missing an opportunity to ask a question.

(UNKNOWN)
(OFF-MIKE)

ROCKEFELLER:

AR 001013

OK. Just preside over the Senate?

(UNKNOWN)
No, actually.

ROCKEFELLER:
Oh, OK.

(UNKNOWN)
A real work meeting.

ROCKEFELLER:
Oh, a real -- OK. OK. OK.

Anyway, Senator Hutchins.

HUTCHISON:
Thank you, Mr. Chairman.

I just want to ask one more question along the same lines as the chairman's. And that is the association with the cleric, the Yemeni cleric who used to be operating out of Maryland.

After the Fort Hood incident, it would seem that there would be a deep looking into everything that might be associated or connected with that particular cleric. And so my question is why wouldn't the -- the -- Mr. Abdulmutallab and his association with that same cleric have been enough to get him on the database, to -- to at least have a big yellow flag, if -- if not a read one.

LEITER:
Absolutely, Senator. To begin, immediately after Fort Hood, and this is continuing, we have in fact engaged in interagency, CIA, FBI, National Security Agency, NCTC, scrub of all of Anwar Awlaki looking at his various contacts to determine who poses a threat.

HUTCHISON:
Would -- would those people that do have tentacles, that he has tentacles to, now be put on watchlist? I mean, can we be assured of that?

LEITER:

AR 001014

Those individuals, it -- it depends. It depends on the nature of those communications. In some cases, under the existing standard were -- standards, were someone to send -- you know, communicate in a way which was completely innocent, it might not put that person on the no-fly list. It might put that person on a different layer of the list.

And of course, the list itself, and being placed on that list, cannot be based purely on protected First Amendment activity. So, there may be some issues there.

With respect to Mr. Abdulmutallab...

HUTCHISON:
Let me ask you one -- one thing more, though.

LEITER:
Of course.

HUTCHISON:
OK, you had the Yemeni connection. And then you had the man's father, who raised a -- a flag of some kind. Would that -- do you have the capability to merge that kind of information and raise the level on -- on someone like that.

LEITER:
Absolutely, Senator. And, in fact, the failure here, and the failure on our part and elsewhere, was not making that connection. It was not making that connection between what the father came in and said, and other sources of intelligence.

Now, some of those sources of intelligence weren't flagged in a way that made is more likely that that intelligence would be connected. So, there were some failings there. But also, the basic act of seeing all that intelligence and piecing it together is what we did not do. But undoubtedly had it been, he could have been in a higher level of watchlist.

HUTCHISON:
OK, let me ask you this, because it goes back to the first thing that the chairman said in his opening statement. Do we have the tools now to communicate completely and effectively without bureaucratic mumbo-jumbo between intelligence sources and security forces on the ground, so that you can put those kinds of different levels of -- of an awareness together to raise it to a substantial awareness level?

LEITER:

AR 001015

Senator, this is going to be hard to believe. But probably the single best example where we go from the most classified sense of intelligence down to the operator in the field -- and this is true even after 12/25 -- is, in fact, the watchlist.

The problem here was not that that information did not flow, because it can flow quite easily to the police officer in the street, to the visa officer, to the Customs and Border Protection officer. Problem is we didn't have the right derogatory information associated with that record. So, we hadn't connected the intelligence to raise the flag. But the information could have flowed quite easily.

But, a second piece of your question is do we have the systems in place that make it easy to connect those pieces of data in the first instance? And the answer is yes in some places and not nearly enough so in others. Some agencies are far ahead of others. And we still have clearly some systems which are so rudimentary and basic, that they're not doing a good job of that.

For example, the State Department's visa system, where, when they mistype one letter in the name, his visa does not come up. I consider that a significant weakness in the technological system that enables effective information sharing.

HUTCHISON:
OK. I guess my final question, to kind of just get to the nugget, is do you have all of the authority to do what needs to be done? And -- and I'm not even saying this is easy, because I know if a -- if a father comes in and says I think my son is someone you should watch, maybe that, in itself, by itself, isn't enough.

But then you have a Yemeni cleric. And maybe that wasn't quite enough to also matter. But together, you've got to be able to say...

LEITER:
Absolutely.

HUTCHISON:
... OK, put this together, it is really big.

So, do you have the authority -- and Madam Secretary, do you all have the authority -- to get to the heart of this, and not have all these constraints and different bureaucracies and different rules, and all of the confusion that seems to maybe exist sometimes?

LEITER:
Senator, I'll try to be very brief. I think the basic system structure works. But there are four areas which undoubtedly we need to focus.

One is technology. The technology is not as advanced as it needs to be to connect all of these pieces.

Second, in terms of authorities, to make sure that people are following up in the way they need to follow up. Those authorities, frankly, to the National Counterterrorism Center were purposefully vague. And we are now working with the White House through the president's direction to make sure there is accountability.

Third, we simply need the people to do it, because you can have the best Google-like tool in the world. You need the people to work that watch list and look at that information.

And fourth, I think...

HUTCHISON:
Are you saying we don't have enough people on the job? Is that...

LEITER:
I think, absolutely. As I tried to make clear, we did not have enough people to put on this Yemen problem. And we did not shift people away from other problems quickly enough.

And now, what we've been directed by the president to do, I think there will be a resource tail to make sure you can pursue these minute leads in a way that you can have greater confidence that they will be tracked down and will be connected, exactly the way you and the American people expect and deserve.

NAPOLITANO:
Senator, what I would add to that is, again, the international dimension of this is so very important.

You know, he traversed two international airports, Lagos and Amsterdam. Not every airport in the world operates at the same level of security standards.

We also, I think, quite frankly, to work more closely on the international scale in terms of sharing information about individuals, who's had a visa revoked and why, for example. And so, that is part and parcel of the corrective action that we are taking.

HUTCHISON:
Thank you.

ROCKEFELLER:
Thank you very much.

AR 001017

This is -- this list, which changes as people come in and go out, which is what always happens, which is fine -- is done in order of original appearance, so that it's fair, although some may like it more than others.

Senator Dorgan?

DORGAN:
Senator Rockefeller, thank you very much.

I am not exactly clear on all of this. And I know it's complicated. I wasn't sure back in 2002 whether creating the Department of Homeland Security was the right thing to do. We put 22 agencies together in the biggest merger of federal agencies since the Second World War. Maybe that's the right thing, but we put a lot of different cultures together.

And then the question of DNI. It wasn't clear to me whether it was very smart to do that, although I understood. We had all these stovepipes sticking up, and nobody trying to coordinate them. So, I understood that wasn't working very well.

But as I understand it now, we have -- we now have 16 different agencies involved in the intelligence system, eight agencies involved in the watch-listing process, those eight agencies in the Terrorist Identities Datamart Environment. And we have, I believe, three different agencies involved in placing individuals on the Terrorist Screening Database. And only then would Homeland Security come in and make decisions about placing individuals on either a no-fly list or a selectee list.

And maybe that's not exactly correct, but it seems to me you've got a lot of agencies doing a lot of different things.

What I don't understand is this. When we created DNI, we were going to try to deal with these stovepipes. So, what happens -- if you can tell me in an unclassified situation -- what happens when a father comes and says to our intelligence community, look, I've got a kid out there -- and I've seen some rumors about what the conversation was -- but I've got a kid out there that's gone wrong. It appears to me there is some -- you ought to have some concerns about links to terrorism.

What happens to that information? Where did it go? And where was the failure?

NAPOLITANO:
If I might, before I'm going to...

DORGAN:
Right.

AR 001018

NAPOLITANO:
... defer to Mike again. But there's something in your question that was not correct.

DORGAN:
All right.

NAPOLITANO:
DHS does not create the selectee or the no-fly list. We receive the selectee or the no-fly list. And that is then used by CBP officials at foreign airports to advise foreign governments, or foreign air carriers, as the case may be, about particular individuals.

DORGAN:
All right.

NAPOLITANO:
I just wanted to be clear about that.

DORGAN:
Thank you.

Mr. Leiter?

LEITER:
Two things should have happened when that father came in. One thing happened, one thing did not.

The first thing is, the agency that received that sent the message back to headquarters, and that message was also available to NCTC. That's the good.

Not so good, it was not disseminated in a way that it was widely available to the rest of the intelligence community.

Now, I do want to stress, that's still different from what happened on 9/11. That was simply...

DORGAN:
Why was it not disseminated?

LEITER:
It was fundamentally the oversight mistake of an individual office. And I believe the director -- Director Panetta, Leon Panetta -- has already taken steps to solve that problem.

DORGAN:
Was there a process or a procedure that was ignored? Or was it a person that made a mistake? Tell me...

LEITER:
Senator, I'd actually prefer -- happy to take it up with you in some sort of closed session. But also, I would frankly like to defer to Director Panetta, who can speak more specifically to the procedures of that agency. But the information was somewhat available.

The second thing that should have happened and did happen was, after that meeting, the State Department and the embassy had a -- the country team had a meeting to say, was this person someone that they had to be worried about. And they, in turn, nominated him to the Terrorist Identities Datamart Environment, to the NCTC, as a possible terrorist, based on this interview.

That occurred. He was nominated. He was placed on the watch list.

The one thing that did not occur there was, again, when they checked to see if he had a visa, they misspelled his name, and, hence, did not discover he had a visa.

DORGAN:
They misspelled the last name, apparently?

LEITER:
Correct.

DORGAN:
And so, one of the intercepts, I understand, one of the earlier intercepts actually had his two first names.

LEITER:
Umar Farouk. That's correct.

DORGAN:

AR 001020

Yes. And so, there's his father. There's an intercept with two first names that were spelled correctly. There's an intercept about maybe something December 25th. There's an intercept with somebody from Nigeria and a possible action.

And so, you have all these things. I guess I'm wondering, with all these agencies -- 16 and eight and three, or whatever -- is there somebody that's sitting around that, as a result of DNI, that gets rid of stovepipes, and you bring it into a desk or a room, or some situation room, and somebody gathers all that and says, aha. I see. This is a puzzle. And I just got the five pieces. I put the five pieces together, and we've got a guy out there that's trouble, and we're going to make damn sure he's not on an airplane.

So...

LEITER:
The primary responsibility for doing that was mine as the director of National Counterterrorism Center, NCTC.

Also with responsibility, pursuant to the president's conclusions and consistent with past practice, was the CIA. We both had responsibility to do that, and we didn't do that.

Now...

DORGAN:
Well, I understand. From an organization, and from heading an organization, I understand what you were saying, and I admire that.

But I'm asking, in the organization, do you have a group of people who are sitting there pulling all those pieces together to say, aha. Now we see something that's about to happen, and we're going to take action.

LEITER:
Senator, two pieces of that. One, I will tell you that, although I can't speak to it fully in an open session, part of what you cited in the press reports was, in fact, discussed in analytic products that we had provided to policymakers concerned with operations.

What we did not know, and what we did not connect, is exactly who and where. So, we were, in fact, concerned of an operation, but we hadn't pieced those pieces together.

But second, if I may, senator, one of the reforms that we've already started to initiate, and which I think is critical and does have some repercussions concerning (ph) the need for people, is to put together exactly the teams that I think you imagine. And their sole job is not to write intelligence for policymakers, but their sole job is to dig into, in interagency way with all the information, these bits of data, and piece them together and uncover the plots.

AR 001021

DORGAN:
Mr. Chairman, my time has expired. Let me thank -- there are other questions I'm going to submit, if I might.

And let me also say to you that I see there are other relatives -- relatives of the victims of Colgan crash. I want to mention that they are here, too. And they are at every hearing that we hold dealing with the issue of safety. And I admire the passion with which they now serve their country, coming to these hearings.

ROCKEFELLER:
Thank you, Senator Dorgan.

And now, Senator Lautenberg.

LAUTENBERG:
Thank you very much, Mr. Chairman. Because we have so many questions that we'd like to ask and that time not permitting that, can we be assured, Mr. Chairman, the record will be kept open and that the witnesses are instructed to respond.

ROCKEFELLER:
Absolutely.

LAUTENBERG:
And I would ask our wonderful witnesses at the table -- that includes all of you, by the way -- that the answers be as brief as possible, rather than the questions taking all the time.

But I want to -- the mystery about whether or not someone on one list doesn't match up with another. I mean, I come out of the computer business, and so does my colleague here. And, you know, there are lots of things that we do in the commercial world that get names, identify it immediately. If you ever walk in with a credit card, and you're in Paris or Lisbon or wherever, put your American Express through the slot, and the answer comes back immediately.

Now, why, therefore, isn't the technology available that talks about those people who are on the no-fly or the terror watch list? I think it's outrageous to suggest that multiple departments are required to check on one another and create an organization that gets rather cumbersome at its roots.

LEITER:

AR 001022

Senator, if I may, because I must have misspoke. The lists are coordinated with one another. There is no disconnect between the lists except if there has been a choice that the lists should not match. And what I mean by that is, if you're in TIDE, we know if you're in TIDE whether or not you're in the next list and whether or not you're no fly, and there's been a decision that one does not qualify for the other.

The lists speak to each other and are fully coordinated with one another.

LAUTENBERG:
Thank you.

Governor Kean, the Detroit bombing attempt raised questions about who should be on the terror watch list -- much of what we're talking about here, including the no-fly list. But even people who oppose such a serious threat that they're not allowed to fly are still able to buy guns in this country. And there's discouragement of excessive interference or follow-up. You have to destroy lists in 36 hours, and you have to respond in three hours.

And here we're talking about something that -- you're talking about, worried about a gun. You've got an airplane full of people. There is, in my view, there is no comparison to the threats that it posed.

Do you support closing the terror gap by giving the attorney general the authority to deny gun purchases to people who are on this list, just to deny them outright?

We've heard the plea on the other side that said, well, someone could be on there incorrectly or unfairly. Too bad. I don't want to break the law, and I don't want to invade privacy. But the fact of the matter is, we ought to be able to access these things and err on the side of the safety of the American people.

What do you think, sir?

KEAN:
Senator, the attorney general has asked for that authority, and I would certainly back him up, that he should be given it. I think, to allow people on the terrorist watch list to go in and purchase weapons of any kind is just not very wise.

And as far as the other law goes, the FBI, as we know, had the Fort Hood shooter under observation and were looking at him. What they didn't see was the fact he had walked into someplace called Guns Galore and bought weapons, because the law now says the records have to be destroyed within 24 hours. It used to be longer than that.

In fact, if it were there longer than that, the FBI might have had that information, might have connected the dots. And who knows whether or not it would have been prevented or not. So, I would recommend that you might look at both of those things. And particularly as this attorney

general has asked for, and the previous administration also asked for, terrorists should not be allowed to get weapons.

LAUTENBERG:

Secretary Napolitano, what's your department think about closing this loophole that permits gun purchase? I am leaving the Detroit situation to the review by my colleagues. I want to focus more on this relatively narrow area.

NAPOLITANO:

You know, senator, I'm not sure that right now I'm prepared to give you an answer on that. What I am prepared to say is that, look. There are a lot of things that have to happen to prevent somebody like an Umar Farouk Abdulmutallab from getting on an airplane. It's a very layered system.

It begins with intel and all of the ways that Mike has described how the intel works, up to when somebody shows up at an airport. Then all the layers within the airport itself -- some seen, some not seen. It's all of those things combining together that, done right and done in a coordinated fashion, minimize the risk that there will be an attack on Americans.

LAUTENBERG:

Mr. Chairman, are you going to permit...

ROCKEFELLER:

Yes, we'll continue (ph).

LAUTENBERG:

... a second? I just want to close by saying, there are some 600 million American Express -- or Visa cards around the world. You can go anyplace in the world and try to buy something, and they know immediately whether you're eligible (ph).

ROCKEFELLER:

Yes, another question that comes from that is, what is it that airlines can do if they're paid in cash? I'm convinced there has to be something they can do to follow up. I don't want an answer to that now.

You have to leave in 10 minutes for Spain -- leave here for Spain.

NAPOLITANO:

AR 001024

Sir, I'll be happy to hang around for a few more minutes, if this can answer some more questions.

ROCKEFELLER:
Well, then, now you've made a liar out of me to Senator Snowe.

LEITER:
I'm happy to leave in 10 minutes for Spain, Mr. Chairman.

(LAUGHTER)

ROCKEFELLER:
Oh, you do. OK. All right.

NAPOLITANO:
Mr. Chairman, if I could...

ROCKEFELLER:
No, I want to...

NAPOLITANO:
... leave by 4:30, that would be...

ROCKEFELLER:
That's what I'm talking about.

NAPOLITANO:
... 4:30, yes.

ROCKEFELLER:
That's called "10 minutes."

(LAUGHTER)

NAPOLITANO:
OK.

ROCKEFELLER:
Thirteen.

(LAUGHTER)

Would you please give me some idea of why, when you go over there and meet with the Europeans, why -- what hope is there for bringing some sense of rationality between the practices that we pursue at home in terms of screening, machinery, you know, whole-body imaging, which is considered a civil liberties problem. On the other hand, that's the only thing which probably would have discovered what this guy had in his underpants.

What do you sit down and talk with them about? There's got to be a common system that works around the world. But you're dealing with separate societies. Some of them are so pro-civil liberties that they are very lax. On the other hand, I don't know how any of them could be in Europe, because they're the ones who have taken most of the pounding.

So, what do you do? I mean, what about the folks at Lagos? What about the folks at Amsterdam? What about the folks in less or well traveled countries? How do you rationalize this system?

What are you going to do for the next few days?

NAPOLITANO:
First, we're using the December 25th attack as a catalyst. There were passengers from 17 countries on this plane. This illustrates the international nature of this problem.

And the initial meetings that the deputy secretary held in the immediate wake of December 25 were fruitful in a way that some meetings that I'd had over the course of last year were not. So, we're going to use this attack as an opportunity to see if we can get agreements made that we have not been able to get before.

Secondly...

ROCKEFELLER:
Like what?

NAPOLITANO:
Like better exchange of information about passengers. Like standardization of the kinds of equipment and procedures that will be used in airports on randomized bases, so that terrorists can't predict what's going to happen, one at one time or one at another.

Like training and increase of capacity of law enforcement on the ground in countries, particularly in airports that may not have the capacity right now. Like a real outreach and focus on airports that have the larger percentage of throughput of last points of departure to the United States -- all of that underway.

We'll be meeting with individual countries. We'll be meeting with groups, i.e., those from the E.U. We'll be meeting with ICATA (ph) -- or I will be meeting with ICATA (ph) -- which is one of the international air travel associations, on Friday. And we've already been meeting with ICAO, which is the U.N. air safety, air security branch, which is located in Canada. We've already been meeting with them.

And our goal, Mr. Chairman, is to say, this is not just a United States problem. In this century, everybody from around the world needs the ability to travel and to know that the air environment is a safe one.

So, it's designed to get more uniform standards, higher standards, increased training capacity, increase both physical law enforcement and technology available around the globe.

ROCKEFELLER:
OK. I thank you.

And I call upon Senator Snowe. And I thank you...

SNOWE:
Thank you, Mr. Chairman. And I thank all of you for being here today.

These are, obviously, very, I think, key forums for eliciting exactly what went wrong and what we must do to prevent it in the future, without question. As one who has been involved in these issues for many years, going back into the 1980s when we were dealing with aviation security, international airports, and the list goes on, information sharing, and so on, it all still has a familiar rings in terms of rigid stovepipes. And it seems still a cascading series of failures, that thankfully and gratefully it was passengers on the plane that stood between a terrorist and a disaster.

So, we could have had a profound consequential event in this country. And I think we all understand that. But I certainly hope that we don't -- you know, somehow the sense of urgency in our institutions are not sublimated into bureaucratic quagmires.

I mean, it's something that we have to be focused on each and every day. And I know there are extraordinary men and women who serve this country. And, you know, so I understand that, and I understand your service and contribution, and I thank you.

AR 001027

And the tireless efforts of Congressman Hamilton and Governor Kean, thank you. You've been tenacious and tireless. And as watchdogs in oversight, and now with this major, mighty endeavor for this nation. And your unparalleled insights and expertise, I deeply appreciate it. And thank you for the continuity of that service.

And to all the families who are here today and who have lost loved ones, that continue to provide extraordinary public service, even in light of the profound personal grief that they have had to endure.

And that's a tribute to them. And it's why we're here today, continuing to ask these tough questions, because this is what it's all about. We've got to get to the heart of the matter.

Secretary Napolitano, I want to ask you several questions regarding Umar Farouk, so that I'm clear on the relationship that DHS had in terms of the information that is gleaned from such individuals.

Now, you said that you're the consumer of information. DHS is the consumer of information. But you also have an analytic branch within the Department of Homeland Security.

Now, was Umar Farouk ever debriefed by the Department of Homeland Security when he visited the United States and after he had traveled to Yemen?

NAPOLITANO:
Senator, I think that in an unclassified setting, that's probably not a question that I should answer.

SNOWE:
OK. So, when Customs and Border Protection obviously received the manifest 72 hours before departure, when or at which point was it clear that they needed to question him more?

NAPOLITANO:
They received 72 hours in advance of departure passenger name data, which is different than the manifest, which has a much more complete set of information.

What they push forward to a forward airport, where they have personnel -- and we don't have personnel in all foreign airports -- but where we do, they push forward the no-fly and the selectee lists. The no-fly list means you advise the carrier that person should not board a plane. Selectee, you advise the foreign government that person needs to get a secondary screening.

And a key difference you're getting at, or your question is getting at is, what happens -- why was it, when he was going to get to Detroit, he was going to be in secondary? He was going to be in secondary when he got to Detroit, because he had been identified as someone -- although not

AR 001028

on no-fly or selectee -- but he was in the larger database that should be looked at for secondary screening before admission into the United States.

So, you have one set of things that say, well, should he be allowed on a plane, and the other is should he be admitted into the United States.

SNOWE:
See, I don't understand that distinction. I have a really hard time with that.

NAPOLITANO:
Yes, I...

SNOWE:
I mean, I'm just stunned by it, to be honest with you. If somebody's a threat, they're a threat. I don't know how you make a distinction between a threat and an aviation threat. I mean, I just don't understand that.

And secondly, how was he ever allowed on the plane?

You know, I think that it's a fair presumption, that once that information has -- it has to be evaluated before anybody gets on the plane. And that's what I don't understand. And they have that manifest and that information 72 hours prior.

And so, all of a sudden they decided that they needed to question him further than a way to Detroit?

NAPOLITANO:
Senator, I'll be happy to provide you with a more detailed briefing, and your staff.

But if I might, again, 72 hours in advance, they have a passenger name record. It can be 30 minutes in advance if they get who actually is boarding a plane with more information that can be matched against a variety of databases.

Now, in terms of why he was allowed to get on the plane, if he had been on the right database, if he had been on the right list -- forget databases. Just take databases out of this equation. If he had been on the right list, he would not have been allowed to get on that plane in Amsterdam.

The mistake made here was, he was not on the right list.

Now, what are we doing to fix that? Part of it is improving the quality and extensiveness of the lists. Part of what we are doing is looking at how we use the lists themselves.

But again, since he was coming in from an international airport, we're not a solo actor even in that regard. Because even in that regard, we need cooperation. In this case from the Dutch, but it could be from another country, as well.

SNOWE:
But what information did you have, that Customs and Border Protection had to warrant further questioning between the time he boarded the plane in Nigeria and the time he landed in Detroit?

NAPOLITANO:
By the time...

SNOWE:
Because that is...

NAPOLITANO:
Yes. And by that time...

SNOWE:
... made certain assumptions that he was somehow, we would have had more information on him.

NAPOLITANO:
By that...

SNOWE:
And he should have been in the database, and that should have been pulled up.

NAPOLITANO:
I'm sorry. I didn't mean to interrupt. I apologize.

By that time, he had been matched with the note that had been issued by the State Department of some concern that he was associated with an extremist organization. That note, which was the State Department note, had never been matched up appropriately with the watch lists and the no-fly list.

SNOWE:
But your department can nominate individuals for the watch list. Is that correct?

NAPOLITANO:
Yes.

SNOWE:
And to the no-fly list.

NAPOLITANO:
Yes.

SNOWE:
I mean, you had that authority.

NAPOLITANO:
Yes.

SNOWE:
I mean, so that you don't create it, but you can nominate individuals, based on your acquisition of information. And you have more than 100 analysts. So, that clearly is a sizable organization to also analyze individuals that you debrief along the way.

I think that's important to understand.

NAPOLITANO:
And senator, I think in terms of that, we should go into classified. But let say this.

And this is an important question for this committee and for the Senate. Because as has already been mentioned, there has been, in the creation of the department and the creation of the NCTC and the creation of the DNI, all sorts of overlapping jurisdictions and authorities, and what have you.

A question is, does the intel and analysis part of DHS do the same thing as NCTC? Does NCTC do the same thing as others? Are we supposed to be a redundancy? What is our contribution in the INA field?

And the fundamental contribution of this INA, this department's INA, is to take information, intel that has been gathered and analyzed, and to push that out -- push that out operationally where it needs to go, or push that out, most importantly -- or as importantly -- to state and local law enforcement.

So, yes, we have an intel function. Yes, we can nominate. But we are not a redundancy. And I don't think we should be a redundancy with NCTC or DNI.

The redundancy here on the intel side -- and this was explained by John Brennan in the aftermath in the immediate report -- the redundancy that was designed in the system with respect to this information was between the NCTC and the CIA.

SNOWE:
Thank you.

ROCKEFELLER:
Thank you, Senator Snowe.

Now, Senator Klobuchar, to be followed by Senator LeMieux, and Senator Ensign and Senator Cantwell and Senator Udall.

HAMILTON:
Mr. Chairman?

ROCKEFELLER:
I want to get one thing straight. Who has to leave at 4:30?

(LAUGHTER)

KLOBUCHAR:
Did I -- after my question then, senator.

HAMILTON:
Mr. Chairman, Governor Kean has a five o'clock train he has to be on, so he has to leave promptly, as well.

ROCKEFELLER:
OK. But you do not, Mr. Director.

LEITER:
I'm here at your pleasure.

AR 001032

ROCKEFELLER:
OK. That's good. I thought you said you had to leave.

OK. Senator Klobuchar?

KLOBUCHAR:
Thank you.

Secretary Napolitano, just to shift for one minute here, we have 17 families in Minnesota that are awaiting children. They've been to Haiti. They've seen these kids. And I do appreciate the front line work that you and Secretary Clinton have done, and also your granting of humanitarian parole that I requested last week.

I spent the weekend with some of these families as they clutched these photos. And I promised them I would ask about not their specific situations, but just what is happening in terms of a safe haven, just the details of how these kids are going to get to the United States or get somewhere safe. And Haiti, as they hear reports, the orphanages, you know, don't have enough water, don't have enough food. And just the sooner we can get them over, the better.

NAPOLITANO:
Yes, Senator Klobuchar. We are working very closely to get orphans out who need to get out, who are already qualified for adoption in the United States. And we will work closely with your office.

But let me just pause a moment and say, we have already removed a number of orphans already to the United States, and some more are coming.

That being said -- and our heart goes out to those families, families in other states, and most importantly, the orphans themselves. In a catastrophe the size of Haiti, the number -- we have to now set up a process, beyond the orphans already identified with adoptive parents, before other children are removed, because we are there, really, at the acquiescence of the government of Haiti. They have to agree that this child...

KLOBUCHAR:
I understand.

NAPOLITANO:
... can be removed, and should be, to another country for care.

So, the State Department is working with Haiti on that. Secretary Clinton is on that. We met about this late last night.

The secretary of Health and Human Services is involved, because when a child is brought here from Haiti, normally there's a lot of medical and health attention that needs to be carried out before they can be...

KLOBUCHAR:
I understand.

NAPOLITANO:
... delivered. And so...

KLOBUCHAR:
Just if I could just impress on you that I realize some of this is in the hands of the Haitian government.

I want to say that your staff has been very helpful today. We've been directly talking to them.

NAPOLITANO:
Right.

KLOBUCHAR:
We feel that the adoptions we have are pretty far along in the process. And so, we will continue to get the details. But I just wanted to impress on you, one, to thank you for what you're doing, but, two, how important it is for these families.

I wanted to ask, as I look for solutions to all of this, as a former prosecutor, I know you know this. It's very easy to look at every detail, and you always think later, what could we have done differently. And you can always find when a crime occurs, the changes that need to be made.

But going forward, the full body scanners, would that have prevented this, if he had gone through a full body scanner in Amsterdam or one of the other airports?

NAPOLITANO:
There is no doubt, in my view, that the whole body imaging, particularly in the current iteration of the technologies and the technologies we're now working on with DOE, would be a very clear improvement over any technology that was used in Schiphol on Christmas.

KLOBUCHAR:

OK. And the timetable here were, I think, 450 new ones. We've got 2,100 airport lanes, I think I read, in our country, 2,500 international flights that I'm sure you'll be dealing with tonight coming in. A timetable of getting these out?

NAPOLITANO:
At least 450 domestically this year. We're obviously looking at how to accelerate that, and then working internationally to see that they will employ that kind of technology -- which by itself, by the way -- and I can't emphasize this enough. In and of itself, no one technology, no one process, no one intel agency is the silver bullet here. It's layer, layer, layer, layer.

It's good technology with behavior detection officers, with canines, with explosives detection equipment, with the right watch lists, with the right names on it and the right intel behind it.

So, as you can, even from this hearing, all of these things have a role to play. It's a very layered, and needs to be a layered process.

KLOBUCHAR:
OK. And one last question on the watch list, something that I've been looking at as a member of this committee for a while. It's my feeling that there are people that shouldn't be on it that waste resources -- a kid going to Disneyland in Minnesota who continually got questioned for years from the time he was a baby -- to people who should be on it that aren't.

Just how do we go about this, not only adding people, but clearly I know that's been a lot of the focus of the questions today. But also, looking at secure flight, what's happening with that, what the implementation date is on that. And finally, working with our airlines.

As you know, this was a Northwest Airlines flight, now owned by Delta. Northwest Airlines, originally based in Minnesota. I've talked to their -- Richard Anderson, the CEO, at length. It was their employees and those brave passengers that were on the front line that stopped this from happening. So, they have a big interest in making this work in the future.

And I just encourage you to work with the industry, because in so many international airports there is no TSA. So, the airlines are still on the front line.

NAPOLITANO:
Right. And the private carriers are part of the process, too. In fact, I've already met with them individually, at least the U.S. flag carriers, had several long conversations with President, or CEO Anderson, among others. They are going to be part of this solution. Trust me.

Secure flight, we should be basically implemented domestically by March of this year. There are two airlines that may lag by another 30 to 60 days. But basically, domestically, that's where we are.

AR 001035

Internationally, longer, but we're looking basically at having it implemented, secure flight internationally, by the end of 2010.

KLOBUCHAR:
Thank you very much.

ROCKEFELLER:
Thank you, senator.

Senator LeMieux?

LEMIEUX:
Thank you, Mr. Chairman.

I've not had the opportunity to interact or interface with you folks yet, so I appreciate that opportunity today. And I know, secretary, you have to go, so let me just ask you a quick question before you have to take your leave for Spain.

I think it's the belief of the American people that 99.99 percent of the folks who are going through security in this country pose no threat. And a lot of folks come to me and say, we really feel like we're being harassed when we go through TSA, whether it's the child that's getting patted down or the 85-year-old grandmother who's being patted down.

At the same time, we have these folks like the Christmas Eve, or Christmas Day bomber, who made it through security.

Do we use -- and if this isn't the right setting for it, I understand -- are we using any kind of predictive modeling to follow up on what Senator Lautenberg was talking about, what credit card companies do in their anti-fraud measures? Do we score people?

I mean, we're not just taking data based upon information. I assume that we use the good intelligence of the people who are working in Homeland Security and other agencies to look for potential threats and use computer modeling to say that this person is a threat.

NAPOLITANO:
Senator, we do that. We also employ, as I've said, a number of things in domestic airports such as behavior detection officers. So that is underway, as well.

But we also employ random selection. And random selection is truly random, so that when the 85-year-old grandmother -- there must be an 85-year-old grandmother who has been pulled aside in every state in the union, because I always hear about the 85-year-old grandmother.

LEMIEUX:
There's a lot in Florida.

(LAUGHTER)

NAPOLITANO:
I'm from Arizona. I can appreciate that. But in any event -- but truly random must mean truly random. And it's also random and differentiated between airports. So, we will not have the same process in place in every airport in the United States on any given day.

LEMIEUX:
Well, that makes sense to me. But I hope when you were talking about the travel for international folks in the future, this kind of clear travel concept, I mean, I would hope that in the future, there is a way through biometrics or other ways for the average American to be able to not go through without any type of screening -- that doesn't make any sense -- but for us to focus on the people that we're concerned with the most, and put all of our -- you know, most of our energy towards them. That seems to make more sense to me.

NAPOLITANO:
Senator, if I might, secure flight, to which Senator Klobuchar was just referring, that will help a lot, because that will exchange data that allows us to remove the false positives from the system.

Those sorts of things, as they get implemented -- we're not talking about the needle in the haystack. In a way, it's about the needle among the needles. And it is not the easiest thing to do in advance.

So what we want to be able to do is, yes, get the false positives out of the system, so we can focus where we need to focus. These sorts of things that are underway will help us with that.

LEITER:
And senator, if I might add, and I can't go into depth in an open session, but we do use biometrics for a number of the levels of screening, both the visa process and entry into the country. That is a costly endeavor to integrate that into all of the screening.

It also poses significant policy issues regarding the protections of privacy data and U.S. persons data. So it's an area that I think we'll probably be coming back to committees like this, seeking assistance either in terms of resources or legislation to ensure that we can, in fact, use this biometric data effectively.

LEMIEUX:
And director, you said a moment ago that you are now putting these teams together who will be able to be responsible for trying to see different issues, put the pieces together. You know, I think the American people assume that that's happening now.

You know, I'm new to the Senate, so I think I have fresh eyes to look at this. I think the American people assume that there are rooms of people around this country working for the federal government in any one of these agencies, who are looking at all of this data, analyzing it and making reports and decisions to not let people on planes or come across borders, or get visas.

Is that correct?

LEITER:
Senator, it is, except, at the same time that they were doing that, they also had to write intelligence and sort of analyze these things, and send them up to policymakers.

The purpose of this is to free them from those requirements, so they can focus all of their time with sufficient numbers on these small bits of data, which again, in combination, paint the very damning picture, but when they come in individually surrounded by thousands of other pieces of data, really don't stand up to the analyst.

LEMIEUX:
For both of you, is there one thing that we could do which would -- I know nothing would solve the problem completely. You're never going to be able to ensure safety 100 percent. But is there one thing? Is it this full body scan? Is there one thing that you think, boy, that would really make a large difference in making our country safe?

What's the first thing we should do?

NAPOLITANO:
Senator, I think that one of the first, if not the first things we should do is push out the advanced technology that we know exists, even as we recognize the next generation of technology is still on its way.

LEITER:
Senator, my real answer is, there isn't one thing. There really is not one thing that would make a huge difference here. It is a combination of many little things.

I will say, if I could only have one thing to pick, it would be to ensure that we do get the international cooperation we need, especially with our European partners, of providing the data and doing the screening that we want them to provide and do. That, otherwise, leaves us with a

AR 001038

significant gap, because we can't cover the entire world. We need their assistance to protect the country.

LEMIEUX:
Thank you. Thank you, Mr. Chairman.

ROCKEFELLER:
Thank you, senator.

Senator Ensign, before I call on you, Secretary Napolitano, can you still get to Europe? I wanted to...

NAPOLITANO:
I think Senator Ensign is the last one here who hasn't had a chance to ask a question. I'd be happy to stay.

ENSIGN:
I have one.

NAPOLITANO:
Yes.

ENSIGN:
OK. A quick question that I'm going to ask all of you. You can start. This gets to ideology.

Do you believe that there's an ideology of radical Islam that has anything to do, or that underlies the USS Cole attack, Hasan, the Christmas Day bomber, 9/11? Do you think that this radical Islam that's out there in the world, that that underlies what's going on?

NAPOLITANO:
Senator, there is no doubt that there is a terrorist ideology in this world that is operating both internationally, and some of it now homegrown, that is underlying the attacks we're seeing now...

ENSIGN:
It's associated...

NAPOLITANO:

... some of the ones we've seen in the past.

ENSIGN:
... with radical Islam?

NAPOLITANO:
That is associated -- if you want to call it that, yes.

ENSIGN:
Well, I mean...

NAPOLITANO:
Yes.

ENSIGN:
... it is.

LEITER:
Yes, and I don't think I should have my job if I said anything else.

NAPOLITANO:
Yes, I mean, I think, absolutely.

HAMILTON:
Yes.

ENSIGN:
Thank you. The reason I ask -- the reason I ask that is, there was actually a report out today on the Fort Hood incident. And in the 86 pages -- actually, John Lehman talks about this, a member of the 9/11 Commission, former Navy secretary. I'll quote him.

And he says that there's a -- there's a reluctance. Not a single place in the 86 pages talking about Hasan does it mention any type -- anything to do with radical Islam.

And what he says, and I'll quote him, he says, it shows you how deeply entrenched the values of political correctness have become. It's definitely getting worse, and is now so engrained that people no longer smirk when it happens.

The reason I ask that, we had a hearing in the Homeland Security Committee before the Christmas break about the Fort Hood incident. And this question was asked about political correctness. Is it clouding our judgment? Are we afraid to ask the wrong questions?

This gets back to, not religious profiling, not racial profiling, but terrorist profiling. If there is an ideology that is underlying what is happening here, we'd better recognize that, and we'd better call it what it is.

We certainly didn't back away from Nazism as a political ideology. Well, if radical Islam is what is -- they call for this jihad against the West, against us, against American values, we'd better recognize that.

The reason I say that, even, you know, that every young military officer is required to read "The Art of War." Well, a big part of the art of war is knowing your enemy. Well, this is a big part of the enemy, is their ideology. It's their motivation.

And one of the reasons I ask that is because it seems to me that the Christmas Day bomber, which we know had ties through this cleric to the -- to Hasan and the Fort Hood tragedy that went on, that it would have seemed to me that after the Fort Hood, because that took place, initially, that if the ideology was the thing that was driving it, we would focus a lot of our intel on the ideology, with this guy's disseminating information in some of the people that he's communicating with.

And Director Leiter, you mentioned something about First Amendment rights, and I want to give you the chance to clarify it. Was Abdulmutallab and the cleric, their communications, is that protected by First Amendment rights as far as not getting on a no-fly list, when those conversations happened overseas?

LEITER:
No, senator. And I want to make clear that, prior to 12/25, we weren't -- we didn't intercept any communications between Abdulmutallab and Anwar al-Awlaki, the cleric to which you're referring.

And my only point on the communication was, certainly, people -- you can imagine some conversations people could have which would be First Amendment, and wouldn't justify watch listing but no-fly.

ENSIGN:
I just wanted to make sure that conversations that were having -- if we had intercepted a conversation between the two of them overseas, even if it...

LEITER:

AR 001041

Oh, absolutely...

ENSIGN:
... it would never be -- it would never be protected by First Amendment.

LEITER:
Absolutely not, senator.

ENSIGN:
OK. I just...

LEITER:
And...

ENSIGN:
That's why I wanted to ask, because it was the way that you said it, it could have been -- and I wanted to give you...

LEITER:
I apologize.

ENSIGN:
... I wanted to give you a...

LEITER:
Senator, can I just add? There is no doubt in my mind -- and we have done everything we can at NCTC to make quite clear to the American people and to members of Congress, that undoubtedly, underlying the reign of violence that Al Qaida has brought, it is inspired by a violent, extremist, Islamic ideology. Period.

That does not mean that Islam is violent. It does not mean that Islam is extremist.

ENSIGN:
I agree. No, I don't -- no, I -- listen, I totally agree. That's why I said a radical form of Islam that exists in the world.

AR 001042

LEITER:
As the director of NCTC, I want to be as clear as possible.

ENSIGN:
Yes, I agree with you. I agree with you, and, you know, don't want to see discrimination against people, just because, you know, they follow the Islam faith.

ROCKEFELLER:
Senator Ensign?

ENSIGN:
Yes.

ROCKEFELLER:
Your time is up. It's just barely up. But Senator Cantwell has a question for Secretary Napolitano, who should have left 15 minutes ago, but is being generous. I want to give Senator Cantwell a chance, with your forbearance, to ask her question.

ENSIGN:
Absolutely. Could I have one minute right after she just asks this one quick question? Just because I want to ask each one of them...

ROCKEFELLER:
You've got it.

ENSIGN:
... just a yes-or-no question.

ROCKEFELLER:
You've got it.
Senator Cantwell?

CANTWELL:
Thank you, Mr. Chairman. Do I have five minutes now? Or...

ROCKEFELLER:
Yes.

CANTWELL:
Oh, OK. Thank you. Thank you, Mr. Chairman.

Secretary Napolitano or Director Leiter, did the U.S. counterterror agencies have any specific negative information about Mr. Abdulmutallab prior to his father alerting the U.S. embassy in Nigeria?

NAPOLITANO:
Let me ask Director Leiter. I don't know whether we should answer all of that in open session.

LEITER:
Senator, the -- I would be happy to give you an answer to that in closed session.

CANTWELL:
Great. Hopefully, I'll see you later, and I'll get that.

My understanding is from news reports, that his name was placed on a British version of a watch list. Was that information shared with the U.S. government or any -- you know, if so, which agencies received that information, and when was it received?

LEITER:
It was not as -- I believe it was not shared. And he was denied a visa for non-terrorist reasons. In my conversations with my British colleagues, they had no information involving his association with terrorism prior to the events of 12/25. Or I should say, no information different from what we had.

CANTWELL:
But he was subsequently put on their equivalent watch list there. And so, if you didn't hear from them, isn't there some sort of one-to-one correspondence between the British government and the United States...

LEITER:
Senator, it's my understanding...

CANTWELL:

AR 001044

... watch lists?

LEITER:
Senator, it's my understanding that he was denied a visa. He was not placed on their terrorist watch list.

We do exchange information regarding terrorist watch lists. He was not on that watch list.

CANTWELL:
You do not believe that he -- if an individual was placed on a watch list in Britain, they should be placed -- that would be sufficient grounds to be on a watch list, the TIDE list?

LEITER:
Oh, I think there's very good reason, if an individual is on the British terrorist watch list, that he should also be placed on the American terrorist watch list. He was not on the British terrorist watch list.

CANTWELL:
OK. And secondly, if we had -- Secretary Napolitano, you mentioned cooperation. And I've been very active in the Visa Waiver Program, saying we should have more conditions on that program.

And so, I know that the current State Department Web site says, to be admitted to the Visa Waiver Program, a country must meet various security and other measurements required, such as enhanced law enforcement, security-related data sharing. And members are also required to maintain high counterterrorism, law enforcement, border control and document security standards. So, that's the current level by which those 35 countries have to cooperate with us.

Now, do you think that we need to enhance that? Or do you think that is the power, now, to say to those individuals?

NAPOLITANO:
I think what we need to do is make sure that the standards that have been set forth for visa waiver are enforced on a continuous and continual basis. And like all of the standards that have been referred to throughout this afternoon's session, that we continually refresh them and make sure they match what we need to match, to make sure that terrorists aren't allowed to travel around the globe.

CANTWELL:

AR 001045

So, you think that their (ph) -- I mean, you mentioned going there and having this dialogue. My question is, do we have enough with that State Department language there to require the cooperation on data sharing that we need? Or do we need to do more?

NAPOLITANO:
Right now, using the U.K. as an example, we have very good cooperation on data sharing. Whether there are new or additional types of data, or new or additional types of things that need to be done in this ever-changing environment is something that we continually need to challenge ourselves with.

CANTWELL:
OK. And then, the -- I'm reading a "New York Times" article, which says that, after Mr. Abdulmutallab's application to renew a student visa was rejected. The secretary said the suspect was in place on a watch list.

NAPOLITANO:
I don't know what article you're referring to.

CANTWELL:
I'm referring to the "New York Times," December 29, 2009.

NAPOLITANO:
You're going to have to help me out. I don't know what the context -- if you can help me, please.

CANTWELL:
It's about Britain's rejected visa renewal for the suspect, and the fact that he was on a -- so, maybe we can find out what watch list he was on in the U.K., and whether that information could have been shared with the United States, or should have been shared with the United States.

My question today was more about the policy ramifications. And if it wasn't, why shouldn't it be? Why shouldn't somebody on Britain's list be shared with this?

And I guess my overall concern, having been a member of the Judiciary Committee in 2002, when we had a great discussion with the FBI after 9/11, and a lot of the questions and (ph) data sharing information about why FBI agents in Arizona didn't share information with FBI agents in Minnesota, that the question is, how far have we come in eight years on this data-gathering, analytical analysis?

AR 001046

I mean, we're spending billions of dollars in Iraq and Afghanistan. We should not be at a hearing today, saying we don't have enough analysts, or that we don't know about cloud computing, and that information across various databases can't be shared, that just because you misspelled somebody's name, information can't come up.

All those are technology solutions that are in the market today. And so, that shouldn't be our barrier to this issue.

And so, I hope that we will realize that the war on terrorism is an asymmetrical threat. And that asymmetrical threat means we have to be a very flat organization with sharing information. And that needs to be very robust.

So, I hope we can resolve this question about the British watch list and whether that information will be shared.

LEITER:
And senator, if I may, I full agree with your underlying point about sharing with the British. In fact, I know Secretary Napolitano and I have both engaged with our British colleagues since to review those very issues, to ensure that this information is being shared fully, especially because we see so many links back through the U.K., through so many of our plots.

CANTWELL:
Thank you, Mr. Chairman.

ROCKEFELLER:
Thank you, Senator Cantwell.

Secretary Napolitano, I'm sort of embarrassed, because you need to go, and I don't know whether you're being polite.

NAPOLITANO:
I think Senator Ensign wanted to have one more question, and then I'm going to ask permission to please to leave.

ROCKEFELLER:
Permission is granted. I mean, you know...

NAPOLITANO:
Yes.

AR 001047

ROCKEFELLER:
OK. So, Senator Ensign?

ENSIGN:
Thank you.

You mentioned before about when Abdulmutallab came into this country, it's a different policy whether or not he's allowed into the country versus getting on an airplane. This is a question going forward. Is that policy going to be changed?

In other words, it doesn't make any sense to me that somebody has to go through a secondary screening to get into the country, but they didn't have to go through a secondary screening to get on an airplane.

NAPOLITANO:
Well, it's the difference between secondary screened, if there's information about being a threat to aviation versus secondary screening, because they may have had some other criminal indicator or some other bad behavior, or what have you. So, and it's the difference between those two things.

But to your question, this isn't about labels. It's not about which list or what list. It's looking at the entirety of the problem and saying, all right. Now, this guy was able -- this individual was able -- to get on a plane. He was able to get on a plane bound for the United States, and get on a plane bound for the United States with PETN. That should not happen. What actions do we need to take to make sure that doesn't happen again?

And that's how we're looking at it, not...

ENSIGN:
Right. The only reason...

NAPOLITANO:
I can go into all the complexities and whatever.

ENSIGN:
The only reason I bring that up...

NAPOLITANO:
It doesn't really...

AR 001048

ENSIGN:
He probably wasn't suspected of some other kind of criminal activity. The reason he was going through secondary screening -- it would be my guess -- the reason he was going through secondary screening in Detroit before he got into the country, after he got off the airplane -- that type of a list you would think should keep him from getting on the airplane in the first place.

In other words...

NAPOLITANO:
Indeed. And we have...

ENSIGN:
And that's what I'm saying. I'm suggesting to you that you look at that as a policy change.

NAPOLITANO:
Indeed. And, senator, we have already made that change. If you are in a State Department database, and those words are associated with a name, we are now already pushing that forward in the international environment.

I have a feeling that there will be other changes made as part of this review, as well.

ENSIGN:
Good. Thank you for your indulgence, Mr. Chairman.

Thank you for staying, very, very much. And I have other questions for the panel that I'll submit for the record.

ROCKEFELLER:
Thank you, Senator Ensign.

I might say to all members, and this isn't the end of the hearing -- thank you very much, Madam Secretary -- that there's a seven-day period to submit any further questions.

(UNKNOWN)
(OFF-MIKE)

ROCKEFELLER:

Oh, absolutely. But I just wanted to make that plain now.

And so, Frank, you'd be up.

LAUTENBERG:
Yes, if I might, Mr. Chairman.

ROCKEFELLER:
I mean, Senator Lautenberg.

LAUTENBERG:
I'd ask of -- since Governor Kean -- I called you Lee. I can't call you Mr. Hamilton. Lee, I have a question that I'd like your view on.

Security cameras seem to be an important -- not seem, are an important part -- of the surveillance that's required to keep people from getting access to secure areas. And I wonder whether you might know, or if anyone knows, whether all airports have security checks.

Mr. Leiter, would you know that?

LEITER:
Senator, I apologize. I simply don't know if every...

LAUTENBERG:
OK.

Lee, would you recommend that every airport that has commercial traffic have security cameras at critical access points?

HAMILTON:
Yes, I think I would. But security cameras raise a lot of questions about privacy. And how you do that, how you set those security cameras up, and who sees the images, makes a lot of difference. I think you have to be very alert to that.

So, I favor security cameras. I think they can be very careful. But their use can certainly be abused.

LAUTENBERG:
Yes. I'm just talking about with security checkpoints.

HAMILTON:
Right.

LAUTENBERG:
So, you agree that...

HAMILTON:
Yes.

LAUTENBERG:
... it's a valuable tool, and we should have them.

Thanks, Mr. Chairman. You've been very indulgent, and I appreciate it.

Thanks to both of you for your endurance, as well as your answers.

ROCKEFELLER:
Well, they're not finished yet.

LAUTENBERG:
Oh, I'm sorry. I didn't mean to preempt exit.

ROCKEFELLER:
Senator LeMieux, is there any question you had?

LEMIEUX:
Just a couple of questions.

Director Leiter, after Abdulmutallab was taken off the plane, at some point, he was Mirandized. Do you agree that he should be Mirandized and treated in that fashion?

LEITER:
Senator, this is really a question that I have to defer to the Department of Justice. Although trained as a lawyer, exactly who, when...

LEMIEUX:
You're more than trained as a lawyer. I think you were the president of the Harvard Law Review and a clerk for a Supreme Court justice. And you're about as accomplished as a lawyer as there is. So...

LEITER:
I'm starting to feel like maybe I should go back to that line of work, senator.

(LAUGHTER)

But in all honesty, ultimately, the decision of when that should be done or has to be done, clearly has to be within the ambit of the Department of Justice and the FBI.

I think what is equally clear is the utility of having interagency discussions prior to that, to inform that decision. So, again, the decision has to be one of the attorney general, but that should be a decision informed by an interagency discussion considering all of the nation's national security priorities -- homeland security, intelligence collection, and the like.

LEMIEUX:
And you're, you know, you're the head of counterterrorism for the country. You're an advocate for trying to stop this terrorism before it starts. And certainly, I would think, in your role, you would want to make sure that someone like Abdulmutallab would be interviewed, and you could receive as much information as possible to help you prevent another attack.

LEITER:
Yes.

LEMIEUX:
And when someone is given their Miranda rights, that the chance that they are going to give that information seems to be less likely.

LEITER:
Senator, as a good lawyer and a former prosecutor, my answer is, it really is fact-specific. And I simply don't have sufficient understanding of the facts on the ground as to when it was or was not appropriate to Mirandize him.

I do think, again, that decision has to be informed by an interagency discussion. And I can tell you from having been a prosecutor, there's no shortage of times when you Mirandize someone and they keep talking.

AR 001052

LEMIEUX:
Sure. But he's not an American citizen. He is a person who is fighting a war against our country, trying to blow up a plane over Detroit. He has none of the rights of an American citizen.

Why does he get afforded the right of Miranda rights? Why should he?

LEITER:
Senator, I really have to defer to the Department of Justice on their decision there. I simply have a different set of interests at that point.

I do have a different set of interests, but that doesn't make the interests of the Department of Justice any less valid. I just want to make...

LEMIEUX:
And I don't ask you to speak for them. But in your role as the head of counterterrorism for the country, wouldn't you prefer that he be treated as an enemy combatant, and that he be -- have the opportunity to be interrogated, so that you could learn information and prevent future attacks?

LEITER:
As the director of NCTC, I absolutely have an interest in ensuring that intelligence is collected, so it can be analyzed and put into action.

I also do have an interest, although not the same interest as the Department of Justice, where it's, I think, even more overriding, of ensuring that basic laws, constitutional principles are followed. I'm not suggesting either one of these paths would not have honored that.

But I do actually have an enormous interest, as the director of NCTC, to make sure that there is a level of trust with the Congress and the American people, that any counterterrorism investigation is being pursued in a lawful, reasonable manner.

LEMIEUX:
Thank you.

Congressman Hamilton, it seems to me that we still don't know who's in charge of protecting the homeland. Obviously, the president of the United States is ultimately responsible. But we have an attorney general, we have a director of intelligence, we have the head of the CIA, we have the head of the FBI, we have Director Leiter.

I mean, do we still need some kind of structural change in the United States government, so that one person is responsible and reports to the president as the ultimate person who is here to protect the country?

HAMILTON:
Yes.

You have the Intelligence Reform and Terrorism Prevention Act. And it has been very clear from the testimony here today, that there is, at the very least, a good bit of ambiguity in that statute as to who has authority.

That statute was very hard to pass. And it is not going to be amended quickly or soon, so you're going to be living with it. And you're going to be -- for a while. I don't know how long. And during that time, the ambiguities are still going to be there.

So, the only person that can make it clear, who has the authority to do what, is the president of the United States. And I believe that he has to make it very clear, who has the authority within the intelligence community.

Now, I think it was the intent of the Congress to put that authority in the Director of National Intelligence. But if you read that statute, it is not crystal clear. So, I think there is a heavy burden, given the fact that you're operating under an ambiguous statute, that the president must say, who has the authority on budget, on personnel, on coordination, on integration in the intelligence community. And I don't know who else can do it.

When you have ambiguity in a statute, it is an invitation to the bureaucracy to struggle, to fight, to protect their turf. And only the president can clear the deck.

LEMIEUX:
Thank you, congressman.

LEITER:
May I add briefly? And I associate myself with all of the very honorable Lee Hamilton's comments. I think he's exactly right.

But I would add an additional layer of complexity here, because the issue to which he was speaking was really coordination of the intelligence community. And that intelligence community is just one bit of the larger national security, counterterrorism effort, which obviously extends to DHS, the attorney general, as you cited, the secretary of defense, the secretary of state.

So, to the extent that it might be a bridge too far right now to even significantly modify the Intelligence Reform and Terrorism Prevention Act with respect to the DNI's authorities and NCTC's authorities, I would simply add that an even broader reform, I think, starts to be a bridge much, much too far.

LEMIEUX:
I guess the challenge that we have is that at some point, somebody has to be accountable. And when you know that you're the person in charge -- and you've both had this experience -- then you institute a different level of action and follow-up than if there is a collective group.

And if one person knows that they're responsible for keeping the homeland safe -- whether it's the secretary, or it would be the attorney general, or it would some other person, director of national intelligence -- the system is going to work differently. Right now it seems like it's collegial. And it didn't work.

And we should be acting -- and I know that you are -- as if the plane blew up.

LEITER:
Senator, I agree fully with what you just said. I think the president did make clear that the buck stops with him, ultimately. That's -- but also, in his tasking to the director of NCTC, he made clear to give me the responsibility to ensure a system of follow-up on high -- prioritizing and follow-up of high priority threats.

Now, consistent with the statutory language that created NCTC, I do not have the authority, nor am I seeking it, to direct the actions to follow up. But at least we will establish a system whereby each of these threats, when we identify threats, can, in fact, be followed up through appropriate department or agency action. And the results of that follow-up is reported back to the National Security Council to ensure that they have the information they need to further direct action as necessary.

LEMIEUX:
Thank you. Thank you, Mr. Chairman.

ROCKEFELLER:
Thank you, senator.

Let me just actually ask one quick question, and then turn to Lee Hamilton for thought.

Always the first question that the press asks is, so, who's going to get fired? Who's going to get fired? In other words, there's got to be somebody who's accountable. Can't fire the president. And so, it's like -- it's the all-consuming answer to our problems. If somebody's fired, it means there's somebody that Farouk would have never gotten on an airplane, et cetera.

I don't -- I think the question of firing at a high level, if it places itself squarely in front of somebody, because there's been a clear case of negligence, has to come before the president of the United States.

To make an absurd comparison, but the only one that I can think of right now, when I was governor of West Virginia, the state still controlled liquor, had liquor stores. West Virginia has had its share of governors who have done time in prison, and things of this sort. This particular one didn't.

However, our director of liquor took a vacation trip to Wyoming with a bunch of liquor lobbyists. Now, he's not a high person in government. He was, you know, in the Cabinet, so to speak. But liquor and beer don't really make the first cut.

I called him up in Wyoming, and I fired him on the spot. And I never questioned my own honesty.

But you always have to worry about not just the people who are at the top, but the people who are down somewhere in the middle, who are making decisions, who are looking at -- who are looking at some of the cable traffic and the interpretation, who are the analysts, or whatever. And you get into this business of people who have been there for 20 or 25 years.

And I always compare it to HHS. You come in and you do Medicare. And you come into the office every morning, somewhere out in Baltimore, and there are stacks -- a big stack of paper here, a big stack paper here, a big stack of paper here. And the question is, you just go from the top down. You come back the next day, you do it. And after a number of years, you just wear out, and you start to miss stuff.

And my question to you, Director Leiter, is, is that on the minds -- I mean, if you've got hundreds of thousands -- and I think the number actually goes a lot higher than that -- pieces of information coming in every day, you are overwhelmed with hearings, with pressure, with the terrifying nature of the modern world. And all of a sudden we're discussing Somalia and Djibouti and Yemen and Kenya, and they're not even in the Middle East. I don't think Yemen qualifies as that. That's Horn of Africa.

So, that doesn't -- that's not Iran. That's not Iraq. That's not Afghanistan.

So, there's an overwhelming obsession of the duties of the day, the responsibilities, what can get up to you.

I do think it's important that people in your position are able to look down, have a mechanism for being able to look down and find out who has gotten tired, who doesn't really want to come to work, in an area where the nation's citizens are at risk. And those folks, if there are some of them who are removed quietly -- I would say, without a lot of public attention -- it will be understood throughout the entire intelligence community within 48 hours, maybe worldwide.

I think that's important. And I think what Senator LeMieux and what a lot of us, you know, we keep saying, somebody's accountable. Therefore, if it's not working, somebody ought to get fired. And sometimes things don't rise to that easy an answer. Because if you fire somebody who's way up here -- and maybe that person should be fired, and that's up to the president -- but then you've sort of taken -- you've sort of taken the pressure off of everybody else.

AR 001056

And where a lot of the main work is going on is four or five levels down, but it's the crucial work. It's the crucial work. It's the selection of which piece of information took precedence over what, and they should be placed in this group or this group, or whatever.

Is this something which -- are you aware of this? I mean, I know you're aware of it. I've just talked about it, and you've been around a long time.

But I think that kind of thing is important.

LEITER:

Senator, absolutely. And I hope -- and I think he has. I think the president has had the same thoughts about his leadership, wondering if we've just been looking at paper and not moving it as quickly. And I expect that he can ask that question. He should ask that question about me as the director of NCTC, to decide if that's the case with me.

But in terms of the workforce, it is certainly something we think about. And I'll tell you that I say something to every new class of people that come to NCTC. And I know you've come out and met many of our analysts, and you know most of them are 26, 27, 28. And I can tell you that the reaction to the events of Christmas Day has just been heartbreaking to many of them -- frankly, heartbreaking to me.

I mean, we know that we should have done better. And it is traumatic, and we obviously dodged a bullet, and very lucky that something more tragic did not occur. And it has caused soul-searching for many of us, myself included.

But at every introduction to the new class of people coming to NCTC as they rotate through from different agencies, I tell them that, at the entrance to our auditorium, there's a display that we put up on our fifth anniversary just a month or two ago, which has the remnants of a flag that was recovered from the World Trade Center site, a piece of the Pentagon and remnants of the steel, twisted steel from the World Trade Center.

And I tell every one of them in those classes, the day that you can no longer walk into this building and look at that display and say, I'm going to do everything I can to protect innocent people from getting killed by terrorists, is the day that you have to turn in your badge and go find something else to do.

And I think that this event will cause some people to have those thoughts, because the pace is so strenuous, the burnout is so high, the pressure is so high. But my belief is, we fundamentally have the right set of people, that they've been walking in every day, they've been seeing that display, and they've been working as hard as humanly possible, and in as cooperative a spirit as possible, to make sure events like Christmas Day don't happen again.

ROCKEFELLER:

AR 001057

And I understand that, and I agree with it. You've left the judgment up to the individuals. And I'm saying, sometimes the judgment has to come from...

LEITER:
Absolutely, Mr. Chairman. And to be clear...

HAMILTON:
Mr. Chairman, let me just add that I'm certainly for accountability in government. And if a person clearly did not do their job, they ought to pay a penalty for that. The immediate problem is to correct the flaws that happened.

This threat is ongoing. They're plotting right now how to get at us. And the urgent task, a prior task to accountability, is to correct the flaws that have been discussed here. That's the priority from my point of view. Accountability, obviously important, but correcting the flaws, more important.

ROCKEFELLER:
Congressman...

HAMILTON:
And incidentally, if I may go back a few years in history, the Hart-Rudman Commission, we made the observation that hiring and firing is a national security issue. I think it was back then, I think it is today.

One of the really great weaknesses of our system is that managers, like Director Leiter, do not have the power to hire and to fire.

ROCKEFELLER:
Well, that's pretty well put. And that goes on the agenda.

Congressman, do you have, in closing, any thoughts that have occurred to you? I know you haven't been around very much and don't have much experience, but...

HAMILTON:
Well, I've learned a lot this afternoon in listening to Director Leiter and Secretary Napolitano. And I've very much appreciated the opportunity to be with you. The questions, I might say, from your senators have really been excellent and on the mark.

The only further comment I would make -- and this has come up in the hearing, but not enough emphasis from my standpoint -- the fundamental problem -- and I think Director Leiter

would agree with me here -- is the analytical function. And if you want to make sure this thing doesn't happen again, many things perhaps have to happen.

But by all odds, it seems to me the most important thing that has to happen is, you have to strengthen this analytical capacity. When you're talking about connecting the dots, that's what you're really talking about.

We have the most remarkable collection ability in producing all of this information that any government or any entity could possibly have. But analysis needs much, much more emphasis. You've got to have better trained analysis. You've got to have more analysts and more of them. And that would be one of my impressions from this hearing.

The second impression is that the analysts have to have the ability to follow up, to pursue a lead and to demand action against a potential threat.

LEMIEUX:
Mr. Chairman?

ROCKEFELLER:
Yes?

LEMIEUX:
(OFF-MIKE)

(LAUGHTER)

Is that better? Sorry. I broke the microphone.

You know, we have the finest computing people in the world in this country, whether it's Google or other countries -- or other companies. I know folks in Florida who do unbelievable spinning of trillions of pieces of data for the private sector. And I hope that you feel like you've got the freedom to reach out to the smartest minds in America to help you. Because I know that they would.

And I don't mean necessarily giving someone a contract. That's one thing, and maybe you need to do that. But just go out to these people, and have them come in and help you, because, you know, what Senator Cantwell was talking about with cloud computing, and all the things that we've done, I assume you have this.

But whatever else you need, you should go get.

LEITER:

AR 001059

Senator, we absolutely have. We have over several years reached out to the private sector or the national labs. We are doing so vigorously -- again, now, in response to this. And if you have particular companies or people that you think would be particularly useful, I am more than happy to speak with you and make sure we get those folks inside and see what our challenges are.

LEMIEUX:
Thank you, Mr. Chairman.

ROCKEFELLER:
Thank you. And thank you all, the departed and the present. Thanks for your patience.

Thanks for you in the audience who have suffered, been through grief. Thanks for those of you who have just simply come here to listen and to learn, and to act out your citizenship.

This hearing is adjourned.

CQ Transcriptions, Jan. 20, 2010

List of Panel Members and Witnesses

PANEL MEMBERS:
SEN. JOHN D. ROCKEFELLER IV, D-W.VA. CHAIRMAN

SEN. DANIEL K. INOUYE, D-HAWAII

SEN. JOHN KERRY, D-MASS.

SEN. BYRON L. DORGAN, D-N.D.

SEN. BARBARA BOXER, D-CALIF.

SEN. BILL NELSON, D-FLA.

SEN. MARIA CANTWELL, D-WASH.

SEN. FRANK R. LAUTENBERG, D-N.J.

SEN. MARK PRYOR, D-ARK.

SEN. CLAIRE MCCASKILL, D-MO.

SEN. AMY KLOBUCHAR, D-MINN.

SEN. TOM UDALL, D-N.M.

SEN. MARK WARNER, D-VA.

SEN. MARK BEGICH, D-ALASKA

SEN. KAY BAILEY HUTCHISON, R-TEXAS RANKING MEMBER

SEN. OLYMPIA J. SNOWE, R-MAINE

SEN. JOHN ENSIGN, R-NEV.

SEN. JIM DEMINT, R-S.C.

SEN. DAVID VITTER, R-LA.

SEN. JOHN THUNE, R-S.D.

SEN. ROGER WICKER, R-MISS.

SEN. JOHNNY ISAKSON, R-GA.

SEN. SAM BROWNBACK, R-KAN.

SEN. MIKE JOHANNS, R-NEB.

SEN. GEORGE LEMIEUX, R-FLA.

WITNESSES:
SECRETARY OF HOMELAND SECURITY JANET NAPOLITANO

MICHAEL LEITER, DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEE HAMILTON, CO-CHAIR, NATIONAL SECURITY PREPAREDNESS GROUP, BIPARTISAN POLICY CENTER

TOM KEAN, CO-CHAIR, NATIONAL SECURITY PREPAREDNESS GROUP, BIPARTISAN POLICY CENTER

Source: CQ Transcriptions

All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of CQ Transcriptions. You may not alter or remove any trademark, copyright or other notice from copies of the content.

© 2010 Congressional Quarterly Inc. All Rights Reserved.

Statement of Janet A. Napolitano
Secretary

U.S. Department of Homeland Security

before

United States Senate
Committee on Homeland Security and Governmental Affairs

on

Intelligence Reform: The Lessons and Implications of the Christmas Day Attack

Wednesday, January 20, 2010

340 Dirksen Senate Office Building
Washington DC

Chairman Lieberman, Senator Collins, and members of the Committee: Thank you for this opportunity to testify on the attempted terrorist attack on Northwest Flight 253.

The attempted attack on December 25 was a powerful illustration that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. This Administration is determined to thwart those plans and disrupt, dismantle and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just DHS, but many other federal agencies and the international community as well.

As our part in this effort, DHS is a consumer of the U.S. Government's consolidated terrorist watchlist, which we use to help keep potential terrorists off flights within, over or bound for the United States and to identify travelers that require additional screening. We work with foreign governments, Interpol, and air carriers to strengthen global air travel security by advising them on security measures and on which passengers may prove a threat. We also work with air carriers and airport authorities to perform physical screening at TSA checkpoints and to provide security measures in flight.

Immediately following the December 25 attack, DHS took swift action at airports across the country and around the world. These steps included enhancing screening for individuals flying to the United States; increasing the presence of law enforcement and explosives detection canine teams at air ports, and of air marshals in flight; and directing the FAA to notify the 128 flights already inbound from Europe about the situation. Nonetheless, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with the explosive

PETN on his person. As President Obama has made clear, this Administration is determined to find and fix the vulnerabilities in our systems that allowed this breach to occur.

Agencies across the federal government have worked quickly to address what went wrong in the Abdulmutallab case. The effort to solve these problems is well underway, with cooperation among DHS, the Department of State, the Department of Justice, the Intelligence Community, and our international allies, among others. As a consumer of terrorist watchlist information, the Department of Homeland Security welcomes the opportunity to contribute to the dialogue on improving the federal government's ability to connect and assimilate intelligence. We are also focused on improving aviation screening and expanding our international partnerships to guard against a similar type of attack occurring again. To those ends, today I want to describe the role that DHS currently performs in aviation security, how DHS responded in the immediate aftermath of the attempted Christmas Day attack, and how we are moving forward to further bolster aviation security.

DHS' Role in Multiple Layers of Defense

Since 9/11, the U.S. government has employed multiple layers of defense across several departments to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities, while other countries and the private sector – especially the air carriers themselves – also have important roles to play.

DHS oversees several programs to prevent individuals with terrorist ties from boarding flights that are headed to, within, or traveling over the United States or, in appropriate cases, to identify them for additional screening. Specifically, DHS uses information held in the Terrorist Screening Database (TSDB), a resource managed by the Terrorist Screening Center (TSC), as

well as other information provided through the Intelligence Community to screen individuals; operates the travel authorization program for people who are traveling to the United States under the Visa Waiver Program (VWP)[1]; and works with foreign governments, international and regional organizations, and airlines to design and implement improved security standards worldwide. This includes routine checks against Interpol databases on wanted persons and lost or stolen passports on all international travelers arriving in the United States. The Department also performs checkpoint screenings at airports in the United States.

To provide a sense of the scale of our operations, every day, U.S. Customs and Border Protection (CBP) processes 1.2 million travelers seeking to enter the United States by land, air or sea; the Transportation Security Administration (TSA) screens 1.8 million travelers at domestic airports; and DHS receives advanced passenger information from carriers operating in 245 international airports that are the last point of departure for flights to the United States, accounting for about 1,600 to 1,800 flights per day. Ensuring that DHS employees and all relevant federal officials are armed with intelligence and information is critical to the success of these efforts.

Safeguards for Visas and Travel

One of the first layers of defense in securing air travel consists of safeguards to prevent dangerous people from obtaining visas, travel authorizations and boarding passes. To apply for entry to the United States prior to boarding flights bound for the U.S. or arriving at a U.S. port of

[1] The 35 countries in the Visa Waiver Program are: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, and the United Kingdom (for the U.K., only citizens with an unrestricted right of permanent abode in the U.K. are eligible for VWP travel authorizations).

entry, most foreign nationals need visas – issued by a U.S. embassy or consulate – or, if traveling under a Visa Waiver Program country, travel authorizations issued through the Electronic System for Travel Authorization (ESTA) .[2]

Issuing visas is the responsibility of the Department of State. At embassies and consulates where it is operational, the Visa Security Program positions personnel of U.S. Immigration and Customs Enforcement (ICE) to assist State Department personnel in identifying visa applicants who may present a security threat. For individuals traveling under the VWP, DHS operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. These systems examine an individual's information to assess whether he or she could pose a risk to the United States or its citizens, including possible links to terrorism. Without presenting a valid authorization to travel to the United States at the airport of departure, a foreign national is not able to board a U.S.-bound flight.

The Department also works with other federal agencies and our foreign partners to try to prevent possible terrorists from obtaining boarding passes. These include the application of the No-Fly List and the implementation of Secure Flight program, which I explain below.

Pre-departure screening

As another layer of defense, DHS conducts pre-departure passenger screening in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. DHS uses TSDB data, managed by the Terrorist Screening Center that is administered by the FBI, to determine who may board, who requires

[2] Exceptions would be citizens of countries under other visa waiver authority such as the Western Hemisphere Travel Initiative or the separate visa waiver program for Guam and the Commonwealth of the Northern Mariana Islands, or those granted individual waivers of the visa requirement under the immigration laws.

further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

Specifically, to help make these determinations, DHS uses the No-Fly List and the Selectee List, two important subsets within the TSDB. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, over, or within the United States. Individuals on the Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

Through the Secure Flight Program, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List, and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, DHS began to transfer this responsibility to TSA in 2009, and the transition is targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination.

As an additional layer of security, DHS also uses the Passenger Name Record (PNR), the Advanced Passenger Information System (APIS), and the Immigration Advisory Program (IAP) to assess a passenger's level of risk and, when necessary, flag them for further inspection. PNR data, obtained from the airline reservations systems, contains various elements, which may include optional information on itinerary, co-travelers, changes to the reservation, and payment information. PNR data is evaluated against "targeting rules" that are based on law enforcement data, intelligence and past case experience. APIS data, which carriers are required to provide to

DHS at least 30 minutes before a flight, contains important identifying information that may not be included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. DHS screens APIS information on international flights to or from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations. APIS is also connected to Interpol's lost and stolen passport database for routine queries on all inbound international travelers.

Another layer in the screening process is the Immigration Advisory Program (IAP). The CBP officers stationed overseas under the IAP program at nine airports in seven countries receive referrals from CBP screening against the TSDB, of which the No Fly list is a subset. IAP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

Checkpoint screenings and in-flight security

The third layer of defense for air travel in which DHS plays a role is the screening of passengers and their baggage. TSA screens passengers and baggage at airports in the United States, but not in other countries. When a traveler at a foreign airport is physically screened, that screening is conducted by the foreign government, air carriers, or the respective airport authority.

Domestically, TSA employs a layered approach to security, which includes measures both seen and unseen by travelers. The 48,000 Transportation Security Officers at hundreds of airports across the country screen passengers and their baggage using advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines,

vapor trace machines that detect liquid explosives, Advanced Imaging Technology, full-body pat-downs, explosives detection systems, Bomb Appraisal Officers, and Behavior Detection Officers – both at the checkpoint and throughout the airport. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security throughout the airport perimeter and in limited access areas of airports. The $1 billion in Recovery Act funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

In an effort to enhance international screening standards, TSA conducts security assessments in accordance with security standards established by the International Civil Aviation Organization (ICAO) at more than 300 foreign airports, which include foreign airports from which flights operate directly to the United States and all airports from which U.S. air carriers operate. If an airport does not meet these standards, TSA works with the host government to rectify the deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. In long-term circumstances of non-compliance with international standards, TSA may recommend suspension of flight service from these airports to the United States. In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level. If an airport is located within one of the 35 VWP countries, DHS conducts additional audits and inspections as part of the statutorily mandated VWP designation and review process.

In terms of in-flight security, Federal Air Marshals (FAM) are deployed on high-risk domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more volunteer pilots serve as armed, deputized Federal Flight Deck Officers. Additionally, armed law enforcement officers from federal, state, local, and tribal law enforcement agencies that have a need to fly armed provide a force multiplier on many flights.

DHS Response to the Christmas Day Attack

The facts of the Christmas Day attempted bombing are well established and were relayed in the report on the incident that the President released on January 7, 2010. On December 16, 2009, Umar Farouk Abdulmutallab, a Nigerian national, purchased a round-trip ticket from Lagos, Nigeria to Detroit. Abdulmutallab went through physical security screening conducted by foreign airport personnel at Murtala Muhammed International Airport in Lagos on December 24 prior to boarding a flight to Amsterdam Airport Schiphol. This physical screening included an x-ray of his carry-on luggage and his passing through a walk-through metal detector. Abdulmutallab went through additional physical screening, conducted by Dutch authorities, when transiting through Amsterdam to Northwest Flight 253 to Detroit, and presented a valid U.S. visa. Abdulmutallab was not on the No Fly or Selectee Lists. Accordingly, the carrier was not alerted to prevent him from boarding the flight or additional physical screening, nor did the IAP officer advise Dutch authorities of any concerns. As with all passengers traveling on that flight, and similar to all other international flights arriving in the United States, CBP evaluated Abdulmutallab's information while the flight was en route to conduct a preliminary assessment of his admissibility and to determine whether there were requirements for additional inspection.

During this assessment, CBP noted that there was a record that had been received from the Department of State, which indicated possible extremist ties. It did not indicate that he had been found to be a threat, or that his visa had been revoked. CBP officers in Detroit were prepared to meet Abdulmutallab upon his arrival for further interview and inspection. The attack on board the flight failed in no small part due to the brave actions of the crew and passengers aboard the plane.

Immediate DHS response

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. TSA directed the Federal Aviation Administration to apprise 128 U.S.-bound international flights from Europe of the attempted attack and to ask them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosive detection canine teams, state and local law enforcement, expanded presence of Behavior Detection Officers, and enhanced screening. That evening, DHS issued a security directive for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

From the first hours following the attempted attack, I worked closely with the President, Assistant to the President for Homeland Security and Counterterrorism John Brennan, senior Department leadership, and agencies across the federal government. I communicated with international partners, members of Congress, state and local leadership and the aviation industry and met with national security experts on counterterrorism and aviation security. The results of

these communications culminated in two reports to the President: one on New Year's Eve and the second on January 2, 2010.

One of our most important conclusions was that it is now clearer than ever that air travel security is an international responsibility. Indeed, passengers from 17 countries were aboard Flight 253. Accordingly, DHS has embarked upon an aggressive international program designed to raise international standards for airports and air safety. On January 3, 2010, I dispatched Deputy Secretary Jane Holl Lute and Assistant Secretary for Policy David Heyman to Africa, Asia, Europe, the Middle East, Australia, and South America to meet with international leadership on aviation security. In these meetings, they reviewed security procedures and technology being used to screen passengers on U.S.-bound flights and worked on ways to bolster our collective tactics for defeating terrorists. This afternoon, I am traveling to Spain to meet with my European Union counterparts in the first of a series of global meetings intended to bring about broad consensus on new, stronger, and more consistent international aviation security standards and procedures.

In addition to these efforts, the Department has been in close contact with Congress, our international partners, the aviation industry and state and local officials across the country since the afternoon of the attempted attack. On December 25, the Department issued a joint bulletin with the FBI to state and local law enforcement throughout the nation; conducted calls with major airlines and the Air Transport Association; distributed the FBI-DHS joint bulletin to all Homeland Security Advisors, regional fusion center directors and Major City Homeland Security Points of Contact in the country; and notified foreign air carriers with flights to and from the United States of the additional security requirements. DHS has maintained close contact with all of these partners since the attempted attack, and will continue to do so.

On January 3, TSA issued a new Security Directive, effective on January 4, which includes long-term, sustainable security measures developed in consultation with law enforcement officials and our domestic and international partners. Because effective aviation security must begin beyond our borders, this Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism[3] or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners.

Steps Forward to Improve Aviation Security

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. On January 7, I joined Assistant to the President for Counterterrorism and Homeland Security John Brennan to announce five recommendations DHS made to the President as a result of the security reviews ordered by President Obama. At the President's direction, DHS will pursue these five objectives to enhance the protection of air travel from acts of terrorism.

First, DHS will work with our interagency partners to re-evaluate and modify the criteria and process used to create terrorist watchlist, including adjusting the process by which names are added to the No-Fly and Selectee Lists. The Department's ability to prevent terrorists from boarding flights to the United States depends upon these lists and the criteria used to create them.

[3] The State Department currently lists Cuba, Iran, Sudan, and Syria as state sponsors of terrorism.

As an entity that is primarily a consumer of this intelligence and the operator of programs that rely on these lists, the Department will work closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watchlist system.

Second, DHS will establish a partnership on aviation security with the Department of Energy and its National Laboratories in order to use their expertise to bolster our security. This new partnership will work to develop new and more effective technologies that deter and disrupt known threats, as well as anticipate and protect against new ways that terrorists could seek to board an aircraft with dangerous materials.

Third, DHS will accelerate deployment of Advanced Imaging Technology to provide capabilities to identify materials such as those used in the attempted December 25 attack, and we will encourage foreign aviation security authorities to do the same. TSA currently has 40 machines deployed at nineteen airports throughout the United States, and plans to deploy at least 450 additional units in 2010. DHS will also seek to increase our assets in the area of explosives-trained canines, explosives detection equipment, and other security personnel.

Fourth, DHS will strengthen the presence and capacity of aviation law enforcement. As an interim measure, we will deploy law enforcement officers from across DHS to serve as Federal Air Marshals to increase security aboard U.S.-flag carriers' international flights. At the same time, we will maintain the current tempo of operations to support high-risk domestic flights, as we look to longer-term solutions to enhance the training and workforce of the Federal Air Marshal Service.

Fifth, as mentioned earlier, DHS will work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in

foreign airports and the commitments of our foreign partners to enhance security – not just for Americans, but also for their nationals traveling to this country.

In all of these action areas to bolster aviation security, we are moving forward with a dedication to safeguard the privacy and rights of travelers.

Conclusion

The attempted attack on Christmas Day serves as a stark reminder that terrorists motivated by violent extremist beliefs are determined to attack the United States. President Obama has made clear that we will be unrelenting in using every element of our national power in our efforts around the world to disrupt, dismantle, and defeat al-Qaeda and other violent extremists.

While we address the circumstances behind this specific incident, we must also recognize the evolving threats posed by terrorists, and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities in all sectors. President Obama has clearly communicated the urgency of this task, and the American people rightfully expect swift action. DHS and our federal partners are moving quickly to provide just that.

I wish I could close by giving you a 100 percent guarantee that no terrorist, ever, will try to take down a plane or attack us in some other fashion. I cannot give you such a guarantee; that is not the nature of the world we live in, nor of the threats that we face. What I can give you, however, is the 100 percent commitment of myself, DHS leadership, and the entire DHS enterprise to do everything we can to minimize the risk of terrorist attacks.

Chairman Lieberman, Senator Collins, and members of the Committee: Thank you for this opportunity to testify. I can now answer your questions.

Homeland Security

Press Briefing by Secretary Napolitano on Aviation Security

Release Date: January 26, 2010

For Immediate Release
Office of the Press Secretary
Contact 202-282-8010

Transcript

Moderator: Good afternoon. Thank you all for joining us. Secretary Napolitano is going to make some remarks, and then we will take some questions. I will moderate and call on the questioners. And we have about 25 minutes or so. So, fire away.

Secretary Napolitano: Thank you. Good afternoon. It has been just over a year since I became the Secretary of Homeland Security. And today I want to briefly discuss some of the Department's key security priorities for the upcoming year.

Let me pause a moment to stress that this is not an exhaustive list. We continue to have ongoing priorities involving

cyber, WMD, and emergency response, among others. Yet the attempted attack on the 25th of December was a powerful illustration that terrorists will stop at nothing to kill Americans, and that counterterrorism remains our top priority. This Administration is determined to thwart those plans, to disrupt, dismantle, and defeat terrorist networks through multiple layers of defense, all working in concert with one another.

Now, our Department, despite its name, is not solely responsible for this effort. The fight against terrorism is a broad-based one, involving all instruments of national power: diplomatic, military, intelligence, and law enforcement. And in that fight, the Department of Homeland Security's role is very clear: protect air travelers, prevent illegal entry, enforce our immigration laws, and utilize local law enforcement as a force multiplier by sharing intelligence and information with them.

And so, in 2010, the Department of Homeland Security will pursue an ambitious agenda in each of those 4 areas. First, aviation security. We will strengthen aviation security by deploying new technology, law enforcement, and canine assets at domestic airports, and we will embark on an unprecedented international initiative to raise global aviation security.

Now, let me spend a minute discussing this international initiative, because while the Department of Homeland Security does not screen passengers at overseas airports, we must ultimately assume responsibility for the security of flights entering the United States. Last week I was in Toledo, Spain and Geneva, Switzerland, to move this agenda forward. I met with foreign ministers, international aviation officials, and representatives from some of the world's largest airlines, to talk about how we can collectively strengthen aviation security.

In Spain, I met with foreign counterparts from across Europe, at the invitation of my Spanish colleague, interior minister Alfredo Rubalcaba. It was a rare invitation for a United States official to join these EU working ministerial meetings. And there were four broad areas of discussion: information sharing, passenger vetting, technology, international standards. And, indeed, I was very gratified to see that there exists a broad consensus in working on these four areas among my European counterparts, and a clear sense of urgency to take immediate action to strengthen security measures and identify areas for further progress.

As evidence of this, we signed a joint declaration affirming the commitment to advance initiatives on these and other areas. The gathering in Spain was the first in what will be a series of regional meetings around the globe facilitated by the International Civil Aviation Organization, ICAO, the United Nations body that supervises global aviation standards.

Last week I was also pleased to find a similarly strong consensus in Geneva, where I met with representatives from more than 20 airlines that are part of the International Air Transport Association, and with officials from ICAO. The private sector's role in aviation security cannot be overstated. I stressed the importance of working to improve international security standards, and heard a strong response and a commitment to work toward common approaches to aviation security.

I believe we have an important opportunity right now, right in front of us, to strengthen a system that has, for half a century, served as an extraordinary engine for progress and prosperity in the United States, and for countries around the world. But that system has its weak links, and we must address them without delay.

Beyond aviation security, the Department of Homeland Security also has responsibility for the security of our land and our sea ports. Indeed, just because the target of attack was in the air, we cannot afford to take our eye off other targets, which is why, in 2010, we are going to build on the unprecedented effort we exerted in 2009 to deploy resources on the southwestern border, and strengthen security along the northern border. We will continue that effort by bolstering security at our land and seaports through enhancing law enforcement, infrastructure, and technology to ensure that all points along our interconnected border security network remain strong.

Additionally, we will be working to improve information sharing with our federal, state, tribal, and territorial law enforcement partners through a robust network of fusion centers and joint terrorism task forces. Our goal is giving that front line law enforcement the tools they need to confront and to disrupt terrorist threats.

And finally, we will be working with the congress to address changes we can make to our nation's immigration laws, because we will never have fully effective national security so long as millions of people remain in the shadows in our country.

Look for announcements of each of these four areas in the weeks ahead. So, with that outline, I would be happy to take questions.

Moderator: Tom (ph)?

Question: Sure. Madame Secretary, on the issues on aviation, the previous administration was trying to do a lot of things

that you just talked about. Are your efforts any different from what the previous administration was doing, (inaudible) continuation of those efforts, particularly with regard to information sharing and passenger vetting?

Secretary Napolitano: What we see now is that whereas we were continuing at the bilateral level to do some of the information sharing and passenger vetting agreements -- the API/PNR agreements that you're familiar with -- what I saw now is a consensus among, for example, the countries of Europe that this needs to be done. And, indeed, the discussion was not just about data sharing with the United States, but within the EU itself.

So that one of the differences is urgency, and international recognition that the terrorists are going to look for any gap they can find in the system. And they are very strategic about it. And they will go, in an international system, to where they think a gap exists to try to get someone like an Umar Farouk with an explosive like PETN on a plane. That system, our system, should never have allowed that to happen. Now we need to use this as an opportunity, as a catalyst, as it were, for international action.

Question: If I could just follow up, what you're basically saying is security is as good as its weakest link. And when you talk about technology, which is one of the issues, you're talking about 100 countries that have non-stop flights to the U.S. (inaudible)?

Secretary Napolitano: Mm-hmm.

Question: (Inaudible) money or the wherewithal to (inaudible) technology?

Secretary Napolitano: Mm-hmm.

Question: What role will the U.S. play in improving technology in countries that might need financial assistance?

Secretary Napolitano: Indeed. And there was a -- there is a frank recognition that some countries lack the resources or the capacity in this area. And so, that's why ICAO and the involvement with the United Nations is so important. That's why I said information sharing, passenger vetting, technology, international standards, they all go together. And there needs to be a discussion involving all of the nations of the world about how you support and make sure that all international airports meet at least some basic level, and maintains some basic level. That is one of the major points of this international initiative.

Moderator: Pete (ph)?

Question: Madame Secretary, you mentioned in your opening remarks weapons of mass destruction. Today, a mission appointed by the congress said that the government still doesn't get it when it comes to weapons of mass destruction, particularly biological hazards, that little progress has been made, and that the threat is actually getting worse. Is that a fair criticism?

Secretary Napolitano: I haven't read the report, so I can't respond to it directly. What I can say is that the Administration has -- had major initiatives on detection in the bio area, on diagnosis in the bio area, on medical countermeasures that can be taken in the bio area, on response and recovery in the bio area, and that we will continue to be working on that issue, as well. That's why I mentioned it in my opening paragraph.

Question: Apart from the report, then, how big a priority is it for the government to be able to counter the biological threat?

Secretary Napolitano: It is a big priority. And we know that it is one of the things that terrorists could use in the future, or indeed, even now. It runs across the federal government, across the administration. Major measures have been taken in the past 11 months, 10 months, as I described. But, obviously, this is an area that we are going to continue to work on. The goal is to keep the American people safe.

Question: I just wanted to check. The four things that you said came out of these meetings seem to have been things that were on -- have been on the table, or should have been on the table for -- you know, since September 11. And yet we're talking about things like a clear sense of urgency. You know, why did it take so long to get people to the table to sign a declaration that they're going to affirm a commitment to this sort of thing?

And if it hasn't taken us this long, if we have already done that, then what's new about this? I guess what is new about this, and why has it taken this long to get there?

Secretary Napolitano: Well, one of the things that is new is the international consensus that has been reached, that this –

Question: There was not an international –

Secretary Napolitano: Not in this -- not at the level we are talking about, no. You would have to ask perhaps internationally. But again, what we have now is -- and are building -- an international consensus. There is a sense of urgency. We are moving forward. And the United States will play a major role.

But I must emphasize that this is the community of nations. And the recognition by these nations that there were passengers from 17-plus countries on Flight 253, all of whom would have perished if Abdul Mutallab had been successful –

Question: Do you have any sense of why this failed thing gave a sense of urgency to the international community when September 11th didn't give a sense of urgency?

Secretary Napolitano: Well, September 11th obviously gave a sense of urgency. But that sense of urgency perhaps dissipated over time, and has been now not only renewed but also added to. The September 11th attack was a large-scale conspiracy involving the take-over of airplanes, and flying them as weapons into buildings. The kind of attack that Umar Farouk Abdul Mutallab was -- embarked upon was a single individual who was able to get on a plane with PETN packed around his body. That's a very different kind of thing from a detection, information-sharing, passenger vetting type of environment. And so that's why it is necessary to use December 25th as the catalyst, and say, "Nations of the world, we all have an interest in this."

The international aviation system is international in every respect. It is only as strong as its weakest link. We need to get together this year, right now, and move to get the agreements that have been discussed for years, discussed by my predecessors, get them done, get them implemented, get technology moving in the right direction, and move to increase capacity at international airports across the world.

Moderator: Mark (ph)?

Question: It seems to me, from what we know of the Christmas Day attack, the weakest link in the process that we know about was the passenger screening (inaudible). And in the case of this guy, he could have been screened in two different ways. He could have been screened physically (inaudible). He also could have been screened, you know, in a questioning way, based on the information which was discovered when the plane was -- had taken off and was in the air, that there was a hit in the system about his father having come and complained (inaudible).

What are you doing specifically to try and improve, number one, the physical screening at these foreign airports, like Amsterdam, immediately, in the short term, and what are you doing to push that information that you have in the system -- in this particular case, (inaudible) the people at the airport so they can use it for screening the guy before he gets on the plane, not after he gets on.

Secretary Napolitano: Indeed. A couple of things. As you know, we don't do screening at international airports, just as we don't, you know, prepare the no-fly list. We receive the no-fly list. Yet there are things that are happening right now. Number one is, given this new international sense of urgency, governments around the world -- including the government in Amsterdam -- have already moved on the technology front. They are moving to add whole-body images, for example, explosives detection equipment, more canine teams, more personnel, greater screening within the airport environment itself.

You will see that when you go to Amsterdam, you will see that when you go to Heathrow, you will see that when you go to the Charles de Gaulle in Paris, you will see that in Frankfurt, in Germany. So international countries, based on what we have seen and what they discerned happened on Christmas Day, already are moving on the technology front.

The advantage, or the thing that we are going to be doing, is all now moving on the -- what is the next iteration of technology? What can we do to make -- improve the likelihood that you pick up a potential bomber like Umar Farouk, but at a minimum of invasiveness and inconvenience to the traveling public? What's the next iteration? How do we do that?

And so, that's why we have inked a memorandum of understanding with the Department of Energy. They have, in turn, gotten the national labs in the United States involved on this very issue. What is the next iteration of screening technology for the United States?

Now, with respect to the information sharing, part two of your question, one of the things we have done is taken a particular part of the State Department's database -- I think it's P3B (ph) data -- which is where, if that had been available in Amsterdam rather than in Detroit, Umar Farouk Abdul Mutallab would have been pulled aside for secondary questioning, or we would have recommended to the Dutch that they pull him aside for secondary questioning. Again,

since we don't control the airport -- but we would have recommended that that happen.

So, we have now pushed that particular kind of information out internationally, so it, like the no-fly list and the terrorist screening database, is available before somebody boards an airplane, not while they're in flight.

Question: So you're making that into the -- you're putting that into the hands of the foreign governments, or (inaudible) --

Secretary Napolitano: In Amsterdam we actually have some U.S. officials who located there. They will get it. They, in turn, will give it to the Dutch.

Moderator: Mike (ph)?

Question: Madame Secretary, State of the Union is tomorrow. Just wondering if you or the Department have had any input on that. And, if so, (inaudible)?

Secretary Napolitano: I don't think it appropriate to talk about what the President is going to talk about tomorrow night.

Question: But did you guys offer any input into it?

Secretary Napolitano: Again, we're always offering input on lots of things.

Question: Ma'am, thanks for being with us. You did some talk shows right after this happened, and you were asked if this was an al-Qaeda plot, and you said it's too early to say whether or not it was or not. I believe it was the next day the President came out and called Abdul Mutallab an isolated extremist. A few days after that, the President came out again. It became clear that he was not an isolated extremist, he was an al-Qaeda (inaudible) operative.

My question is, how did the U.S. Government get it so wrong, in terms of who this guy was, and who sent him here to kill Americans or other people who were on that plane to Detroit? How did we get it so wrong? And did that affect the posture, literally, in terms of defending the country, if people were assuming for several days there after this attempted attack, that he was not with a terrorist group, in spite of the sophistication of the bomb, he was just one guy, an isolated extremist? Did that change the defensive posture of this country? But again, how did we get it so wrong, that he wasn't with an al-Qaeda franchise?

Secretary Napolitano: Well, I think in answer to the first part of the question, I don't know that it was that so much as making sure that the right information was given to the public about who this fellow really was, and who he was associated with. It had absolutely no impact on our response. We immediately, while flights were in the air, notified pilots to alert their flight crews what to watch out for. We immediate alerted international partners and airlines around the world to increase their screening of potential passengers. We immediately increased security at domestic airports within the United States. And that was all happening, some of that within 60, 90, 120 minutes of the actual attack. So –

Question: So you did assume that there could be 10 more guys, 20 more guys, 50 more –

Secretary Napolitano: Right.

Question: -- Abdul Mutallabs. But yet, there was this assumption, though, that he was not -- he was an isolated extremist. That's what the President said. How did -- why did that get out there? I know you don't speak for the President, but as his Homeland Security director, how did that -- how did he get that wrong?

Secretary Napolitano: James (ph), I'm going to say there was no -- operationally, which is where the Department lives, we assume the worst until we know that it's not the worst. And we assumed that we needed to immediately provide information across the globe, both to carriers themselves, to domestic airports, and to international airports and international law enforcement. We practice this, because of that kind of an operational assumption. We carried out an assumption that there was an attempted terrorist attack on a plane, and then moved accordingly.

Moderator: Mike (inaudible).

Question: You talked about how there is this renewed sense of urgency in the international community. I was wondering about domestically. It seems, if I recall, during one of your first speeches you barely mentioned the word "terrorism." You talked about the need for immigration reform and other things, but you barely mentioned terrorism. And it seems to be the theme of your event today. Is there also a renewed sense of urgency within your own Department?

Secretary Napolitano: We have always had terrorism as our top priority. I think the attack of December 25 is something that instills in all of us the recognition that al-Qaeda and its adherents, and some of the spin-off groups, literally will stop

at nothing to kill Americans.

And while we do not want to be a nation that lives in fear -- and that's why we want to supply as much information to the public as we can, and we want to make sure that we are resilient, because there are no guarantees in this world that somebody won't succeed, right -- but nonetheless, I think that we are -- we were created in the wake of 9/11, and our priorities are now shaped around the counter-terrorism activity we must undergo in aviation, but also in other areas that are within this Department: the land, the seaports, immigration, and looking at the security issues involving immigration if we don't get immigration reform. So, that's what we are going to do.

Question: Very quickly –

Secretary Napolitano: Sure.

Question: The Olympics are just around the corner. I don't know what the terror picture is. I was hoping you could tell us a little bit about the terror picture surrounding the Olympics.

Secretary Napolitano: Right. We have been working with the Canadians all year long on the security for the Olympics. We have a joint command center up near the border. We also have taken other measures. And we will be working very closely with them. Obviously, they are the lead. It's -- they are the host nation. But we are providing a lot of support to them.

Question: As far as people attending the Olympics, is there any special concern beyond the normal concerns?

Secretary Napolitano: No.

Moderator: We just have time for one last question.

Question: A couple of things. On the aviation side, you mentioned that there is this new sense of urgency, and you have these agreements that you're working with. But I noticed that some of the agreements mentioned, of course, that any security can't violate the laws of the nations. And there are various privacy laws in many of these nations, and this has been a problem in the past.

Are you going to truly be able to get the information you need on the passengers that are coming here, given the laws that exist in the EU and other places?

Secretary Napolitano: The discussions we had in Europe were not only getting information, but standardizing the kind of information that we get so it's the most useful in identifying, ahead of time, passengers and giving us greater ability to run passenger lists against the terrorist watch lists, the no-fly lists, and the like.

We understand that in Europe there are privacy laws that are different than those in the United States. But they have a joint interest in the security of their citizenry, as well. And we believe that we can reach these agreements and get this information and share it, but also do it in a way that deals with their privacy issues, as with the U.S. I mean, our privacy office has been involved in these from the beginning.

And we have been on the cusp so many times already with several nations. Again, I don't know that there is a new sense of urgency, but a renewed sense of urgency that we are talking about in the international realm. It's aviation security, it's the security of our land and our seaports of entry. It's information sharing so that state and local law enforcement can serve as a force multiplier across our country. These are the kinds of initiatives that this Department can employ to keep the American public safe. And that's what we are focused upon.

Moderator: Thanks, everybody.

Question: Just really quickly, are we pressing to get that information, that passenger information, more quickly, sooner?

Secretary Napolitano: Yes. In some countries the answer is yes. Thank you all.

###

This page was last reviewed/modified on January 26, 2010.

I Want To

- Learn about the Travelers' Redress Process

- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

GAO

United States Government Accountability Office

Statement for the Record
To the Committee on Homeland Security,
House of Representatives

For Release on Delivery
Expected on Wednesday,
January 27, 2010

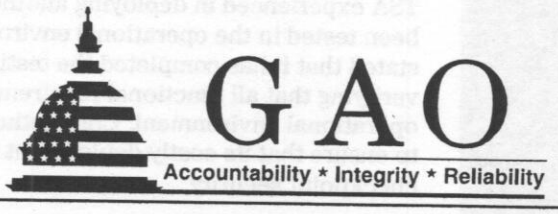
HOMELAND SECURITY

Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security

Statement for the Record by Eileen R. Larence
Director, Homeland Security and Justice Issues

and

Stephen M. Lord
Director, Homeland Security and Justice Issues



GAO-10-401T

AR 001085

January 27, 2010

HOMELAND SECURITY

Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Checkpoint Technologies Could Further Strengthen Security

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-10-401T, a statement for the record to the Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The December 25, 2009, attempted bombing of flight 253 raised questions about the federal government's ability to protect the homeland and secure the commercial aviation system. This statement focuses on the government's efforts to use the terrorist watchlist to screen individuals and determine if they pose a threat, and how failures in this process contributed to the December 25 attempted attack. This statement also addresses the Transportation Security Administration's (TSA) planned deployment of technologies for enhanced explosive detection and the challenges associated with this deployment. GAO's comments are based on products issued from September 2006 through October 2009 and selected updates in January 2010. For these updates, GAO reviewed government reports related to the December 25 attempted attack and obtained information from the Department of Homeland Security (DHS) and TSA on use of the watchlist and new technologies for screening airline passengers.

What GAO Recommends

GAO is not making new recommendations, but has made recommendations in prior reports to DHS, the Federal Bureau of Investigation (FBI), and the White House Homeland Security Council to enhance the use of the watchlist and to TSA related to checkpoint technologies. The agencies generally agreed and are making some progress, but full implementation is needed.

View GAO-10-401T or key components. For more information, contact Eileen Larence at (202) 512-6510 or larencee@gao.gov and Stephen Lord at (202) 512-4379 or lords@gao.gov.

What GAO Found

The intelligence community uses standards of reasonableness to evaluate individuals for nomination to the consolidated terrorist watchlist. In making these determinations, agencies are to consider information from all available sources. However, for the December 25 subject, the intelligence community did not effectively complete these steps and link available information to the subject before the incident. Therefore, agencies did not nominate the individual to the watchlist or any of the subset lists used during agency screening, such as the "No Fly" list. Weighing and responding to the potential impacts that changes to the nomination criteria would have on the traveling public will be an important consideration in determining what changes may be needed. Also, screening agencies stated that they do not check against all records in the watchlist, partly because screening against certain records may not be needed to support a respective agency's mission or may not be possible because of the requirements of computer programs used to check individuals against watchlist records. In October 2007, GAO reported that not checking against all records may pose a security risk and recommended that DHS and the FBI assess potential vulnerabilities, but they have not completed these assessments. TSA is implementing an advanced airline passenger prescreening program—known as Secure Flight—that could potentially result in the federal government checking passengers against the entire watchlist under certain security conditions. Further, the government lacks an up-to-date strategy and implementation plan—supported by a clearly defined leadership or governance structure—which are needed to enhance the effectiveness of terrorist-related screening and ensure accountability. In the 2007 report, GAO recommended that the Homeland Security Council ensure that a governance structure exists that has the requisite authority over the watchlist process. The council did not comment on this recommendation.

As GAO reported in October 2009, since TSA's creation, 10 passenger screening technologies have been in various phases of research, development, procurement, and deployment, including the Advanced Imaging Technology (AIT)—formerly known as the Whole Body Imager. TSA expects to have installed almost 200 AITs in airports by the end of calendar year 2010 and plans to install a total of 878 units by the end of fiscal year 2014. In October 2009, GAO reported that TSA had not yet conducted an assessment of the technology's vulnerabilities to determine the extent to which a terrorist could employ tactics that would evade detection by the AIT. Thus, it is unclear whether the AIT or other technologies would have detected the weapon used in the December 25 attempted attack. GAO's report also noted the problems TSA experienced in deploying another checkpoint technology that had not been tested in the operational environment. Since GAO's October report, TSA stated that it has completed the testing as of the end of 2009. We are currently verifying that all functional requirements of the AIT were tested in an operational environment. Completing these steps should better position TSA to ensure that its costly deployment of AIT machines will enhance passenger checkpoint security.

AR 001086

Mr. Chairman and Members of the Committee:

We are pleased to submit this statement on the progress federal agencies have made and the challenges they face in key areas of terrorism information sharing and the deployment of checkpoint technologies. The December 25, 2009, attempted bombing of flight 253 has led to increased scrutiny of how the government creates and uses the consolidated terrorist screening database (the watchlist) to screen individuals and determine if they pose a security threat, and highlighted the importance of detecting improvised explosive devices and other prohibited items on passengers before they board a commercial aircraft. The White House's initial review of these events exposed gaps in how intelligence agencies collected, shared, and analyzed terrorism-related information to determine if the subject—Umar Farouk Abdulmutallab—posed enough of a threat to warrant placing him on the watchlist, which could have altered the course of events that day. To enhance its ability to detect explosive devices and other prohibited items on passengers, the Transportation Security Administration (TSA) is evaluating the use of Advanced Imaging Technology (AIT)—formerly called the Whole Body Imager—as an improvement over current screening capabilities.

In October 2007, we released a report on the results of our review—conducted at your request—of how the watchlist is created and maintained, and how federal, state, and local security partners use the list to screen individuals for potential threats to the homeland.[1] As a result of that review, we identified potential vulnerabilities, including ones created because agencies were not screening against all records in the watchlist. We made a number of recommendations aimed at addressing these potential vulnerabilities and helping to enhance the effectiveness of the watchlist process, which the agencies have not yet fully addressed. These recommendations—which we discuss later in this statement—are still important to address and can inform ongoing reviews of the December 25 attempted terrorist attack.

Also, in January 2005, we designated information sharing for homeland security a high-risk area because the government faced formidable challenges in analyzing and disseminating this information in a timely,

[1]GAO, *Terrorist Watchlist Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*, GAO-08-110 (Washington, D.C.: Oct. 11, 2007).

accurate, and useful manner.[2] Since then, we have been monitoring and making recommendations to improve the government's efforts to share terrorism-related information, not only among federal agencies but also with their state, local, tribal, and private sector security partners.[3] Addressing this high-risk area is important to help remove barriers that lead to agencies maintaining information in stove-piped systems, and to hold them accountable to the Congress and the public for ensuring terrorism information is shared, is used, and makes a difference. We are continuing to review federal agencies' efforts to share terrorism-related information and expect to report the results of this work later this year.[4]

In addition, in October 2009, we released a report on TSA's efforts to deploy checkpoint technologies and the challenges the agency faces in these efforts.[5] We made eight recommendations related to the research, development, and deployment of these technologies. The Department of Homeland Security (DHS) agreed with our recommendations and identified actions planned or under way to implement them. While DHS is taking steps to address our recommendations related to conducting risk assessments, the actions DHS reported that TSA had taken or plans to take do not fully address the intent of the majority of our recommendations.

This statement for the record discusses (1) the government's efforts to use the terrorist watchlist to screen individuals and determine if they pose a threat, as well as how aspects of this process contributed to the December 25 attempted terrorist attack and (2) TSA's planned deployment of the AIT

[2]See GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009), for our most recent update.

[3]See, for example, GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006); *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492 (Washington, D.C.: June 25, 2008); and *Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed*, GAO-10-41 (Washington, D.C.: Dec. 18, 2009).

[4]We have three ongoing reviews of terrorism-related information sharing that are being conducted based on separate requests from your committee, the House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Governmental Affairs.

[5]GAO, *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face* Challenges, GAO-10-128 (Washington, D.C.: Oct. 7, 2009).

for enhanced explosive detection and the challenges associated with this deployment.

This statement is based on products GAO issued from September 2006 through October 2009.[6] In conducting our prior work, we reviewed documentation obtained from and interviewed officials at the various departments and agencies with responsibilities for compiling and using watchlist records. We also reviewed documentation and obtained information on current checkpoint screening technologies being researched, developed, and deployed. Our previously published reports contain additional details on the scope and methodology for those reviews. In addition, this statement contains selected updates conducted in December 2009 and January 2010. For the updates, GAO reviewed government reports and other information related to the December 25 attempted attack, obtained information from DHS and TSA on the use of watchlist records and new technologies for screening airline passengers, and interviewed a senior TSA official. We conducted our updated work in December 2009 and January 2010 in accordance with generally accepted government auditing standards.

In Summary

Because the subject of the December 25 attempted terrorist attack was not nominated for inclusion on the government's consolidated terrorist screening database, federal agencies responsible for screening activities missed several opportunities to identify him and possibly take action. We have previously reported on a number of issues related to the compilation and use of watchlist records, such as the potential security risk posed by not checking against all records on the watchlist. We also identified the need for an up-to-date strategy and implementation plan—one that describes the scope, governance, outcomes, milestones, and metrics, among other things—for managing the watchlist process across the federal government. Such a strategy and plan, supported by a clearly defined leadership or governance structure, can be helpful in removing cultural, technological, and other barriers—such as those problems that the December 25 attempted terrorist attack exposed—that inhibit the effective use of watchlist information.

[6]See GAO, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, GAO-06-1031 (Washington, D.C.: Sept. 29, 2006); GAO-08-110; *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*, GAO-09-292 (Washington, D.C.: May 13, 2009); and GAO-10-128.

With regard to the deployment of technology to detect explosives on passengers, TSA expects to have installed almost 200 AITs in airports by the end of calendar year 2010, and plans to procure and install a total of 878 units by the end of fiscal year 2014. While recently providing GAO with updated information to our October 2009 report, TSA stated that operational testing for the AIT was completed as of the end of calendar year 2009. We are in the process of verifying that TSA tested all of the AIT functional requirements in an operational environment. Moreover, we previously reported that TSA had not yet conducted an assessment of the technology's vulnerabilities to determine the extent to which a terrorist could employ tactics that would evade detection by the AIT. While we recognize that the AIT could provide an enhanced detection capability, completing these steps should better position TSA to have the information necessary to ensure that moving ahead with a costly deployment of AIT machines will enhance passenger checkpoint security.

Background

Terrorist Watchlist Process

The Terrorist Screening Center (TSC)—administered by the Federal Bureau of Investigation (FBI)—is responsible for maintaining the U.S. government's consolidated watchlist and providing it to federal agencies as well as state, local, and selected foreign partners for their use in screening individuals. TSC receives the vast majority of its watchlist nominations and information from the National Counterterrorism Center (NCTC), which compiles information on known or suspected international terrorists from executive branch departments and agencies.[7] In addition, the FBI provides TSC with information on known or suspected domestic terrorists who operate primarily within the United States. To support agency screening processes, TSC first determines if each nomination contains specific minimum derogatory information for inclusion in its terrorist screening database. TSC then sends applicable records from the terrorist watchlist to screening agency systems for use in efforts to deter or detect the movements of known or suspected terrorists. For instance, applicable TSC records are provided to TSA for use in prescreening airline

[7]By law, NCTC, which is within the Office of the Director of National Intelligence, serves as the primary organization in the U.S. government for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except for intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. See 50 U.S.C. § 404o(d)(1).

passengers; to a U.S. Customs and Border Protection (CBP) system for use in screening travelers entering the United States; to a Department of State system for use in screening visa applicants; and to an FBI system for use by state and local law enforcement agencies pursuant to arrests, detentions, and other criminal justice purposes.[8]

Airline Passenger Screening Using Checkpoint Screening 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.[9] 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.[10] Secondary screening involves additional means for screening passengers, such as by hand-wand; physical pat-down; or, at certain airport locations, an explosives trace portal (ETP), which is used to detect traces of explosives on passengers by using puffs of air to dislodge particles from their bodies and clothing into an analyzer. Selectees' carry-on items are also physically searched or screened for explosives, such as by using explosives trace detection machines.

[8]See GAO-08-110 for additional details on the compilation and use of terrorist watchlist records.

[9]Sterile areas are generally located within the terminal where passengers are provided access to boarding aircraft, and access is controlled in accordance with TSA requirements.

[10]A nonselectee passenger who alarms the walk-through metal detector on the first pass is offered a second pass. If the passenger declines the second pass, the passenger must proceed to additional screening. If the nonselectee passenger accepts the second pass and the machine does not alarm, the passenger may generally proceed without further screening.

Assessing Potential Vulnerabilities Related to Not Screening against All Watchlist Records and Ensuring Clear Lines of Authority over the Watchlist Process Would Provide for Its More Effective Use

Agencies Rely upon Standards of Reasonableness in Assessing Individuals for Nomination to TSC's Watchlist, but Did Not Connect Available Information on Mr. Abdulmutallab to Determine Whether a Reasonable Suspicion Existed

Federal agencies—particularly NCTC and the FBI—submit to TSC nominations of individuals to be included on the consolidated watchlist. For example, NCTC receives terrorist-related information from executive branch departments and agencies, such as the Department of State, the Central Intelligence Agency, and the FBI, and catalogs this information in its Terrorist Identities Datamart Environment database, commonly known as the TIDE database. This database serves as the U.S. government's central classified database with information on known or suspected international terrorists. According to NCTC, agencies submit watchlist nomination reports to the center, but are not required to specify individual screening systems that they believe should receive the watchlist record, such as the No Fly list of individuals who are to be denied boarding an aircraft.[11] NCTC is to presume that agency nominations are valid unless it has other information in its possession to rebut that position.

To decide if a person poses enough of a threat to be placed on the watchlist, agencies are to follow Homeland Security Presidential Directive (HSPD) 6, which states that the watchlist is to contain information about individuals "known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to

[11]As discussed later in this statement, agencies generally do not use the full terrorist watchlist to screen individuals. Rather, they generally use subsets of the full list based on each agency's mission and other factors.

terrorism."[12] HSPD-24 definitively established the "reasonable suspicion" standard for watchlisting by providing that agencies are to make available to other agencies all biometric information associated with "persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security."[13] NCTC is to consider information from all available sources and databases to determine if there is a reasonable suspicion of links to terrorism that warrants a nomination, which can involve some level of subjectivity. The guidance on determining reasonable suspicion, which TSC most recently updated in February 2009, contains specific examples of the types of terrorism-related conduct that may make an individual appropriate for inclusion on the watchlist.

The White House's review of the December 25 attempted terrorist attack noted that Mr. Abdulmutallab's father met with U.S. Embassy officers in Abuja, Nigeria, to discuss his concerns that his son may have come under the influence of unidentified extremists and had planned to travel to Yemen.[14] However, according to NCTC, the information in the State Department's nomination report did not meet the criteria for watchlisting in TSC's consolidated terrorist screening database per the government's established and approved nomination standards. NCTC also noted that the State Department cable nominating Mr. Abdulmutallab had no indication that the father was the source of the information. According to the White House review of the December 25 attempted attack, the U.S. government had sufficient information to have uncovered and potentially disrupted the attack—including by placing Mr. Abdulmutallab on the No Fly list—but analysts within the intelligence community failed to connect the dots that could have identified and warned of the specific threat.

After receiving the results of the White House's review of the December 25 attempted attack, the President called for members of the intelligence community to undertake a number of corrective actions—such as clarifying intelligence agency roles, responsibilities, and accountabilities to document, share, and analyze all sources of intelligence and threat

[12]The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, D.C., Sept. 16, 2003).

[13]The White House, *Homeland Security Presidential Directive/HSPD-24, Subject: Biometrics for Identification and Screening to Enhance National Security* (Washington, D.C., June 5, 2008).

[14]The White House, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack* (Washington, D.C., Jan. 7, 2010).

threads related to terrorism, and accelerating information technology enhancements that will help with information correlation and analysis. The House Committee on Oversight and Government Reform has asked us, among other things, to assess government efforts to revise the watchlist process, including actions taken related to the December 25 attempted attack.

As part of our monitoring of high-risk issues, we also have ongoing work—at the request of the Senate Committee on Homeland Security and Governmental Affairs—that is assessing agency efforts to create the Information Sharing Environment, which is intended to break down barriers to sharing terrorism-related information, especially across federal agencies.[15] Our work is designed to help ensure that federal agencies have a road map that defines roles, responsibilities, actions, and time frames for removing barriers, as well as a system to hold agencies accountable to the Congress and the public for making progress on these efforts. Among other things, this road map can be helpful in removing cultural, technological, and other barriers that lead to agencies maintaining information in stove-piped systems so that it is not easily accessible, similar to those problems that the December 25 attempted attack exposed. We expect to issue the results of this work later this year.

By Not Placing Mr. Abdulmutallab on the Consolidated Watchlist or Its Subsets, the Government Missed Opportunities to Use These Counterterrorism Tools

Following the December 25 attempted terrorist attack, questions were raised as to what could have happened if Mr. Abdulmutallab had been on TSC's consolidated terrorist screening database. We created several scenarios to help explain how the watchlist process is intended to work and what opportunities agencies could have had to identify him if he was on the watchlist. For example, according to TSC, if a record from the terrorist screening database is sent to the State Department's system and the individual in that record holds a valid visa, TSC would compare the identifying information in the watchlist record against identifying information in the visa and forward positive matches to the State Department for possible visa revocation. If an individual's visa is revoked,

[15]The Intelligence Reform and Terrorism Prevention Act of 2004, as amended, defines the Information Sharing Environment as "an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out [section 1016]." See Pub. L. No. 108-458, § 1016(a)(2), 118 Stat. 3638, 3665 (codified as amended at 6 U.S.C. § 485(a)(3)). See also Homeland Security Act of 2002, 6 U.S.C. § 482 (requiring the establishment of procedures for the sharing of homeland security information, as defined by this section).

under existing procedures, this information is to be entered into the database CBP uses to screen airline passengers prior to their boarding, which we describe below. According to CBP, when the individual checks in for a flight, the on-site CBP Immigration Advisory Program officers already would have been apprised of the visa revocation by CBP and they would have checked the person's travel documents to verify that the individual was a match to the visa revocation record. Once the positive match was established, the officers would have recommended that he not be allowed to board the flight.

Under another scenario, if an individual is on TSC's terrorist screening database, existing processes provide CBP with the opportunity to identify the subject of a watchlist record as part of the checks CBP is to conduct to see if airline passengers are eligible to be admitted into the country. Specifically, for international flights departing to or from the United States (but not for domestic flights), CBP is to receive information on passengers obtained, for example, when their travel document is swiped. CBP is to check this passenger information against a number of databases to see if there are any persons who have immigration violations, criminal histories, or any other reason for being denied entry to the country, in accordance with the agency's mission. According to CBP, when it identifies a U.S. bound passenger who is on the watchlist, it coordinates with other federal agencies to evaluate the totality of available information to see what action is appropriate. In foreign airports where there is a CBP Immigration Advisory Program presence, the information on a watchlisted subject is forwarded by CBP to program officers onsite. The officers would then intercept the subject prior to boarding the aircraft and confirm that the individual is watchlisted, and when appropriate based on the derogatory information, request that the passenger be denied boarding.

In a third scenario, if an individual is on the watchlist and is also placed on the No Fly or Selectee list, when the person checks in for a flight, the individual's identifying information is to be checked against these lists. Individuals matched to the No Fly list are to be denied boarding. If the individual is matched to the Selectee list, the person is to be subject to further screening, which could include physical screening, such as a pat-down. The criteria in general that are used to place someone on either of these two lists include the following:

- Persons who are deemed to be a threat to civil aviation or national security and should be precluded from boarding an aircraft are put on the No Fly list.

- Persons who are deemed to be a threat to civil aviation or national security but do not meet the criteria of the No Fly list are placed on the Selectee list and are to receive additional security screening prior to being permitted to board an aircraft.[16]

The White House Homeland Security Council devised these more stringent sets of criteria for the No Fly and Selectee lists in part because these lists are not intended as investigative or information-gathering tools or tracking mechanisms, and TSA is a screening but not an intelligence agency.[17] Rather, the lists are intended to help ensure the safe transport of passengers and facilitate the flow of commerce. However, the White House's review of the December 25 attempted terrorist attack raised questions about the effectiveness of the criteria, and the President tasked the FBI and TSC with developing recommendations for any needed changes to the nominations guidance and criteria.

Weighing and responding to the potential impacts that changes to the nominations guidance and criteria could have on the traveling public and the airlines will be important considerations in developing such recommendations. In September 2006, we reported that tens of thousands of individuals who had similar names to persons on the watchlist were being misidentified and subjected to additional screening, and in some cases delayed so long as to miss their flights.[18] We also reported that resolving these misidentifications can take time and, therefore, affect air carriers and commerce. If changes in criteria result in more individuals being added to the lists, this could also increase the number of individuals who are misidentified, exacerbating these negative effects. In addition, we

[16]Of all of the screening databases that accept watchlist records, only the No Fly and Selectee lists require certain nomination criteria or inclusion standards that are narrower than the "known or appropriately suspected" standard of HSPD-6. The most recent guidance related to the No Fly and Selectee list criteria was issued in February 2009.

[17]The Homeland Security Council originally was established in 2001 by executive order and subsequently codified into law by the Homeland Security Act of 2002 for the purpose of more effectively coordinating the policies and functions of the federal government relating to homeland security. See Exec. Order No. 13,228; Pub. L. No. 107-296, tit. IX, 116 Stat. 2135, 2258-59 (codified at 6 U.S.C. §§ 491-496). On May 26, 2009, the President announced the full integration of White House staff supporting national security and homeland security into a new "National Security Staff" supporting all White House policy-making activities relating to international, transnational, and homeland security matters. The Homeland Security Council was maintained as the principle venue for interagency deliberations on issues that affect the security of the homeland, such as terrorism, weapons of mass destruction, natural disasters, and pandemic influenza.

[18]GAO-06-1031.

explained that individuals who believe that they have been inappropriately matched to the watchlist can petition the government for action and the relevant agencies must conduct research and work to resolve these issues. If more people are misidentified, more people may trigger this redress process, increasing the need for resources. Finally, any changes to the criteria or process would have to ensure that watchlist records are used in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by federal law.

Agencies Do Not Screen Individuals against All Records in the Watchlist, Which Creates Potential Security Vulnerabilities; GAO Continues to Recommend That Agencies Assess and Address These Gaps

In reacting to the December 25 attempted terrorist attack, determining whether there were potential vulnerabilities related to the use of watchlist records when screening—not only individuals who fly into the country but also, for example, those who cross land borders—are important considerations. Screening agencies whose missions most frequently and directly involve interactions with travelers generally do not check against all records in the consolidated terrorist watchlist. In our October 2007 report, we noted that this is because screening against certain records may not be needed to support a respective agency's mission or may not be possible because of computer system limitations, among other things.[19]

For example, CBP's mission is to determine if any traveler is eligible to enter the country or is to be denied entry because of immigration or criminal violations. As such, CBP's computer system accepts all records from the consolidated watchlist database that have either a first name or a last name and one other identifier, such as a date of birth. Therefore, TSC sends CBP the greatest number of records from the consolidated watchlist database for its screening. In contrast, one of the State Department's missions is to approve requests for visas. Since only non-U.S. citizens and nonlawful permanent residents apply for visas, TSC does not send the department records on citizens or lawful permanent residents for screening visa applicants.

Also, the FBI database that state and local law enforcement agencies use for their missions in checking individuals for criminal histories, for example, also receives a smaller portion of the watchlist. According to the FBI, its computer system requires a full first name, last name, and other identifier, typically a date of birth. The FBI noted that this is because having these identifiers helps to reduce the number of times an individual

[19]GAO-08-110.

is misidentified as being someone on the list, and the computer system would not be effective in making matches without this information. Finally, the No Fly and Selectee lists collectively contain the lowest percentage of watchlist records because the remaining ones either do not meet the nominating criteria, as described above, or do not meet system requirements—that is, include full names and dates of birth, which TSA stated are required to minimize misidentifications.

TSA is implementing a new screening program that the agency states will have the capability to screen an individual against the entire watchlist.[20] Under this program, called Secure Flight, TSA will assume from air carriers the responsibility of comparing passenger information against the No Fly and Selectee lists.[21] According to the program's final rule, in general, Secure Flight is to compare passenger information only to the No Fly and Selectee lists.[22] The supplementary information accompanying the rule notes that this will be satisfactory to counter the security threat during normal security circumstances. However, the rule provides that TSA may use the larger set of watchlist records when warranted by security considerations, such as if TSA learns that flights on a particular route may pose increased risks. TSA emphasized that use of the full terrorist screening database is not routine. Rather, TSA noted that its use is limited to circumstances in which there is information concerning an increased risk to transportation security, and the decision to use the full watchlist database will be based on circumstances at the time. According to TSA, as of January 2010, the agency was developing administrative procedures for utilizing the full watchlist when warranted.

In late January 2009, TSA began to assume from airlines the watchlist matching function for a limited number of domestic flights, and has since phased in additional flights and airlines. TSA expects to assume the watchlist matching function for all domestic and international flights departing to and from the United States by December 2010. It is important to note that under the Secure Flight program, TSA requires airlines to provide the agency with each passenger's full name and date of birth to facilitate the watchlist matching process, which should reduce the number

[20]GAO-09-292.

[21]Pub. L. No. 108-458, § 4012(a), 118 Stat. 3638, 3714-15 (codified at 49 U.S.C. § 44903(j)(2)(C)).

[22]See 73 Fed. Reg. 64,018 (Oct. 28, 2008) (codified at 49 C.F.R. pt. 1560).

of individuals who are misidentified as the subject of a watchlist record. We continue to monitor the Secure Flight program at the Congress's request.

In our October 2007 watchlist report, we recommended that the FBI and DHS assess the extent to which security risks exist by not screening against certain watchlist records and what actions, if any, should be taken in response.[23] The agencies generally agreed with our recommendations but noted that the risks related to not screening against all watchlist records needs to be balanced with the impact of screening against all records, especially those records without a full name and other identifiers. For example, more individuals could be misidentified, law enforcement would be put in the position of detaining more individuals until their identities could be resolved, and administrative costs could increase, without knowing what measurable increase in security is achieved. While we acknowledge these tradeoffs and potential impacts, we maintain that assessing whether vulnerabilities exist by not screening against all watchlist records—and if there are ways to limit impacts—is critical and could be a relevant component of the government's ongoing review of the watchlist process. Therefore, we believe that our recommendation continues to have merit.

Identifying Additional Screening Opportunities and Determining Whether There Are Clear Lines of Authority for and Accountability over the Watchlist Process Would Help Ensure Its Effective Use

As we reported in October 2007, the federal government has made progress in using the consolidated terrorist watchlist for screening purposes, but has additional opportunities to use the list. For example, DHS uses the list to screen employees in some critical infrastructure components of the private sector, including certain individuals who have access to vital areas of nuclear power plants or transport hazardous materials. However, many critical infrastructure components are not using watchlist records, and DHS has not finalized guidelines to support such private sector screening, as HSPD-6 mandated and we previously recommended.[24]

In that same report, we noted that HSPD-11 tasked the Secretary of Homeland Security with coordinating across other federal departments to

[23]GAO-08-110.

[24]The identification of critical infrastructure components that are not using watchlist records for screening is considered Sensitive Security Information that cannot be disclosed in a public statement.

develop (1) a strategy for a comprehensive and coordinated watchlisting and screening approach and (2) a prioritized implementation and investment plan that describes the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of necessary activities.[25] We reported that without such a strategy, the government could not provide accountability and a basis for monitoring to ensure that (1) the intended goals for, and expected results of, terrorist screening are being achieved and (2) use of the watchlist is consistent with privacy and civil liberties. We recommended that DHS develop a current interagency strategy and related plans.

According to DHS's Screening Coordination Office, during the fall of 2007, the office led an interagency effort to provide the President with an updated report, entitled, HSPD-11, An Updated Strategy for Comprehensive Terrorist-Related Screening Procedures.[26] The office noted that the report was formally submitted to the Executive Office of the President through the Homeland Security Council and reviewed by the President on January 25, 2008. Further, the office noted that it also provided a sensitive version of the report to the Congress in October 2008. DHS provided us an excerpt of that report to review, stating that it did not have the authority to share excerpts provided by other agencies, and we were unable to obtain a copy of the full report. The information we reviewed only discussed DHS's own efforts for coordinating watchlist screening across the department. Therefore, we were not able to determine whether the HSPD-11 report submitted to the President addressed all of the components called for in the directive or what action, if any, was taken as a result. We maintain that a comprehensive strategy, as well as related implementation and investment plans, as called for by HSPD-11, continue to be important to ensure effective governmentwide use of the watchlist process.

In addition, in our October 2007 report, we noted that establishing an effective governance structure as part of this strategic approach is particularly vital since numerous agencies and components are involved in

[25]The White House, *Homeland Security Presidential Directive/HSPD-11, Subject: Comprehensive Terrorist-Related Screening Procedures* (Washington, D.C., Aug. 27, 2004).

[26]DHS established the Screening Coordination Office in July 2006 to enhance security measures by integrating the department's terrorist-and immigration-related screening efforts, creating unified screening standards and policies, and developing a single redress process for travelers.

the development, maintenance, and use of the watchlist process, both within and outside of the federal government. Also, establishing a governance structure with clearly-defined responsibility and authority would help to ensure that agency efforts are coordinated, and that the federal government has the means to monitor and analyze the outcomes of such efforts and to address common problems efficiently and effectively. We determined at the time that no such structure was in place and that no existing entity clearly had the requisite authority for addressing interagency issues. We recommended that the Homeland Security Council ensure that a governance structure was in place, but the council did not comment on our recommendation.

At the time of our report, TSC stated that it had a governance board in place, comprised of senior-level agency representatives from numerous departments and agencies. However, we also noted that the board provided guidance concerning issues within TSC's mission and authority. We also stated that while this governance board could be suited to assume more of a leadership role, its authority at that time was limited to TSC-specific issues, and it would need additional authority to provide effective coordination of terrorist-related screening activities and interagency issues governmentwide. In January 2010, the FBI stated that TSC has a Policy Board in place, with representatives from relevant departments and agencies, that reviews and provides input to the government's watchlist policy. The FBI also stated that the policies developed are then sent to the National Security Council Deputies Committee (formerly the Homeland Security Council) for ratification. The FBI noted that this process was used for making the most recent additions and changes to watchlist standards and criteria. We have not yet been able to determine, however, whether the Policy Board has the jurisdiction and authority to resolve issues beyond TSC's purview, such as issues within the intelligence community and in regard to the nominations process, similar to the types of interagency issues the December 25 attempted attack identified. We maintain that a governance structure with the authority for and accountability over the entire watchlist process, from nominations through screening, and across the government is important.

On January 7, 2010, the President tasked the National Security Staff with initiating an interagency review of the watchlist process—including the business processes, procedures, and criteria—and the interoperability and sufficiency of supporting information technology systems. This review offers the government an opportunity to develop an updated strategy, related plans, and governance structure that would provide accountability

to the administration, the Congress, and the American public that the watchlist process is effective at helping to secure the homeland.

Recent Work Highlights the Importance of Conducting Vulnerability Assessments and Operational Testing Prior to Deployment of New Checkpoint Technologies

While TSA Has Not Yet Deployed Any New Checkpoint Technologies Nationwide, It Plans to Have Installed Almost 200 AITs by the End of 2010

As we reported in October 2009, in an effort to improve the capability to detect explosives at aviation passenger checkpoints, TSA has 10 passenger screening technologies in various phases of research, development, procurement, and deployment, including the AIT (formerly Whole Body Imager).[27] TSA is evaluating the AIT as an improvement over current screening capabilities of the metal detector and pat-downs specifically to identify nonmetallic threat objects and liquids. The AITs produce 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.[28] The energy reflected back from the body or other objects on the body is used to construct a three-dimensional image. Millimeter wave

[27]GAO-10-128.

[28]According to TSA, this description of the millimeter wave technology applies only to the machine manufactured by L3 and does not apply to other millimeter wave technologies that TSA is evaluating, such as the Smiths millimeter wave AIT.

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.[29]

As we reported in October 2009, TSA has not yet deployed any new technologies nationwide. However, as of December 31, 2009, according to a senior TSA official, the agency has deployed 40 of the millimeter wave AITs, and has procured 150 backscatter X-ray units in fiscal year 2009 and estimates that these 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 will be purchased with funds from the American Recovery and Reinvestment Act of 2009.[30] TSA plans to procure and deploy a total of 878 units at all category X through category IV airports.[31] Full operating capability is expected in fiscal year 2014. TSA officials stated that the cost of the AIT is about $130,000 to $170,000 per unit, excluding installation costs. In addition, the estimated training costs are $50,000 per unit.

While TSA stated that the AIT will enhance its explosives detection capability, 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 never sees the image that the technology produces, and the officer who views the image is remotely located in a secure resolution room and never sees 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

[29]Research and development of the AIT technology is continuing, specifically, to develop passive terahertz (THz) and active gigahertz (GHz) technologies to improve detection performance and reduce operational costs of commercially available systems.

[30]According to TSA, some of the 300 AIT units to be procured in fiscal year 2010 will begin to be deployed to airports in the latter half of fiscal year 2010.

[31]TSA classifies the commercial airports in the United States into one of five security risk categories (X, I, II, III, and IV). In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest. Categories X, I, II, and III airports account for more than 90 percent of the nation's air traffic.

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 direct physical pat-down before the passenger is cleared to enter the sterile area.[32] 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 segregated from the checkpoint to help ensure passenger privacy.

TSA Reports That It Is Taking Steps to Operationally Test AITs but Has Not Conducted Vulnerability Assessments

We previously reported on several challenges TSA faces related to the research, development, and deployment of passenger checkpoint screening technologies and made a number of recommendations to improve this process.[33] Two of these recommendations are particularly relevant today, as TSA moves forward with plans to install a total of 878 additional AITs—completing operational testing of technologies in airports prior to using them in day-to-day operations and assessing whether technologies such as the AIT are vulnerable to terrorist countermeasures, such as hiding threat items on various parts of the body to evade detection.

First, in October 2009, we reported that TSA had relied on technologies in day-to-day airport operations that had not been proven to meet their functional requirements through operational testing and evaluation, contrary to TSA's acquisition guidance and a knowledge-based acquisition approach. 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.[34] In commenting

[32]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.

[33]GAO-10-128.

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

on our report, TSA agreed with this recommendation. A senior TSA official stated that although TSA does not yet have a written policy requiring operational testing prior to deployment, TSA is now including in its contracts with vendors that checkpoint screening machines are required to successfully complete laboratory tests as well as operational tests. The test results are then incorporated in the source selection plan. The official also stated that the test results are now required at key decision points by DHS's Investment Review Board. While recently providing GAO with updated information to our October 2009 report, TSA stated that operational testing for the AIT was completed as of the end of calendar year 2009. We are in the process of verifying that TSA has tested all of the AIT's functional requirements in an operational environment.

Deploying technologies that have not successfully completed operational testing and evaluation can lead to cost overruns and underperformance. TSA's procurement guidance provides that testing should be conducted in an operational environment to validate that the system meets all functional requirements before deployment. 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.[35] 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.

TSA's experience with the ETPs, which the agency uses for secondary screening, demonstrates the importance of testing and evaluation in an operational environment. 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.[36] TSA deployed the ETPs even though agency officials were aware that tests conducted during 2004 and 2005 on earlier ETP models suggested that they did not demonstrate reliable performance. Furthermore, the ETP

[35]GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition*, GAO-04-386SP (Washington, D.C.: January 2004).

[36]TSA deployed the ETPs from January to June 2006. Since June 2006, TSA removed all but 9 ETPs from airports because of maintenance issues.

models that were subsequently deployed were not first 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. TSA estimates that the 9 remaining ETPs will be removed from airports by the end of calendar year 2010. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security. Furthermore, retaining existing screening procedures until the effectiveness of future technologies has been validated could provide assurances that use of checkpoint technologies improves aviation security.

Second, as we reported in October 2009, TSA does not know whether its explosives detection technologies, such as the AITs, are susceptible to terrorist tactics. Although TSA has obtained information on vulnerabilities at the screening checkpoint, the agency has not assessed vulnerabilities—that is, weaknesses in the system that terrorists could exploit in order to carry out an attack—related to passenger screening technologies, such as AITs, that are currently deployed. 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, where he concealed an explosive in his underwear. However, TSA has not assessed whether these and other tactics that terrorists could use to evade detection by screening technologies, such as AIT, increase the likelihood that the screening equipment would not detect the hidden weapons or explosives. Thus, without an assessment of the vulnerabilities of checkpoint technologies, it is unclear whether the AIT or other technologies would have been able to detect the weapon Mr. Abdulmutallab used in his attempted attack. TSA is in the process of developing a risk assessment for the airport checkpoints, but the agency has not yet completed this effort or clarified the extent to which this effort addresses any specific vulnerabilities in checkpoint technology.

TSA officials stated that to identify vulnerabilities at airport checkpoints, the agency analyzes information such as the results from its covert testing program. TSA conducts national and local covert tests, whereby individuals attempt to enter the secure area of an airport through the

passenger checkpoint with prohibited items in their carry-on bags or hidden on their persons. However, TSA's covert testing programs do not systematically test passenger and baggage screening technologies nationwide to ensure that they identify the threat objects and materials the technologies are designed to detect, nor do the covert testing programs identify vulnerabilities related to these technologies. We reported in August 2008 that while TSA's local covert testing program attempts to identify test failures that may be caused by screening equipment not working properly or caused by screeners and the screening procedures they follow, the agency's national testing program does not attribute a specific cause of a test failure.[37] We recommended, among other things, that TSA require the documentation of specific causes of all national covert testing failures, including documenting failures related to equipment, in the covert testing database to help TSA better identify areas for improvement. TSA concurred with this recommendation and stated that the agency will expand the covert testing database to document test failures related to screening equipment.

In our 2009 report, we also recommended that the Assistant Secretary for TSA, among other actions, conduct a complete risk assessment—including threat, vulnerability, and consequence assessment—for the passenger screening program and incorporate the results into TSA's program strategy, as appropriate. TSA and DHS concurred with our recommendation, but have not completed these risk assessments or provided documentation to show how they have addressed the concerns raised in our 2009 report regarding the susceptibility of the technology to terrorist tactics.

Mr. Chairman, this concludes our statement for the record.

Contacts and Acknowledgments

For additional information on this statement, please contact Eileen Larence at (202) 512-6510 or larencee@gao.gov or Stephen Lord at (202) 512-4379 or lords@gao.gov.

[37]See GAO, *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests*, GAO-08-958 (Washington, D.C.: Aug. 8, 2008).

In addition to the contacts named above, Kathryn Bernet, Carissa Bryant, Frances Cook, Joe Dewechter, Eric Erdman, Richard Hung, Anne Laffoon, Linda Miller, Victoria Miller, and Michelle Woods made key contributions to this statement.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper

Transportation Security Administration

Imaging Technology

Innovation & Technology

Overview | Advanced Technology | Biometrics | BLS | CastScope
EDS | ETD | Paperless Boarding Pass | Threat Image Projection
Imaging Technology

TSA began deploying state-of-the-art advanced imaging technologies in 2007. This technology can detect a wide range of threats to transportation security in a matter of seconds to protect passengers and crews. Imaging technology is an integral part of TSA's effort to continually look for new technologies that help ensure travel remains safe and secure by staying ahead of evolving threats.

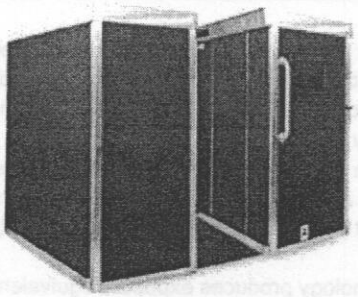
TSA uses two types of imaging technology, millimeter wave and backscatter. Currently, there are 40 millimeter wave imaging technology units in use at 19 airports. Six machines are used as primary screening at six airports and 34 machines are used for secondary, or random screening, as an alternative to a pat down at 13 airports.

In March 2010, TSA began deploying 150 backscatter imaging technology units, which were purchased with American Recovery and Reinvestment Art (ARRA) funds. TSA plans to deploy a total of approximately 450 imaging technology units in 2010.

Advanced imaging technology screening is safe for all passengers, and the technology meets national health and safety standards. Backscatter technology was evaluated by the Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH), the National Institute for Science and Technology (NIST), and the Johns Hopkins University Applied Physics Laboratory (APL), and results confirmed that radiation doses are well below those specified by the American National Standards Institute. The amount of radiation from backscatter screening is equivalent to two minutes of flight on an airplane, and the energy projected by millimeter wave technology is 10,000 times less than a cell phone transmission.

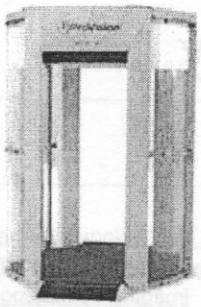
TSA has implemented strict measures to protect passenger privacy, which is ensured through the anonymity of the image. The image cannot be stored, transmitted or printed, and is deleted immediately once viewed. Additionally, advanced imaging technology screening is optional to all passengers.

How the Technology Works



Backscatter

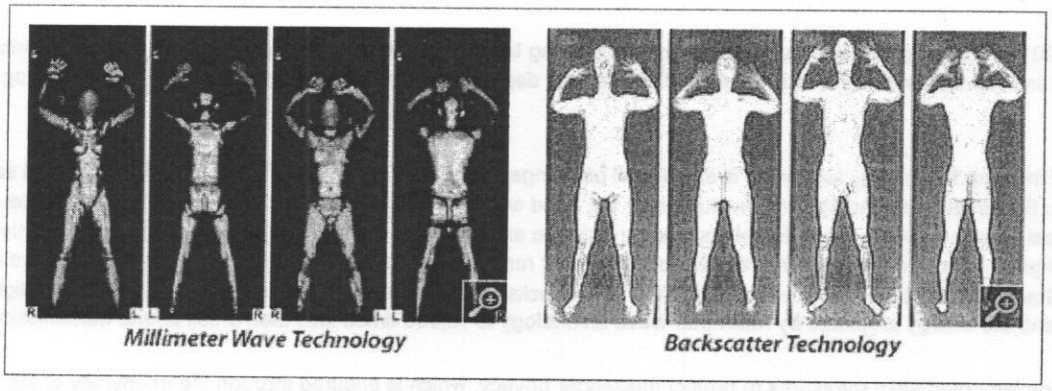
- Backscatter technology projects low level X-ray beams over the body to create a reflection of the body displayed on the monitor.



Millimeter Wave

- Millimeter wave technology bounces harmless electromagnetic waves off the body to create a black and white three-dimensional image.

What TSA Sees



- Millimeter wave technology produces an image that resembles a fuzzy photo negative.
- Backscatter technology produces an image that resembles a chalk etching.
- Both technologies are viewed by a Transportation Security Officer in a remote, secure location.

Safety Features

- Advanced imaging technology is safe and meets national health and safety standards.
- Backscatter technology was evaluated by the Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH), the National Institute for Science and Technology (NIST), and the Johns Hopkins University Applied Physics Laboratory (APL).
- All results confirmed that the radiation doses for the individuals being screened, operators, and bystanders were well below the dose limits specified by the American National Standards Institute.
- For comparison, the energy projected by millimeter wave technology is 10,000 times less than a cell phone transmission.
- A single scan using backscatter technology produces exposure equivalent to two minutes of flying on an airplane.

Protecting Passenger Privacy

- Strict privacy safeguards are built into the foundation of TSA's use of advanced imaging technology to protect passenger privacy and ensure anonymity.
- The officer who assists the passenger never sees the image the technology produces.
- The officer who views the image is remotely located, in a secure resolution room and never sees the passenger.
- To further protect passenger privacy, millimeter wave technology blurs all facial features and backscatter has an algorithm applied to the entire image.
- The two officers communicate via wireless headset. Once the remotely located officer determines threat items are not present, that officer communicates wirelessly to the officer assisting the passenger. The passenger may then continue through the security process.
- Advanced imaging technology cannot store, print, transmit or save the image.
- Officers evaluating images are not permitted to take cameras, cell phones or photo-enabled devices into the resolution room.
- Each image is automatically deleted from the system after it is cleared by the remotely located security officer.

What to Expect

- Each passenger will walk into the imaging portal. Once inside, they will be asked to stand in different positions and remain still for just a few moments while the technology creates an image of the passenger in real time.
- Once complete, the passenger will exit the opposite side of the portal.
- Advanced imaging technology does not store, print, transmit or save the image. All machines have zero storage capability and all images are automatically deleted from the system after they are reviewed by the remotely located security officer.

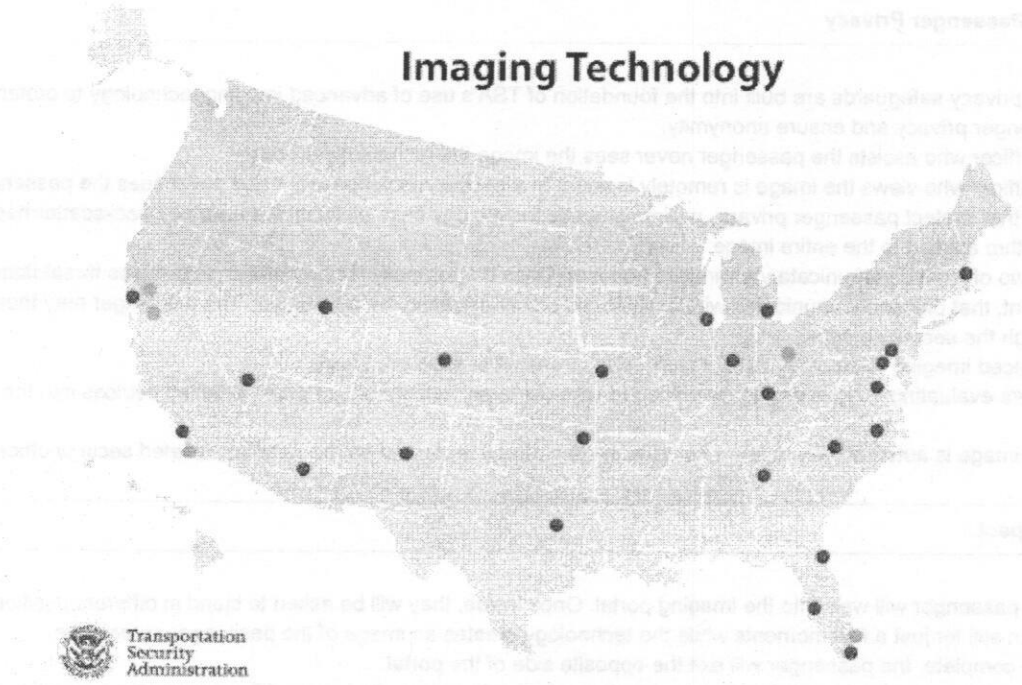
What are my Options?

- Advanced imaging technology screening is **optional for all passengers**.
- Passengers who do not wish to utilize this screening will receive an equal level of screening, including a physical pat-down.
- Multiple signs informing passengers about the technology, including sample images, are displayed in plain sight at the security checkpoints, in front of the advanced imaging units.
- Many passengers prefer advanced imaging technology. In fact, over 98 percent of passengers who encounter this technology during TSA pilots prefer it over other screening options.
- Additionally, passengers with joint replacements or other medical devices that would regularly alarm a metal detector often prefer this technology because it is quicker and less-invasive than a pat down.

Detection

This walk-through imaging technology efficiently detects metallic and non-metallic threats, including weapons, explosives and other items that a passenger is carrying on his/her person, without physical contact.

Where It Is



Airports receiving technologies soon:

- Boston Logan International Airport
- Charlotte Douglas International Airport
- Chicago O'Hare International Airport
- Cincinnati/Northern Kentucky International Airport
- Fort Lauderdale-Hollywood International Airport
- Kansas City International Airport
- Los Angeles International Airport
- Mineta San José International Airport
- Oakland International Airport
- Port Columbus International Airport
- San Diego International Airport

Airports who currently have technologies:

- Albuquerque International Sunport Airport
- Hartsfield-Jackson Atlanta International Airport
- Baltimore/Washington International Thurgood Marshall Airport
- Denver International Airport
- Dallas/Fort Worth International Airport
- Detroit Metro Airport
- Indianapolis International Airport
- Jacksonville International Airport

- McCarran International Airport
- Los Angeles International Airport
- Miami International Airport
- Phoenix Sky Harbor International Airport
- Raleigh-Durham International Airport
- Richmond International Airport
- Ronald Reagan Washington National Airport
- San Francisco International Airport
- Salt Lake City International Airport
- Tampa International Airport
- Tulsa International Airport

Other Advanced Imaging Technology Deployments

Domestic locations:

- Colorado Springs Court House (CO)
- Cook County Court House (IL)
- Department of Corrections facility (PA)
- Douglas County Colorado Justice Center
- Montana State Prison
- Utah State Correctional Facility

International locations:

Advanced imaging technology is used in hundreds of locations around the world in aviation and mass transit environments, including Canada, France, the Netherlands, Nigeria and the United Kingdom.

More on Advanced Imaging Technology:

- Click here to read the Privacy Impact Assessment for TSA's Whole Body Imaging (pdf, 183Kb)
- TSA Continues Millimeter Wave Passenger Imaging Technology Pilot

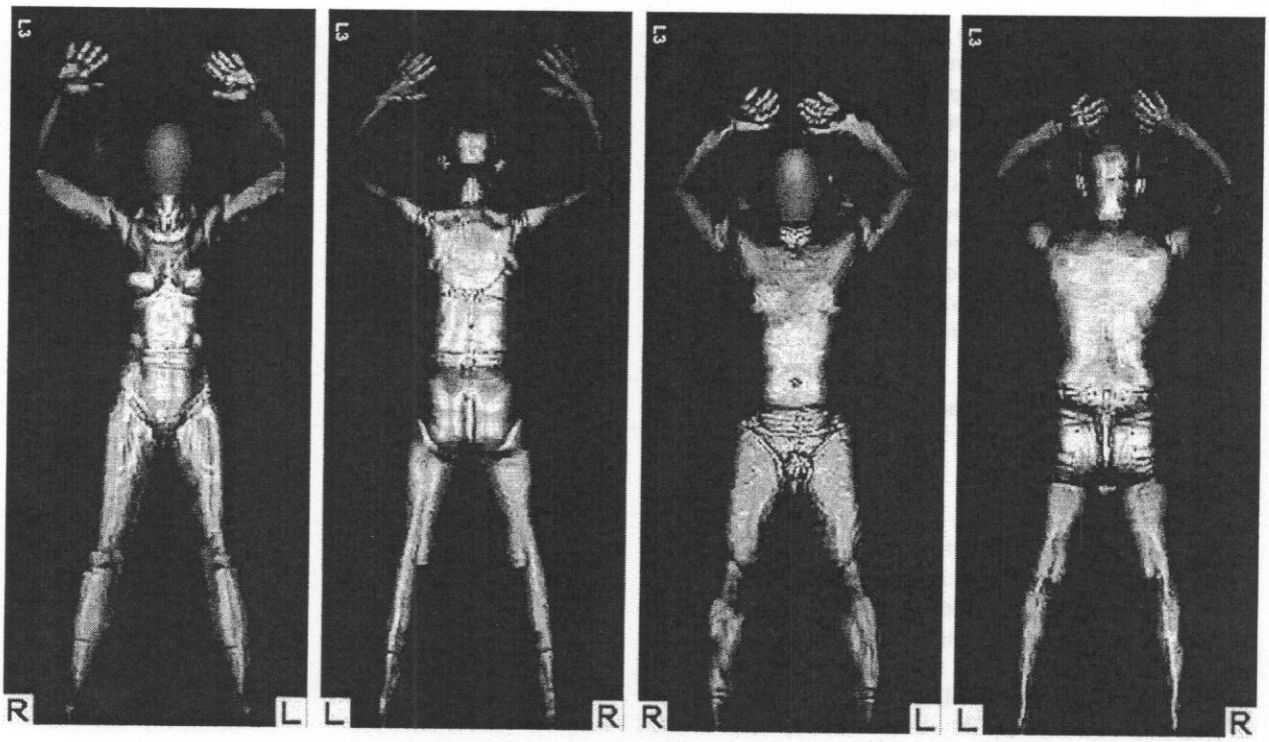
- Watch a CBS 60 Minutes segment about advanced imaging technology.
- Watch a video demonstrating how advanced imaging technology works (streaming | download) (wmv, 3.4mb).
- Watch how technology detects threats to transportation and helps keep passengers safe (streaming | download) (wmv, 3.4mb).

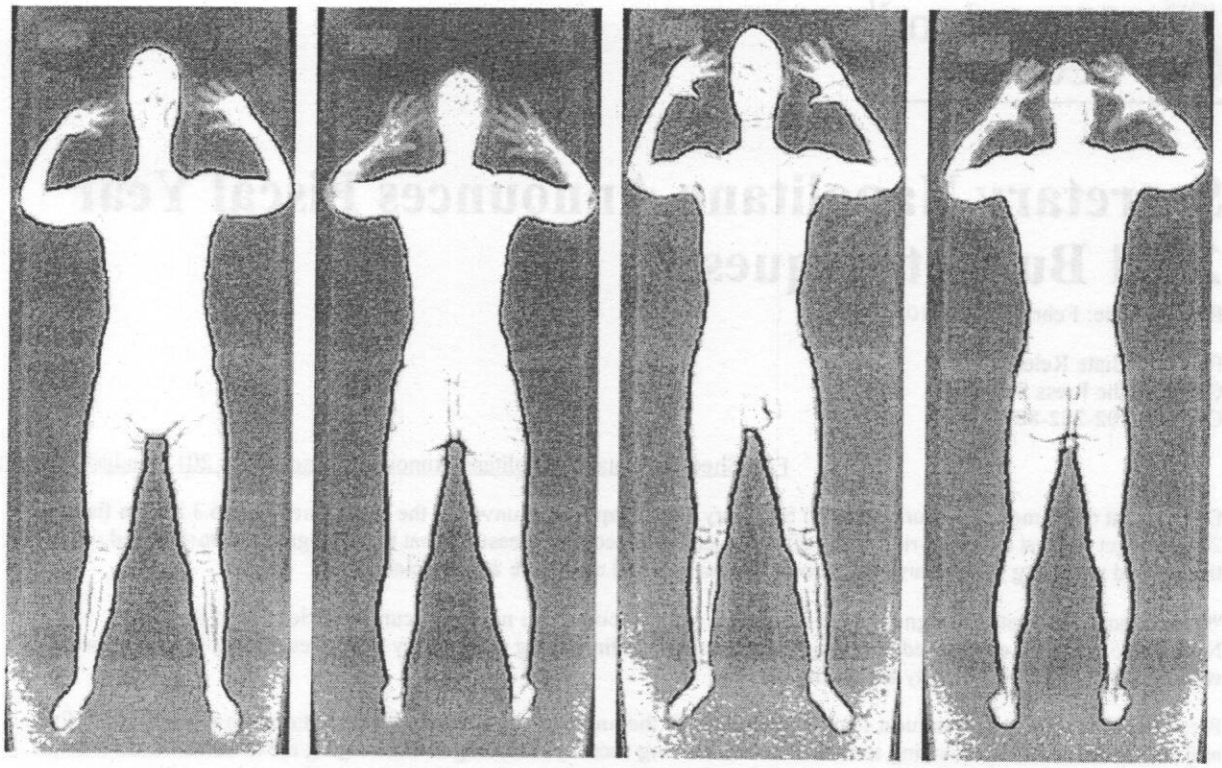
- Click here to read 'Screeners get closer look' (TulsaWorld.com)
- Click here to view the story from KSL-TV (NBC) Salt Lake City.

Download Plug-in
Some of the links on this page require a plug-in to view them, which are available below.

Adobe Acrobat (PDF)

Windows Media Player


L3
R
L
L3
L
R
L3
R
L
L3
L
R



http://www.tsa.gov/graphics/images/approach/backscatter_large.jpg 9/13/2010

Homeland Security

Secretary Napolitano Announces Fiscal Year 2011 Budget Request

Release Date: February 1, 2010

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Fact Sheet: Secretary Napolitano Announces Fiscal Year 2011 Budget Request

Department of Homeland Security (DHS) Secretary Janet Napolitano unveiled the Department's $56.3 billion fiscal year 2011 budget request today—prioritizing efforts to enhance security measures that protect against terrorism and other threats and reflecting the Department's commitment to fiscal discipline and efficiency.

"Our proposed budget is designed to ensure we have the resources we need to secure America," said Secretary Napolitano. "We are committed to strong fiscal discipline, eliminating redundancy and investing our resources in what works while enhancing security across the board."

President Obama's budget request for DHS strengthens the ongoing work across the Department in each of DHS' five major mission areas—preventing terrorism and enhancing security; securing and managing the nation's borders; smart and effective enforcement of immigration laws; safeguarding and securing cyberspace; and ensuring resiliency to disasters.

The proposed budget also furthers Secretary Napolitano's major reform goals to continue institutionalizing a new culture of efficiency and fiscal discipline at DHS.

FY2011 Budget Priorities:

Preventing Terrorism and Enhancing Security— Guarding against terrorism was the founding mission of DHS and remains our top priority today. A key element of preventing terrorism is recognizing the evolving threats posed by violent extremists and taking action to ensure our defenses continue to evolve to deter and defeat them. The proposed DHS budget strengthens several aviation security programs by increasing Federal Air Marshal coverage on international flights and through the deployment of additional canine teams, Behavior Detection Officers, Explosive Trace Detection machines and Advanced Imaging Technology units to increase the Department's ability to detect metallic and non-metallic explosives and other threats at airports across the country.

Securing and Managing the Nation's Borders— DHS monitors our air, land and sea borders to prevent illegal trafficking that threatens our country, while facilitating lawful travel and trade. DHS will continue to strengthen security efforts on the southwest border to combat and disrupt cartel violence and provide critical security upgrades—through infrastructure and technology—along the northern border. The fiscal year 2011 DHS budget request includes funding for increased staffing and better pay for frontline officers; additional Border Enforcement Security Task Forces and border intelligence analysts; new technology to support intellectual property rights enforcement; and enhancements to Coast Guard maritime border security air and marine assets.

Smart and Effective Enforcement of Immigration Laws—DHS is responsible for enforcing the nation's immigration laws while streamlining and facilitating the legal immigration process. In FY 2011, we will continue to strengthen enforcement activities while targeting criminal aliens who pose a threat to public safety and employees who knowingly violate the law. This budget request supports enhancements to *E-Verify*—DHS' simple and effective online system to verify employment eligibility of new hires; funding to continue nationwide implementation of the Secure Communities program—which uses biometrics to identify and remove criminal aliens incarcerated in state and local jails; and programs that promote citizenship awareness, enhance English-language education and assist community-based organizations prepare immigrants for citizenship.

Safeguarding and Securing Cyberspace—The Department defends against, and responds to, attacks on cyber networks – analyzing threats and vulnerabilities, coordinating the response to cyber incidents and working with the private sector and our state, local, international and private sector partners to ensure that our computers, networks and cyber systems remain safe. The proposed DHS budget includes funding for the National Cyber Security Division to identify and reduce vulnerabilities in our nation's key cyber networks and to enhance cyber security coordination capabilities across the Federal Government.

Preparing for, Responding to, and Recovering from Disasters—The Department provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergencies while working with federal, state, local and private sector partners to ensure a swift and effective recovery effort. DHS will continue its efforts to build a ready and resilient nation by bolstering information sharing; providing grants, plans, and training to our homeland security and law enforcement partners; and further streamlining rebuilding and recovery along the Gulf Coast. The proposed DHS budget prioritizes program and technical support for state, local and tribal governments to reduce risk; modernization of flood maps to better communicate flood hazards; enhancement of emergency response and rapid recovery capabilities; and upgrading key Federal Emergency Management Agency facilities to better accommodate its critical mission.

The full DHS FY 2011 budget request can be found at www.dhs.gov/xabout/budget/.

###

This page was last reviewed/modified on February 1, 2010.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government

- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

Homeland Security

Fact Sheet: Secretary Napolitano Announces Fiscal Year 2011 Budget Request

Release Date: February 1, 2010

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

The Department of Homeland Security (DHS) unveiled its $56.3 billion fiscal year 2011 budget request today—prioritizing efforts to enhance security measures that protect against terrorism and other threats and reflecting the Department's commitment to fiscal discipline and efficiency.

Preventing Terrorism and Enhancing Security

- *Advanced Imaging Technology (AIT)*: An increase of $214.7M is requested to procure and install 500 advanced imaging technology machines at airport checkpoints to detect dangerous materials, including non-metallic materials. This request, along with planned deployments for 2010, will provide AIT coverage at 75 percent of Category X airports and 60 percent of the total lanes at Category X through II airports.
- *Transportation Security Officers (TSOs) to Staff AITs*: An increase of $218.9M is requested for additional Transportation Security Officers (TSOs), managers and associated support costs to operate additional AITs at airport checkpoints. Passenger screening is critical to detecting and preventing individual carrying dangerous or deadly objects from boarding planes.
- *Federal Air Marshals (FAMs)*: An increase of $85M is requested for additional FAMS to increase international flight coverage. FAMs help detect, deter and defeat terrorist and other criminal hostile acts targeting U.S. air carriers, airports, passengers and crew.
- *Portable Explosive Trace Detection (ETD)*: An increase of $60M is requested to purchase approximately 800 portable ETD machines ($39M) and associated checkpoint consumables ($21M).
- *Canine Teams*: An increase of $71M is requested to fund an additional 275 proprietary explosives detection canine teams, 112 teams at 28 Category X airports and 163 teams at 56 Category I airports.
- *Behavior Detection Officers (BDOs)*: An increase of $20M is requested to further enhance Transportation Security Administration's (TSA's) Screening Passengers by Observation Techniques program. The FY 2011 request includes a total of 3,350 officers to enhance coverage at lanes and shifts at high risk Category X and I airports and expand coverage to smaller airports.
- *Domestic Nuclear Detection Office Systems Engineering and Architecture*: An increase of $13.4M is requested to fund systems engineering efforts to address vulnerabilities in the Global Nuclear Detection Architecture, the multi-layered system of detection technologies, programs and guidelines designed to enhance the Nation's ability to detect and prevent a radiological or nuclear attack.
- *Radiological/Nuclear Detection Systems*: An increase of $41M is requested for the procurement and deployment of radiological and nuclear detection systems and equipment to support efforts across the Department.
- *Law Enforcement Detachment Teams*: An increase of $3.6M is requested to bring deployable U.S. Coast Guard Law Enforcement Detachment (LEDET) teams to full capacity. LEDETs help prevent terrorism, secure U.S. borders, disrupt criminal organizations and support counter drug missions overseas. In FY 2009, for example, LEDETs aboard U.S naval and partner nation assets accounted for more than 50 percent of total maritime cocaine

removals.

- *2012 Presidential Campaign*: Total funding of $14M is requested for startup costs associated with the 2012 Presidential Campaign including training for candidate/nominee protective detail personnel. The Secret Service will also begin to procure and pre-position equipment, services and supplies to support candidate/nominee protective operations throughout the country.

- *Secret Service Information Technology*: Total funding of $36M is requested for the Information Integration and Transformation program. This funding will allow the Secret Service to successfully continue its comprehensive Information Technology (IT) transformation and provide a multi-year, mission-integrated program to engineer a modernized, agile and strengthened IT infrastructure to support all aspects of the Secret Service's mission.

Securing and Managing Our Borders

- *Journeyman Pay Increase*: In the spring of 2010, DHS will implement the journeymen pay increase, raising the journeyman grade level for frontline Customs and Border Protection (CBP) Officers, Border Patrol Agents and Agricultural Specialists from GS-11 level to the GS-12 level. An adjustment to base of $310.4M will fund the full-year impact of the salary and benefit requirements associated with this implementation.

- *CBP Officers*: An increase of $44.8M is requested to fund 318 CBP Officers FTEs within the Office of Field Operations and 71 support FTEs for CBP. The decline in the number of passengers and conveyances entering the United States in FY 2009 resulted in an almost 8 percent decrease in revenues from inspection user fees. CBP, therefore, has fewer resources to maintain critical staffing levels for CBP officers. The proposed funding will allow CBP to maintain staffing for critical positions to protect the United States at its ports of entry.

- *Border Enforcement Security Task Forces (BESTs)*: An additional $10M is requested to establish BESTs in three additional locations: Massena, NY; San Francisco, CA and Honolulu, HI. These multi-agency teams work to identify, disrupt and dismantle criminal organizations posing significant threats to border security, including terrorist groups, gang members, and criminal aliens.

- *Intellectual Property Rights (IPR) Enforcement*: An increase of $25M is requested to support CBP IPR enforcement efforts including information technology systems that support IPR activities and implementation of the 5-year IPR Plan. An increase of $5M is also requested for the Immigration and Customs Enforcement (ICE)-led National Intellectual Property Rights Coordination Center (IPR Center). The IPR Center brings key U.S. government agencies together to combat IPR violations that threaten our economic stability, restrict the competitiveness of U.S. industry and endanger the public's health and safety. ICE will also use these funds to focus on disrupting criminal organizations through the internet and support for anti-counterfeiting efforts.

- *Intelligence Analysts*: An increase of $10M is requested to fund 103 Intelligence Analysts for CBP. This staffing increase will support 24/7 operations of CBP Intelligence Watch, Operations Coordination and the Commissioner's Situation Room.

- *Coast Guard Asset Recapitalization*: A total of $1.4B is requested to continue recapitalization of aging Coast Guard surface and air assets. Included in this request is $538M for production of the Coast Guard's fifth National Security Cutter to continue replacement of the 378-foot High Endurance Cutters fleet. Also included is $240M for production of four Fast Response Cutters to continue replacement of the 110-foot Class Patrol Boat fleet. The Fast Response Cutters have enhanced capability, high readiness, speed, and endurance, which will allow them to quickly and effectively respond to emerging threats. Additionally, $40M is requested to purchase one Maritime Patrol Aircraft (MPA) HC 144A. The HC-144A will address the Coast Guard's MPA flight hour gap by providing 1,200 hours every year per aircraft. Finally, $13.9M is requested for improvement and/or acquisition of housing to support military families.

Enforcing and Administering Our Immigration Laws

- *E-Verify*: A total of $103.4M is requested for the E-Verify Program. In FY 2011, U.S. Citizenship and Immigration Services (USCIS) will develop and implement an E-Verify portal that will provide a single-user interface for the program's products and services. In addition, USCIS will enhance E Verify's monitoring and

compliance activities through analytical capabilities that will support more robust fraud detection and improved analytic processes and will continue developing system enhancements in response to customer feedback, surveys, mission requirements and capacity needs.

- *Secure Communities*: Total funding of $146.9M is requested to continue FY 2010 progress toward nationwide implementation of the Secure Communities program—which involves the identification, apprehension and removal of all Level 1 criminal aliens in state and local jails through criminal alien biometric identification capabilities. Secure Communities, in cooperation with federal, state and local law enforcement agencies, will provide a safeguard to American communities by removing those criminal aliens from the United States that represent the greatest threats to public safety and by deterring their re-entry through aggressive prosecution.

- *Immigrant Integration*: A total of $18M is requested to fund USCIS Office of Citizenship initiatives, including expansion of the competitive Citizenship Grant Program to support national and community-based organizations preparing immigrants for citizenship, promote and raise awareness of citizenship rights and responsibilities, and enhance English language education and other tools for legal permanent residents. The Office of Citizenship will support the implementation of the Immigration Integration program and lead initiatives to educate aspiring citizens about the naturalization process, monitor and evaluate the administration and content of the new naturalization test, and develop educational materials and resources for immigrants and the organizations that serve them.

Safeguarding and Securing Cyberspace

- *National Cyber Security Division (NCSD)*: Total funding of $379M is requested for the NCSD to support the development of capabilities to prevent, prepare for and respond to incidents that could degrade or overwhelm the Nation's critical information technology infrastructure and key cyber networks. These funds will identify and reduce vulnerabilities, mitigate threats and ensure that cyber intrusions and disruptions cause minimal damage to public and private sector networks.
- *National Cyber Security Center (NCSC)*: A total of $10M is requested for the NCSC to enhance cyber security coordination capabilities across the Federal Government including mission integration, collaboration and coordination, situational awareness and cyber incident response, analysis and reporting, knowledge management, and technology development and management.

Ensuring Resilience to Disasters

- *Disaster Relief Fund (DRF)*: The budget seeks funding of $1.95B, an increase of $0.35B for the DRF. The DRF provides a significant portion of the total federal response to victims in declared major disasters and emergencies.

- *Federal Emergency Management Agency (FEMA) Facilities*: An additional $23.3M is requested to address critical FEMA real estate needs. By FY 2011, the capacity of FEMA facilities will be unable to accommodate key mission responsibilities and staff. FEMA also faces a critical need to maintain and repair aging and deteriorating national facilities. To address these needs, FEMA has developed a 5 year capital plan to begin critical regional facility acquisitions and repairs.

- *Pre-Disaster Mitigation Grants*: Total funding of $100M is requested to provide program support and technical assistance to state, local and tribal governments to reduce the risks associated with disasters, support the national grant competition and provide the required $500,000 per state allocation. Resources will support the development and enhancement of hazard mitigation plans, as well as the implementation of pre-disaster mitigation projects.

- *Flood Map Modernization*: A total of $194M is requested to analyze and produce flood hazard data and map products and communicate flood hazard risk. The funding will support the review and update of flood hazard data and maps to accurately reflect flood hazards and monitor the validity of published flood hazard information.

- *Rescue 21*: $36M is requested for the Rescue 21 system, enabling the U.S. Coast Guard to enhance preparedness, ensure efficient emergency response and rapidly recover from disasters. The Rescue 21 system replaces the U.S. Coast Guard's legacy National Distress and Response System and improves communications and command and control capabilities in the coastal zone. The system is the foundation for coastal Search and Rescue and enhances maritime domain awareness through increased communications ability with mariners and interagency partners.

Maturing and Strengthening the Homeland Security Enterprise

- *St. Elizabeth's Headquarters Consolidation*: To streamline the Departments core operations, $287.8M is requested to consolidate executive leadership, operations coordination and policy and program management functions in a secure setting at St. Elizabeth's. The Department's facilities are currently dispersed over more than 40 locations throughout the National Capital Region (NCR). This consolidation at St. Elizabeth's will reduce the fragmentation of components and will improve communications, coordination and cooperation across all DHS headquarters organizations.

- *Lease Consolidation* – Mission Support: A total of $75M is requested to align the Department's real estate portfolio in the NCR to enhance mission performance and increase management efficiency.

- *Data Center Migration*: A total of $192.2M is requested for the continuation of system and application migration of legacy data centers to two enterprise-wide DHS Data Centers to meet current and anticipated data service requirements. Funding will also be utilized for upgrading infrastructure requirements.

- *Acquisition Workforce*: The FY 2011 request includes an increase of $24M to strengthen the Department's acquisition workforce capacity and capabilities. The increase is requested to mitigate the risks associated with skill gaps of the acquisition workforce, ensure that the Department achieves the best terms possible in major acquisitions and improve the effectiveness of the workforce.

- *Science and Technology (S&T) Safe Container (SAFECON)/Time Recorded Ubiquitous Sensor Technology (TRUST) R&D*: A total of $8M is requested for the S&T SAFECON and TRUST programs. These initiatives develop high reliability, high-throughput detection technologies to scan cargo containers entering the country for weapons of mass destruction, explosives, contraband and human cargo.

- *Grants*: A total of $4B is requested for grant programs to support our nation's first responders. This funding assists state and local governments in the prevention of, protection against, response to and recovery from incidents of terrorism and other events.

###

This page was last reviewed/modified on February 1, 2010.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)

- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

Homeland Security

Transcript of Background Call with Senior DHS Officials on the Department's Fiscal Year 2011 Budget Proposal

Release Date: February 1, 2010

For Immediate Release
Office of the Press Secretary
Contact 202-282-8010
Washington, D.C.

Moderator: I'm going to turn the conference call over to Mr. Bobby Whithorne. Mr. Whithorne, please go ahead.

Mr. Whithorne: Thank you very much. I'd like to welcome everybody to the background briefing for the DHS fiscal year 2011 budget request. I'm joined by our Acting Chief Financial Officer, Peggy Sherry, and other senior DHS officials. Peggy will be on the record and everybody else will be attributed to a DHS official. We will have the transcript out shortly after the call, and with that, I'll turn it over to Peggy.

Ms. Sherry: Thank you. Good afternoon. I'm Peggy Sherry, the Acting Chief Financial Officer for the Department of Homeland Security [DHS], and thank you for participating in this call.

The fiscal year 2011 DHS budget will strengthen efforts that are critical to the nation's security, bolster the Department's ability to combat terrorism, respond to emergencies and potential threats, and allow DHS to tackle its responsibilities to protect the nation and keep Americans safe.

DHS secures the United States against all threats through five main missions, specifically, these mission areas are preventing terrorism and enhancing security; guarding against terrorism was the sounding mission of DHS and remains our top priority today.

Securing and managing our borders. DHS monitors our air, land and sea borders to prevent illegal trafficking that threatens our country while facilitating lawful travel and trade.

Enforcing and administering our immigration laws. DHS is responsible for enforcing the nation's immigration laws while streamlining and facilitating the legal immigration process.

Safeguarding and securing cyber space. The Department defends against and responds to attacks on its cyber networks through which Americans communicate with each other, do business and manage infrastructure, and ensuring resilience to disasters.

The Department provides a coordinated comprehensive response in the event of a terrorist attack, natural disaster or other large scale emergency while working with Federal, state, local and private sector partners to ensure a swift and effective recovery effort.

The total fiscal year 2011 budget request for DHS, including fee funded and mandatory spending, is $56.3 billion, a two percent increase over the fiscal year 2010 enacted level.

The Department's fiscal year 2011 net discretionary or appropriated funding request is $43.6 billion, an increase of three percent over the fiscal year 2010 enacted level.

Some highlights of the fiscal year 2011 budget request pertaining to the five main mission areas are as follows: to prevent terrorism and enhance security, the DHS budget request includes an additional $214.7 million to put in place 500 more advance imaging technology machines at airport check points to detect dangerous materials, including non-metallic materials. Combined with the 500 deployments that are already planned through 2010, this appropriation will place this

technology in 75 percent of the country's largest airports. This budget also includes an additional $218.9 million for personnel to operate those machines.

The request also includes an increase of $85 million for additional Federal air marshals to increase international flight coverage, an increase of $60 million to purchase approximately 800 additional explosive trace detection machines, and a $71 million increase to fund an additional 275 explosive detection K-9 teams at airline check points.

To secure and manage our borders, the proposed budget fully funds the existing cadre of approximately 20,000 Border Patrol agents. This budget also asks for $44.8 million to maintain staffing levels for Customs and Border Patrol officers within the Office of Field Operations.

This budget includes $10 million in additional funding to expand the Border Enforcement Security Task Force model that has played an important role in increasing seizures of contraband in every major category last year.

Additionally, a total of $1.4 billion is requested to recapitalize the Coast Guard's aging fleet. This is a step we have to take in order to secure our country's vast maritime borders into the future.

This budget also strengthens last year's successes in the area of enforcing and administering our immigration laws. A total of $103.4 million is requested to strengthen the E-verify program, a critical tool to ensure a legal workforce. This funding will provide resources to move forward with important improvements already planned for the E-verify program and its online system.

Total funding of $146.9 million is also requested to continue the expansion of the secured community program which focuses enforcement efforts on aliens already incarcerated in state prisons and local jails. This program is the cornerstone of our efforts to keep criminal aliens off the streets and remove them from the country.

To safeguard and secure cyber space, we requested $379 million to develop the National Cyber Security Division, which will work both within the dot.gov and dot.com domains, to limit our vulnerabilities to attacks and to mitigate the damage of any attacks.

To ensure resilience to disasters, the Department seeks funding of $1.95 billion, an increase of $350 million for the Disaster Relief Fund. Total funding of $100 million is requested for pre-disaster mitigation, grant support and technical assistance to state, local and tribal governments, to reduce the risks associated with disasters.

A total of $194 million is requested to modernize flood maps and communicate flood hazard risks.

All these efforts depend on maturing and strengthening the DHS enterprise. A critical step in this process is consolidating the Department's headquarters at the St. Elizabeth's campus. This budget contains $287.8 million for that purpose.

Finally, a total of $4 billion is requested for grant programs to support our nation's first responders.

At this time, we will be happy to take questions from you on the budget.

Moderator: Thank you. At this time, if you would like to ask a question, you may do so by pressing "*" and "1" on your touchtone phone. "*" and "2" will withdraw your name from the list. Again, pressing "*" and "1" allows you to ask a question, and "*" then "2" withdraws your question. Please wait a moment while we hold for questions.

Moderator: The first question comes from Eileen Sullivan with AP.

Moderator: Hi. I was wondering if you could talk about whether there is a reduction called for the Coast Guard active duty members, and if so, how much of a reduction, and also if you could talk about the reduction in Border Patrol agents by 180 or whatever the number is?

DHS Official: The Coast Guard active duty reduction is slightly over 1,100 people.

Question: How do you justify that?

DHS Official: As was stated, recapitalization is a critical element of the future of the Coast Guard. We have several assets that were scheduled for de-commissioning, as we are bringing new assets on line as part of the Deep Water Acquisition Program.

In addition, we are looking to reorganize and restructure certain elements of the Coast Guard to create greater efficiency, and there are obviously tradeoffs made as part of that to ensure we could continue to recapitalize the Coast Guard.

Question: Okay. And the Border Patrol?

DHS Official: Yes, the budget includes an 180 personnel reduction for Border Patrol, as you mentioned, and the explanation there or the thinking behind that is we do not believe the 180 personnel reduction will in any way reduce the overall operating effectiveness of the Border Patrol because over the past five years, the Border Patrol has doubled in size. A lot of the agent workforce, the substantial portion of it, has only a couple of years experience. As they become more seasoned and more mature in their jobs, their effectiveness will increase, and because we are not doing the extensive hiring of 2,000 to 3,000 new agents a year, we can afford to put less into training improvement because obviously with this budget we are really only looking at maintaining the current workforce.

Question: How will the positions be reduced? Is it by attrition?

DHS Official: Yes. Each year, the Border Patrol staff is somewhere on the order of 1,500 to 1,700 agents per year who leave because of retirement or just otherwise leave the service. That 180 reduction is well within the amount that would typically leave during the course of a year. We will just fill a few less positions next year.

Question: Okay. Thanks.

Mr. Whithorne: Thanks, Eileen. The next question comes from Tom Frank with USA Today.

Question: Thanks. A question about the body scanners. First, what is the number of CAT-X airports?

DHS Official: Twenty-eight.

Question: You had mentioned the total deployments will be 1,000. I just wanted to see where you are getting that number. When you talk about 50 deployments planned for 2010, you are talking about the 40 that are presently in airports plus 450 to be deployed this year, that would bring you to 490 or roughly 500?

DHS Official: That's correct.

Question: The budget briefing talks about having AIT coverage at 75 percent of the CAT-X airports and then 60 percent of the total lanes at the CAT-X-II airports. Why would you be putting these machines in CAT-II airports but not in 25 percent of the CAT-X airports?

DHS Official: I think the decisions on final deployment take into account the fact that anybody entering into an airport is entering into the total aviation security system.

Question: As I understand CAT-X, that is by definition the highest risk. I would think you would want to have these machines in all the CAT-X airports before you go down to CAT-I and CAT-II.

DHS Official: The highest risk plus largest. As we know, once you enter the sterile area in the airport, you're in the system.

Question: Do you know what the total number of lanes is in the CAT-X through CAT-II airports?

DHS Official: I do not have that total number.

Mr. Whithorne: We will follow up with you after the call. I will ask you to limit your questions to one question per caller since we have a lot of folks to get to.

Question: That was one very important question. Just kidding. Go ahead.

Moderator: The next question comes from Mickey McCarter from Homeland Security Today.

Question: There was a lot of talk last year about actually proposing cuts in the DHS budget this year and in future years. I'm kind of thinking some of the reasons that didn't happen is the Christmas Day bombing attempt.

Is anybody talking about proposed budget cuts in future years if not this year?

DHS Official: The out years for the President's budget for DHS grow at roughly the rate of inflation.

Question: There had been talk as recently as November, I believe, of putting in a budget that was going to be a little less this year. I guess I'm wondering was there any reversal on that in recent months?

DHS Official: As part of the budget process, we examined different scenarios and options. Those are discussions that are

internal to the Administration and what you see in the budget release today is the end product of all those budget deliberations, which is a three percent increase for fiscal year 2011 and continues roughly modest growth roughly at the rate of inflation in the outer years.

Question: Okay. Thanks.

Mr. Whithorne: The next question comes from Rob Margatta from Professional Quarterly.

Question: Hi. I was just wondering, given the number of people in acting positions, there has been criticism from Congress that without permanent leadership, DHS is going to have a lot of trouble determining budget priorities and operations priorities.

I was wondering how DHS is looking at that with this budget with some key positions still unfilled.

DHS Official: This is something that the Administration, the former Administration as well as this one has made a very top priority. We have had many of the people who were in an acting position positioned in order to be able to develop this budget based on the current Administration's priorities. This was something that we planned for several years.

Question: Thank you.

Mr. Whithorne: Thank you. The next question comes from Joan Turro from Government Executive Magazine.

Question: Hi. I was actually hoping to get a clarification on the Border initiatives. It appears from the actual budget numbers that effort was going to see about a 25 percent cut in funding, from $800 million to $574 million, approximately.

I was hoping perhaps to get a clarification on those cuts, on where cuts are being made and whether I'm reading that correctly.

DHS Official: You are reading that correctly. There is no reduction to the secure Border initiative funding. It basically comes about because the deployment roll out schedule for the project is taking longer than anticipated. The Secretary also recently announced a review of that program.

The funding that was originally programmed into the fiscal year 2011 baseline that is being reduced puts forth further deployments in different geographic areas along the Border, assuming it is rolling along the previously projected path. The funding, what is in there, continues what we call block one of the project, basically future releases are not funded in this budget.

Question: The future remains to be seen?

DHS Official: Yes. I think when the Secretary announced her review, she indicated she was going to take a look at the status of the project and where it was ultimately going to go, and I think the reduction reflects that.

Question: Thanks.

Mr. Whithorne: Thank you. The next question comes from Russell Rommer from AOL News.

Question: Hi. Thanks for having the call. I was wondering if you could talk about the state and city grant programs, specifically if you are asking for any other funding, and whether that is an increase or a decrease from previous years? This is always a big issue in New York, Chicago and L.A., and there has also been questions about the funding formula and whether it's spread too thin across the country.

Can you talk about whether there will be any changes to that?

DHS Official: Let me take those two separately. On the state programs for this year, you will notice we have bumped that up by $100 million. The plan is also to consolidate some of the smaller programs into that pot. One of the things we have heard for many years -- many of the things, for example, that were eligible under the Citizen Corps or the NMRS are eligible under the state program anyway.

Our consolidation of these programs allows the states and territories to really have more flexibility on what they want to fund. Again, we are increasing the money by $100 million and also giving them some flexibility on how they spend that.

Question: Is that consolidated -- what is the umbrella sort of name for it now?

DHS Official: The name is the same, it is still the state homeland security program, so for example, under the state

homeland security program, you can use it for Citizen Corps activities. That used to be a separate grant program. You can do metropolitan medical responses or medical planning, mass fatalities management. You can do that under the state program.

Again, this idea that we have heard from stakeholders of consolidating on the state level, those activities are under a larger umbrella program.

On the other program, that is a very targeted program that seeks to protect the highest risk cities. We are adding additional funding in that pot this year as well. As you probably know, the list changes from year to year. It's unclear who will participate in that for 2011, but certainly the Department seeks to use that for their highest risk cities across the nation.

Many of the same activities that I mentioned in the state program are also allowable there. For example, you can do metropolitan medical responses and planning there. You can do Citizen Corps activities.

In both of those programs, again, we have added additional money, and for the state one in particular, we really fought to consolidate that to give the states more flexibility.

Question: How much was the additional funding? You said $100 million for the state.

DHS Official: It was increased by $213 million this year over last year.

Question: Okay; great. Thank you.

Moderator: Thank you. The next question is from Stu Leggeson from National Defense Magazine.

Question: Hi. I was hoping you could give me some details of the National Cyber Security Center, where is that going to be, when is that going to get up and running, and how is it different from what you are already doing.

DHS Official: The National Cyber Security Center is still in its infancy. There is $5 million -- there is an increase of $5 million in the fiscal year 2011 budget. Right now, the Director of the National Cyber Security Center is the Deputy Under Secretary for the National Protection of Programs Directorate, that's Phil Rodner.

It is proposed that it will increase its staffing to 40 people in the coming fiscal year 2011 year, and it is developing its knowledge on line basis and its procedures in order to integrate with the other cyber centers through the Federal Government.

Question: The amount for this year was only $5 million?

DHS Official: $5 million. The amount for 2011 is $10 million.

Question: That will be located where?

DHS Official: Currently, it is going to be located at the Glebe Watch Center.

Question: Okay. Thank you.

Moderator: Thank you. The next question comes from Chris Strom with Congress Daily.

Question: Hi. I'm wondering about the $200 million for the 9/11 trials, for security. Obviously, Mayor Bloomberg has said if it's going to be done in New York, the cost could be $1 billion. Are you all considering any kind of a contingency in which the amount of money that would have to be available would be increased, and how would that money -- I know it's under UASCI, how would that money actually be distributed to -- would people apply for it and then have to go through a complication in order to get access to that money?

DHS Official: As with any grant program, folks always have to apply and make known their intentions for that money. That is something we do in all of our programs. We envision the same thing with this money. We feel that $200 million is an appropriate amount, even though it's in the UASCI program, of course, that money goes to the state as well, so there is flexibility, and again, we feel that we wanted to put something in the budget for that and we have a mechanism to make that grant, so we will use those mechanisms that we already have.

Question: As far as the estimates for the security of the trials that it could be $1 billion, how do you reconcile the difference in the estimate?

DHS Official: Again, I think if you went to any person on any given day, you would get a different estimate. The Department took a look at it and we think the $200 million is really our best estimate of the costs.

Question: Just on the whole body scanners at the airports, are these scanners going to be put in primary screening and will they be mandatory?

DHS Official: The final decision on other places has not been made. I think the intention is principally in primary, but there is no final decision. Right now, the process is that if you are directed to an AIT, you have an option of going through a walk through metal detector and having a full pat down.

Question: Okay. Thanks.

Moderator: Thank you. The next question comes from Jeff Bliss with Bloomberg News.

Question: Hi. I just wanted to double check, there is a restriction saying CBP funding can't be used to prevent people from re-importing drugs from Canada. I just wanted to double check. Is that something you guys have been doing over the years or is this a change just for this year?

DHS Official: I believe that's been in past appropriation language in the general provision. I don't believe that is new language this year.

Question: Okay. That's what I assumed. I just wanted to double check. Thank you.

Moderator: The next question comes from Secretary of Defense Daily.

Question: Hi. If you could break out the TSA funding a little more by line here. I see the AIT money and the ETD money. Could you give us like x-ray and explosive detection systems for checked baggage and that ETD money, is that liquid scanners, is that hand held devices or is that the traditional bench top explosive detectors? Any comment will be appreciated. Thanks.

DHS Official: On the ETD, actually, I think we are looking at a portable ETD, which is different slightly. I don't have the information immediately available --

Question: You were cutting out there, sir. You don't have the information available on checked baggage?

DHS Official: The amount in the 2011 budget for EDS equipment for the checked baggage is $374 million.

Question: How about --

DHS Official: I don't have that one broken out separately.

Question: That portable EDT the gentleman is referring to, he said that is different. Is that something TSA is currently buying or is that going to be a new procurement?

DHS Official: I believe that's a new procurement.

Question: Okay; appreciate that.

Moderator: Thank you. The next question comes from Paul Kirby with TR Daily.

Question: You answered the question I was going to ask about the interoperability funds and other programs. I guess I have one other question. In looking at the state and local money, you are asking for $4 billion, the budget indicates that the current fiscal year is $3.015, but the Congress when they passed their conference report said it was $4.17 billion.

Are you guys saying this is an increase from the current fiscal year, what you're asking for for state and local grant programs or a reduction?

DHS Official: A net reduction of $164 million.

Question: Thank you.

Moderator: The next question is from Logan Young.

Question: Hello. Thank you very much for taking my question. The money you are requesting for immigration related

verification programs, how much will specifically go to community --

DHS Official: $103 million would go to verify and $34 million is targeted -- some of that $34 million could be used for the verify programs as well.

Question: Thank you.

Moderator: We have a question from Matt Coray from Congressional Quarterly.

Question: Hi. I have a question on the obligated funds. I see there grants have decreased substantially. I was wondering about the justification for that.

My other question relates to the other funds within FEMA, for example, the pre-disaster mitigation fund would be decreased by about $100 million, emergency food and shelter also of $100 million. That is about a third of that budget. Disaster relief by about $670 million. Management itself for FEMA also has a proposed reduction of about $124 million. I was just wondering what some of the rationale is for some of these proposed reductions.

DHS Official: Yes. Let me take the AFG one. Our ask this year is $610 million, which is down I think $200 million from enacted. Again, when we look at the grant numbers, we do have the stakeholders first of all, and in talking with the fire service community, that number was where they thought we should be at frankly, and also there is a fair amount of money in the pipeline already with 2009 and also some of the 2010 grants that we are just now starting to make.

In terms of the job bill, nothing has been passed on that. We are certainly aware of some possible funding for SAFER, half a billion dollars, that could be coming down the pike as well. Again, that hasn't been passed so that wasn't necessarily taken into consideration.

We do feel like the number of 610 is appropriate, again given where the communities feel they are and the money that will be granted for the 2010 cycle.

Question: Okay.

DHS Official: With regard to the FEMA budget at large, the Federal budget this year, the proposal was $10.5 billion relative to $10.359 enacted last year. Pretty much level from last year. To get to some of those specific appropriations you mentioned, starting with the Disaster Relief Fund, the amount appropriated last year was $1.6 billion, but what we are requesting in fiscal year 2011 is actually higher than that. It is $1.95 billion with an increase of about $350 million.

For management and administration, that one was enacted last year at $797,650,000, and what is not reflected there is the transfer from the DRF, but this year we are reflecting $902 million. It is pretty much the same amount. Actually, there is a slight increase in there for facilities of about $23 million. There is no reduction there.

You also mentioned PDM, that one last year was enacted at $100 million and what we are proposing for 2011 is $100 million as well.

Question: Okay. Great. Thanks very much.

Moderator: Thank you. We have a follow up question from Defense Daily.

Question: Hi. I guess this would maybe be for Peggy. Along the lines of the acquisition reform, I guess, the Administration has been moving towards more in sourcing, and I wonder if that trend will continue with fiscal year 2011, and I think the Secretary said we will see more of that in fiscal year 2011 than before just because you have been gaining momentum there.

Could you provide any color or more specific metrics along those lines about what we can expect to see in fiscal year 2011 regarding more moving to Government work versus Federal contract work, and also, sort of how things are changing in the fixed price versus cost plus contract environment in fiscal year 2011.

Ms. Sherry: In terms of re-balancing the workforce, there are multiple areas in the DHS budget in 2011 where we are doing workforce balancing, and that is bringing more Feds on board to do work that today is done by contractors.

Question: Do you have an example?

Ms. Sherry: You have heard about our major initiative in cyber security where we are hiring substantial numbers of people. A significant number of those hire's will be performing work currently performed by contractors. Also, in our analysis and operations activity, we have a major increase in the number of Feds doing intelligence type work. Those are

two big examples.

Question: I know DHS is talking about having to better define requirements in order to move more of its contracting to fixed price versus cost plus, if you are able to enlighten us on what's going on there and what progress is being made, that would be helpful.

Ms. Sherry: There is no specific initiatives in the budget for that. As you noticed, we have an initiative to enhance the acquisition workforce across the Department. I think we'd have to get back to you in terms of specific acquisition plans, where we are transitioning from one type of contract to another.

Question: Thanks.

Mr. Whithorne: There are no more questions at the present time. I appreciate you guys taking the time, and we will conclude the conference call.

###

This page was last reviewed/modified on February 1, 2010.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Aviation Security

Fiscal Year 2011
Congressional Justification

AR 001135

Department of Homeland Security
Transportation Security Administration
Aviation Security
Checkpoint Support
Program Performance Justification
(Dollars in Thousands)

PPA: Checkpoint Support

	Perm Pos	FTE	Amount
2009 Actuals	**41**	**35**	**$160,817**
2010 Enacted	**41**	**40**	**128,739**
2011 Adjustments-to-Base	15	14	87
2011 Current Services	**56**	**54**	**128,826**
2011 Program Change	10	5	231,200
2011 Total Request	**66**	**59**	**360,026**
Total Change 2010-2011	25	19	231,287

*FY 2009 Actuals include American Recovery and Reinvestment Act (ARRA) funds.

The Transportation Security Administration requests $360.0 million for Checkpoint Support activities. This is an increase of $231.3 million over FY 2010 for technologies for explosives detection at airport checkpoints. An adjustment-to-base increase of 15 FTP and $87 thousand reflect positions to support the American Recovery and Reinvestment Act (ARRA) in addition to a program change of 10 FTP.

CURRENT SERVICES PROGRAM DESCRIPTION

The following table provides the components of this PPA.

(dollars in millions)

	FY 2010	FY 2011
Checkpoint Technology	$117.3	$344.1
Advanced Surveillance Program	6.0	6.0
Payroll	5.4	9.9
Total	**$128.7**	**$360.0**

The checkpoint support program provides the resources required to test, evaluate, integrate, and deploy passenger screening and carry-on baggage screening capabilities. This involves technologies, training, checkpoint reconfigurations, closed circuit television surveillance equipment, operational integration of systems, and safety and optimization services at approximately 2,225 passenger checkpoint lanes in our Nation's airports. TSA developed a strategic plan to enhance screening through improved checkpoint technology which will refine passenger security for aviation. This initiative extends beyond the airport checkpoint and considers the end-to-end passenger experience to improve security and increase efficiency. Focus is on three key elements: improved explosives detection, enhanced hostile intent detection, and extended presence in the passenger journey.

AR 001136

Current technologies that have been deployed include Threat Image Protection (TIP) Ready X-Ray machines (TRX); enhanced walk-through metal detectors (WTMD) that screen persons for metallic weapons such as guns or knives; explosives trace detectors (ETD), which are used to test for explosive residue on selected carry-on items or can be used as a portable device that allows for increased security and an added layer of random screening within the sterile area; bottle liquids scanners (BLS), which screen bottles to determine if they contain explosives or benign liquids; Credential Authentication Technology (CAT), which is used to verify a passenger's travel documents; Automatic Wait Time (AWT) technology, which allows the TSA to monitor wait times at checkpoints; Chemical Analysis Devices (CAD), which are small devices used to identify suspect substances; advanced imaging technology (AIT) consisting of millimeter wave, backscatter x-ray, and other technologies capable of providing images of threat objects on a person's body; and Advanced Technology systems (AT), which are X-ray systems with advanced visual detection capabilities, using multi-view capabilities or automated explosives detection capabilities.

The TSA received ARRA funding to be used at the checkpoint in order to procure and install checkpoint explosives detection equipment. The TSA will use these funds to accelerate the large scale deployment of AT systems, Universal Conveyor Systems (UCS), BLS, AIT, CAT, CAD, and Next Generation Explosive Trace Detectors (NextGen ETDs). By the end of FY 2010, enough AT and BLS will be procured to complete the current nationwide requirements of these systems. ARRA procurements of AIT, UCS, CAT, CAD and NextGen ETD will provide a significant percentage of coverage toward full operating capability of these systems.

FY 2009 significant accomplishments include:

- Conducted Lab Testing on Advanced Technology X-ray systems (AT2) manufactured by 3 vendors, AIT systems from 2 vendors, BLS from 5 vendors, and 1 NextGen ETD vendor.
- Conducted Operational Testing on AIT systems manufactured by 2 vendors, BLS from 2 vendors, and 1 NextGen ETD vendor.
- Procured 44 AT Systems; 400 NextGen ETD; 150 AIT, 500 BLS.
- Deployed 512 AT, 12 AIT, and 89 ETD.

FY 2010 planned accomplishments include:

- Establish a Qualified Products List for AT2 with increased liquids detection capabilities;
- Achieve full operating capability (FOC) for BLS;
- Procure and deploy Credential Authentication Technology/Boarding Pass Scanning Systems (CAT-BPSS);
- Conduct laboratory and operational testing and evaluation for AWT and Shoe Scanner Devices (SSD); and
- Conduct test and evaluation (T&E) support for AT Carry-on Screening, AIT, BLS and NextGen ETD systems, Security Technology Integrated Program (STIP), CAT-BPSS, SSD, and Enhanced Metal Detection (EMD).

FY 2011 planned accomplishments include:

- Continue procurement and deployment for AIT and AWT;
- Continue modifications to the CAT-BPSS to provide ID verification capabilities for law enforcement, airline and airport IDs;
- Procure and deploy SSD that will allow passengers to avoid the inconvenience of removing their shoes for security screening;
- Procure and deploy Portable ETD that will allow for the increased security and an added layer of random screening within the sterile area;
- Continue evaluation and modification of AT2 systems to increase detection capabilities to allow liquids and laptops to remain in carry-on bags for screening;

- Continue evaluation and modification of AIT to provide automated detection capabilities to increase throughput and further remove operator subjectivity from the security decision process. Assessments will continue on new technologies in support of the checkpoint area, as well as enhancing existing T&E capabilities. TSA will also continue to evaluate technologies planned for checkpoint, improvements to existing screening technologies, and products emerging from DHS Science and Technology's R&D program; and
- Establish a new set of technology qualification groups based on Innovative Technology Review Process (ITRP) data and information on next generation technologies to include:
    - Emerging spectrum-based inspection technologies;
    - Advanced EMD including echo-imaging; and
    - Next generation x-ray based systems.

Checkpoint Technology: $344.1 million: This request includes $344.1 million to test, procure and deploy improved technology systems to further extend explosives and prohibited item detection coverage at aviation checkpoints. It includes funding to test, purchase, and install new screening equipment and update existing equipment. Funds will also be used for program, engineering, technical support and travel, original equipment manufacturer training, warehousing, consumables, and refurbishing equipment, to provide functionality and performance enhancements, as well as for life-cycle replacements for units reaching the end of their useful life.

TSA analyzes integration of new and modified systems and concepts of operation to ensure operational effectiveness and suitability prior to full system production and deployment. The purpose of this work is to test, evaluate, and analyze pre-production or production representative systems under realistic conditions, including operation by those who will use the equipment under the proposed concept of operations, in the field under a variety of environmental conditions. In particular, this includes:

- Operational test and evaluation as part of the acquisition process for items procured by TSA, including Early Utility Assessments, Initial Operational Test and Evaluation, and Follow-on Operational Test and Evaluation over the project lifecycle;
- Operational test and evaluation in support of regulatory and policy decisions;
- Pilots, concept demonstrations, and field experimentation in support of mission area analyses, concept of operations development, process optimization and improvement, and workforce / vector characterizations; and
- Testing and evaluation capabilities development, to improve the quality and utility of evaluation products.

Equipment purchases may include AT, AIT, AWT, BLS, CPI, SSD, CAT, CAD, NextGen ETD, technology integration solutions, and additional units or upgrades to legacy equipment. This equipment will enable TSA to detect a greater range of threats more quickly and with greater accuracy than existing equipment. TSA will be deploying additional AIT systems that will build off current capabilities such as auto detection algorithms, networking and multiplexing.

This effort will also incorporate, as appropriate, alternative configurations that improve security and throughput while reducing congestion at "soft target" locations like airport lobbies. These enhancements may include remote screening centers, improved divestiture and reorganization zones, or special lanes for no/single carry-on baggage. Funds will also be used for the movement of equipment, small scale construction, and to purchase any ancillary equipment such as roller tables, lift carts, and fatigue mats needed for a particular project.

AR 001138

Advanced Technology[1]	2325	1561	67%	639	95%	0	95%	25	96%	*2225*
Universal Conveyor System	2325	0	0%	0	0%	75	3%	35	5%	*110*
Advanced Imaging Technology	1800	132	7%	365	28%	0	28%	503	56%	*1000*
Credential Authentication Technology	2325	500	22%	0	22%	800	56%	600	82%	*1900*
Bottled Liquids Scanner	1300	680	52%	500	91%	120	100%	0	100%	*1300*
NextGen Explosives Trace Detector	1500	100	7%	600	47%	100	53%	35	56%	*835*
Portable Explosives Trace Detector	811	0	0%	0	0%	0	0%	811	100%	*811*
Chemical Analysis Device	140	0	0%	140	100%	0	100%	0	100%	*140*
Enhanced Metal Detector - 2	1875	0	0%	0	0%	125	7%	50	9%	*175*
Shoe Scanning Device	2325	0	0%	0	0%	50	2%	50	4%	*100*
Automated Wait Times	470	0	0%	0	0%	225	48%	245	100%	*470*

[1] Percentage of FOC based on FY14 estimates. Current nationwide requirements are being met.

FEB 2 4 2010

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

Transportation Security Administration

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

Dear Chairman Thompson:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The above include both Federal employees and government contractors.

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

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

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

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

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

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

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

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

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

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

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

Sincerely yours,

Gale D. Rossides
Acting Administrator

FOR FRONT OFFICE USE ONLY – DO NOT DUPLICATE

TSA CONTROL NUMBER	TSA-100122-022 DHS OLA 854106 THOMPSON	ORIGINATING OFFICE: OST/PSP WRITER: N. Moses PHONE: x71470 DUE DATE: 2/5/10

Transportation Security Administration

☐	Action Memo	☐	DHS SOL
☐	Information Memo	☒	DHS Congressional
☐	QFR	☐	TSA Congressional
☐	Report to Congress	☐	Other:

TSA Executive Level Clearance Sheet

AA Approvals:	Date:	SUBJECT:
1.R. Kane, OPT/CTO, x71096	2/4/10	100.1 --DHS Correspondence -- COORDINATE w/ PRIVACY: Chairman Thompson writes regarding privacy concerns that have been raised about TSA's Advanced Imaging Technology, and its capability to store, print, record, and export images.
2.		
3.		

OFFICE OF THE EXECUTIVE SECRETARIAT PREPARATION

Title	ES Editor	Date	Approve	Approve w/ edits	Reject	Comments
IMS	Christine Jemerson	2/4/2010	☒	☐	☐	Folder to J. Wright for dist to writer/editor
W/E	Michael Rogan	2/4	☐	☐	☐	to Bill
Sr. W/E	Bill Ryan	2/4	☐	☑	☐	Ahead → OLA

OFFICE OF THE EXECUTIVE SECRETARIAT APPROVAL

To: OLA	Michael Rogan	2/4	☐	☐	☐	
To: FO	David Ortiz	2/17	☐	☐	☐	

CLEARANCE

Review Requested?			Action Taken						
Check all Needed	Reviewer	Office	Initials	Date	Approve	Approve w/ edits	Reject	Use Autopen	Comments
☒	LaVita LeGrys	OLA	JW	2/17	☐	☒	☐	N/A	
☒	Francine Kerner	OCC	FK	2/17	☐	☒	☐	N/A	See email
☐	Kim Walton	OSC			☐	☐	☐	N/A	
☐	Art Macias	Chief of Staff			☐	☐	☐	N/A	
☒	Peter Pietra	Privacy	PP	2/17	☒	☐	☐	N/A	See email

MW: ~~ok~~ OS. 2/22/10

APPROVAL

☒	Keith Kauffman	Acting Deputy Administrator			☐	☐	☐	N/A	
☒	Gale D. Rossides	Acting Administrator	GDR		☐	☐	☐	☐	

2/22/10 Cork Did the chg get made Yrequeste

AR 001143

FOR FRONT OFFICE USE ONLY – DO NOT DUPLICATE

TRANSPORTATION SECURITY ADMINISTRATION

TSA CLEARANCE SHEET

ORIGINATOR			
Nina Moses, OST/PSP - 71470			
DOCUMENT FOR ACTION	**OFFICE**	**PHONE**	**DATE**
☐ Action Memo ☐ Letter ☐ Info Memo ☐ Other	OST		02/04/10

SUBJECT: 100.1 -DHS Correspondence - COORDINATE w/ PRIVACY: Chairman Thompson writes regarding privacy concerns that have been raised about TSA's Advanced Imaging Technology, and its capability to store, print, record, and export images.

TSA CONTROL NUMBER: TSA-100122-022

ACTION REQUIRED

REVIEWERS		OFFICE	DIRECT PHONE NO.	INITIAL	DATE	CORRECTION REQUIRED
1.	Peter Pietra, Privacy Office - 73654Maurine Fanguy, OPT/Chief of Staff - 73741Robin Kane, OPT/CTO - AA - 71096					
2.						
3.	Robin Kane					
4.	Maurine Fanguy -CoS	OPT/CTO		/s/	2-18-10	see email
5.						
6.						

EXECUTIVE SECRETARIAT		INITIAL	DATE	CORRECTION REQUESTED
Logging				
Review				
OFFICE OF THE ADMINISTRATOR		**INITIAL**	**DATE**	**CORRECTION REQUESTED**
1.				
2.				
3.				
4.				
5.				

Explanation, Special Instructions, Comments:

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Eleventh Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

January 21, 2010

Gail Rossides
Acting Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Ms. Rossides,

It has come to the Committee's attention that the Transportation Security Administration's (TSA's) Advanced Imaging Technology (AIT), a form of whole body scanning, has the ability to store, print, record, and export images.

According to procurement specifications for AIT, the machines are required to have the ability to store and export images during testing and training. Additionally, the procurement specifications allow for the storage and transfer of images through Universal Serial Bus (USB) devices. The machines also allow for certain users—designated as Level Z—to disable privacy protections, save images, enable image filters, and modify user access levels.[1]

Yet, TSA has repeatedly stated to Congress and the public that screening images obtained by AIT will not be stored, exported, or printed. This apparent contradiction between the procurement specifications for AIT and the stated policy positions of TSA should be resolved as TSA moves forward with expanding the use of AIT. The public needs assurance that AIT deployed at airports will not have the ability to store, print, record, and export images obtained through AIT screenings.

In an effort to ensure the safety of the flying public, technological advancements can certainly be of assistance. However, we must ensure that the use of technology does not erode individual privacy protections. As TSA continues to evolve its screening procedures, it is imperative that it safeguard constitutionally protected privacy principles.

To that end, please provide responses to the following:

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

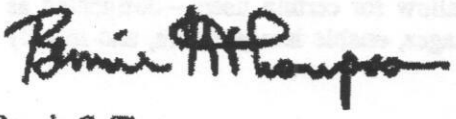
[1] TSA Procedural Specifications Document, p. C-1, Figure 1.

TSA-10012-0022

2) What is the extent of the ability AIT to store and transmit data?
3) Provide the titles of the employees who have the authority to place the machines in test mode and the number of employees that fall into this category.
4) Under what circumstances, if any, can AIT machines be entered into test mode in the airport setting?[2]
5) Who at TSA is authorized as a Level Z user? Please provide the titles of these employees and state if any government contractors or any other non-TSA officials are Level Z users. Also, provide the number of employees and or contractors that have this designation.
6) What are the details of the privacy filters built into the AIT?
7) Has TSA asked the Chief Privacy Officer to amend or update the current Privacy Impact Assessment to reflect the storage capability of AIT and identify the individuals who have this authority?
8) What protections does the AIT have that will prevent people outside of TSA from obtaining image data through the device's USB and Ethernet capabilities?

Pursuant to Rule X (3) (g) and Rule XI of the Rules of the House of Representatives, please respond in writing by February 1, 2010. If you have any questions, feel free to contact Cherri Branson, Chief Oversight Counsel, at 226-2616.

Sincerely,



Bennie G. Thompson
Chairman

CC: Mary Ellen Callahan, Chief Privacy Officer

[2] TSA Procedural Specifications Document, p. 5, Figure 3.

Statement for the Record

The Honorable Janet Napolitano

Secretary
United States Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs

AR 001147

Mr. Chairman, Senator Collins, and Members of the Committee:

Let me begin by saying thank you for the strong support you have provided me and the Department this past year. I look forward to another year working with you to make certain that we have the right resources to protect the homeland and the American people and that we make the most effective and efficient use of those resources.

I am pleased to appear before the Committee today to present President Obama's Fiscal Year (FY) 2011 Budget Request for the Department of Homeland Security (DHS).

As you know, the attempted attack on Northwest Flight 253 on December 25 was a powerful illustration that terrorists will go to great lengths to try to defeat the security measures that have been put in place since September 11, 2001. This Administration is determined to thwart those plans and disrupt, dismantle and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This effort involves not just DHS, but also many other federal agencies as well as state, local, tribal, territorial, private sector and international partners. As President Obama has made clear, this Administration is determined to find and fix the vulnerabilities in our systems that allowed this breach to occur – and the FY 2011 Budget Request prioritizes these security enhancements.

The Department is also working hand-in-hand with our federal partners to respond to the devastation and loss of life in Haiti following the January 12 earthquake. Collaboration within DHS among our many components has allowed us to leverage unprecedented resources and personnel to assist with the humanitarian efforts in Haiti, once again demonstrating what these offices can accomplish together. The FY2011 Budget Request strengthens the ongoing work in each of our Department's offices to fulfill our unified mission.

I will now summarize the FY 2011 budget request along with some of our key accomplishments from last year.

FY 2011 BUDGET REQUEST

The FY 2011 DHS budget will strengthen efforts that are critical to the Nation's security, bolster the Department's ability to combat terrorism and respond to emergencies and potential threats, and allow DHS to tackle its responsibilities to protect the Nation and keep Americans safe.

DHS executes a wide array of responsibilities in its unified security mission. To bolster these efforts, DHS collaborates and coordinates with many partners—state, local and tribal governments and law enforcement agencies, international allies, the private sector and other federal departments. These partnerships are essential to DHS' ability to fulfill its security mission.

The FY 2011 budget continues efforts to use our resources as efficiently and effectively as possible. We must exercise strong fiscal discipline, making sure that we are investing our resources in what works, cutting down on redundancy, eliminating ineffective programs and making improvements across the board.

To institutionalize a culture of efficiency across the Department, DHS launched the Department-wide Efficiency Review Initiative in March 2009. One major element of the Efficiency Review is

the Balanced Workforce Strategy, a three-pronged approach to ensuring that the right workforce balance is achieved. First, we are taking steps to ensure that no inherently governmental functions are performed by contractors. Second, we put in place rigorous review procedures to ensure that future activities do not increase our reliance on contractors. Third, we are coordinating workforce assessments across the Department to seek economies and service improvements and reduce our reliance on contractors. In FY 2011, the Department will continue executing the Balanced Workforce Strategy by converting contractor positions to federal jobs.

DHS secures the United States against all threats through five main missions, each of which is strengthened by this budget:

- *Preventing Terrorism and Enhancing Security*: Guarding against terrorism was the founding mission of DHS and remains our top priority today. A key element of preventing terrorism is recognizing the evolving threats posed by violent extremists and taking action to ensure our defenses continue to evolve to deter and defeat them.
- *Securing and Managing Our Borders*: DHS monitors our air, land and sea borders to prevent illegal trafficking that threatens our country, while facilitating lawful travel and trade. We will continue to strengthen security efforts on the southwest border to combat and disrupt cartel violence and provide critical security upgrades—through infrastructure and technology—along the northern border.
- *Enforcing and Administering our Immigration Laws*: DHS is responsible for enforcing the Nation's immigration laws while streamlining and facilitating the legal immigration process. In FY 2011, we will continue to strengthen enforcement activities while targeting criminal aliens who pose a threat to public safety and employers who knowingly violate the law.
- *Safeguarding and Securing Cyberspace*: The Department defends against and responds to attacks on the cyber networks through which Americans communicate with each other, conduct business and manage infrastructure. DHS analyzes and reduces cyber threats and vulnerabilities, distributes threat warnings, coordinates the response to cyber incidents and works with the private sector and our state, local, international and private sector partners to ensure that our computers, networks and cyber systems remain safe.
- *Ensuring Resilience to Disasters*: The Department provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergencies while working with federal, state, local and private sector partners to ensure a swift and effective recovery effort. DHS will continue its increased efforts to build a ready and resilient nation by bolstering information sharing, providing grants and training to our homeland security and law enforcement partners and further streamlining rebuilding and recovery along the Gulf Coast.

Ensuring shared awareness of risks and threats, increasing resilience in communities and enhancing the use of science and technology underpin these national efforts to prevent terrorism, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace and ensure resilience to disasters.

The total FY 2011 budget request for DHS is $56.3 billion in total funding; a 2 percent increase over the FY 2010 enacted level. The Department's FY 2011 gross discretionary budget request[1] is $47.1 billion, an increase of 2 percent over the FY 2010 enacted level. The Department's FY 2011 net discretionary budget request is $43.6 billion,[2] an increase of 3 percent over the FY 2010 enacted level. For purposes of comparison the Overseas Contingency Operation funding and transfer from the National Science Foundation are not included in the FY 2010 enacted level.

The following are highlights of the FY 2011 Budget Request:

PREVENTING TERRORISM AND ENHANCING SECURITY

- *Advanced Imaging Technology (AIT)*: An increase of $214.7M is requested to procure and install 500 advanced imaging technology machines at airport checkpoints to detect dangerous materials, including non-metallic materials. This request, combined with units the Transportation Security Administration (TSA) plans to install in 2010, will mean that 1,000 AIT scanners, will total AIT coverage at 75 percent of Category X airports and 60 percent of the total lanes at Category X through II airports.
- *Transportation Security Officers (TSOs) to Staff AITs*: An increase of $218.9M is requested for additional Transportation Security Officers (TSOs), managers and associated support costs to operate additional AITs at airport checkpoints. Passenger screening is critical to detecting and preventing individuals carrying dangerous or deadly objects and materials from boarding planes.
- *Federal Air Marshals (FAMs)*: An increase of $85M is requested for additional FAMs to increase international flight coverage. FAMs help detect, deter and defeat terrorist and other criminal hostile acts targeting U.S. air carriers, airports, passengers and crew.
- *Portable Explosive Trace Detection (ETD)*: An increase of $60M is requested to purchase approximately 800 portable ETD machines ($39M) and associated checkpoint consumables ($21M).
- *Canine Teams*: An increase of $71M and 523 positions (262 Full-Time Equivalents, or FTE) is requested to fund an additional 275 proprietary explosives detection canine teams, 112 teams at 28 Category X airports and 163 teams at 56 Category I airports.
- *Behavior Detection Officers (BDOs)*: An increase of $20M and 350 BDOs (210 FTE) is requested to further enhance TSA's Screening Passengers by Observation Techniques program. The FY 2011 request includes a total of 3,350 officers to enhance coverage at

---

[1] Gross Discretionary funding does not include funding such as Coast Guard's retirement pay account and fees paid for immigration benefits

[2] This does not include fee collections such as funding for the Federal Protective Service (NPPD), aviation security passenger and carrier fees (TSA), credentialing fees (such as TWIC – TSA), and administrative costs of the National Flood Insurance Fund (FEMA).

lanes and shifts at high risk Category X and I airports and expand coverage to smaller airports.

- *Domestic Nuclear Detection Office Systems Engineering and Architecture*: An increase of $13.4M is requested to fund systems engineering efforts to address vulnerabilities in the Global Nuclear Detection Architecture, the multi-layered system of detection technologies, programs and guidelines designed to enhance the Nation's ability to detect and prevent a radiological or nuclear attack.

- *Radiological/Nuclear Detection Systems*: An increase of $41M is requested for the procurement and deployment of radiological and nuclear detection systems and equipment to support efforts across the Department.

- *Law Enforcement Detachment Teams*: An increase of $3.6M is requested to bring deployable U.S. Coast Guard Law Enforcement Detachment (LEDET) teams to full capacity. LEDETs help prevent terrorism, secure U.S. borders, disrupt criminal organizations and support counter drug missions overseas. In FY 2009, for example, LEDETs aboard U.S. naval and partner nation assets accounted for more than 50 percent of total maritime cocaine removals.

- *2012 Presidential Campaign*: Total funding of $14M is requested for startup costs associated with the 2012 Presidential Campaign including training for candidate/nominee protective detail personnel. The Secret Service will also begin to procure and pre-position equipment, services and supplies to support candidate/nominee protective operations throughout the country.

- *Secret Service Information Technology*: Total funding of $36M is requested for the Information Integration and Transformation program. This funding will allow the Secret Service to successfully continue its comprehensive Information Technology (IT) transformation and provide a multi-year, mission-integrated program to engineer a modernized, agile and strengthened IT infrastructure to support all aspects of the Secret Service's mission.

SECURING AND MANAGING OUR BORDERS

- *Journeyman Pay Increase*: In the spring of 2010, DHS will implement the journeyman pay increase, raising the journeyman grade level for frontline Customs and Border Protection (CBP) Officers (including Border Patrol agents and Agricultural Specialists) from GS-11 level to the GS-12 level. An adjustment to the base of $310.4M will fund the full-year impact of the salary and benefit requirements associated with this implementation

- *CBP Officers*: An increase of $44.8M is requested to fund 318 CBP Officer FTEs within the Office of Field Operations and 71 support FTEs for CBP. The decline in the number of passengers and conveyances entering the United States in FY 2009 resulted in an almost 8 percent decrease in revenues from inspection user fees. CBP, therefore, has fewer resources to maintain critical staffing levels for CBP officers. The proposed funding will

allow CBP to maintain staffing for critical positions to protect the United States at its ports of entry.

- *Border Enforcement Security Task Forces (BESTs)*: An additional $10M is requested to establish BESTs in three additional locations: Massena, NY; San Francisco, CA and Honolulu, HI. These multi-agency teams work to identify, disrupt and dismantle criminal organizations posing significant threats to border security, including terrorist groups, gang members, and criminal aliens.

- *Intellectual Property Rights (IPR) Enforcement*: An increase of $30M is requested to support CBP and ICE IPR enforcement efforts. This includes information technology systems that support IPR activities and implementation of the 5-year IPR Plan. An increase of $5M is also requested for the Immigration and Customs Enforcement (ICE)-led National Intellectual Property Rights Coordination Center (IPR Center). The IPR Center brings key U.S. government agencies together to combat IPR violations that threaten our economic stability, restrict the competitiveness of U.S. industry and endanger the public's health and safety. ICE will also use these funds to focus on disrupting criminal organizations through the internet and support for anti-counterfeiting efforts.

- *Intelligence Analysts*: An increase of $10M is requested to fund 103 Intelligence Analysts for CBP. This staffing increase will support 24/7 operations of CBP Intelligence Watch, Operations Coordination and the Commissioner's Situation Room.

- *Coast Guard Asset Recapitalization*: A total of $1.4B is requested to continue recapitalization of aging Coast Guard surface and air assets. Included in this request is $538M for production of the Coast Guard's fifth National Security Cutter to continue replacement of the 378-foot High Endurance Cutters fleet. Also included is $240M for production of four Fast Response Cutters to continue replacement of the 110-foot Class Patrol Boat fleet. The Fast Response Cutters have enhanced capability, high readiness, speed, and endurance, which will allow them to quickly and effectively respond to emerging threats. Additionally, $40M is requested to purchase one Maritime Patrol Aircraft (MPA) HC-144A. The HC-144A will address the Coast Guard's MPA flight hour gap by providing 1,200 hours every year per aircraft. Finally, $13.9M is requested for improvement and acquisition of housing to support military families.

ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

- *E-Verify*: A total of $103.4M and 338 FTEs is requested for the E-Verify Program. In FY 2011, U.S. Citizenship and Immigration Services (USCIS) will develop and implement an E-Verify portal that will provide a single-user interface for the program's products and services. In addition, USCIS will enhance E-Verify's monitoring and compliance activities through analytical capabilities that will support more robust fraud detection and improved analytic processes and will continue developing system enhancements in response to customer feedback, surveys, mission requirements and capacity needs.

- *Secure Communities*: Total funding of $146.9M is requested to continue FY 2010 progress toward nationwide implementation of ICE's Secure Communities program—which involves

the identification, apprehension and removal of all Level 1 criminal aliens in state prisons and local jails through criminal alien biometric identification capabilities. Secure Communities, in cooperation with federal, state and local law enforcement agencies, will provide a safeguard to American communities by removing those criminal aliens from the United States who represent the greatest threats to public safety and by deterring their re-entry through aggressive prosecution.

- *Immigrant Integration*: A total of $18M is requested to fund USCIS Office of Citizenship initiatives, including expansion of the competitive Citizenship Grant Program to support national and community-based organizations preparing immigrants for citizenship, promoting and raising awareness of citizenship rights and responsibilities, and enhancing English language education and other tools for legal permanent residents. The Office of Citizenship will support the implementation of the Immigration Integration program and lead initiatives to educate aspiring citizens about the naturalization process, monitor and evaluate the administration and content of the new naturalization test, and develop educational materials and resources for immigrants and the organizations that serve them.

SAFEGUARDING AND SECURING CYBERSPACE

- *National Cyber Security Division (NCSD)*: Total funding of $379M is requested for the NCSD to support the development of capabilities to prevent, prepare for and respond to incidents that could degrade or overwhelm the Nation's critical information technology infrastructure and key cyber networks. These funds will identify and reduce vulnerabilities, mitigate threats and ensure that cyber intrusions and disruptions cause minimal damage to public and private sector networks.

- *National Cyber Security Center (NCSC)*: A total of $10M is requested for the NCSC to enhance cyber security coordination capabilities across the Federal Government including mission integration, collaboration and coordination, situational awareness and cyber incident response, analysis and reporting, knowledge management, and technology development and management.

ENSURING RESILIENCE TO DISASTERS

- *Disaster Relief Fund (DRF)*: The budget seeks funding of $1.95B, an increase of $350M for the DRF. The DRF provides a significant portion of the total federal response to victims in declared major disasters and emergencies.

- *Federal Emergency Management Agency (FEMA) Facilities*: An additional $23.3M is requested to address critical FEMA real estate needs. By FY 2011, the capacity of FEMA facilities will be unable to accommodate key mission responsibilities and staff. FEMA also faces a critical need to maintain and repair aging and deteriorating national facilities. To address these needs, FEMA has developed a 5-year capital plan to begin critical regional facility acquisitions and repairs.

- *Pre-Disaster Mitigation Grants*: Total funding of $100M is requested to provide program support and technical assistance to state, local and tribal governments to reduce the risks

associated with disasters, support the national grant competition and provide the required $500,000 per state allocation. Resources will support the development and enhancement of hazard mitigation plans, as well as the implementation of pre-disaster mitigation projects.

- *Flood Map Modernization*: A total of $194M is requested to analyze and produce flood hazard data and map products and communicate flood hazard risk. The funding will support the review and update of flood hazard data and maps to accurately reflect flood hazards and monitor the validity of published flood hazard information.

- *Rescue 21*: A total of $36M is requested for the Rescue 21 system, enabling the U.S. Coast Guard to enhance preparedness, ensure efficient emergency response and rapidly recover from disasters. The Rescue 21 system replaces the U.S. Coast Guard's legacy National Distress and Response System and improves communications and command and control capabilities in the coastal zone. The system is the foundation for coastal Search and Rescue and enhances maritime situational awareness through increased communications ability with mariners and other responders.

MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

- *St. Elizabeths Headquarters Consolidation*: To streamline the Departments core operations, $287.8M is requested to consolidate executive leadership, operations coordination and policy and program management functions in a secure setting at St. Elizabeths. The Department's facilities are currently dispersed over more than 40 locations throughout the National Capital Region (NCR). This consolidation at St. Elizabeths will reduce the fragmentation of components and will improve communications, coordination and cooperation across all DHS headquarters organizations.

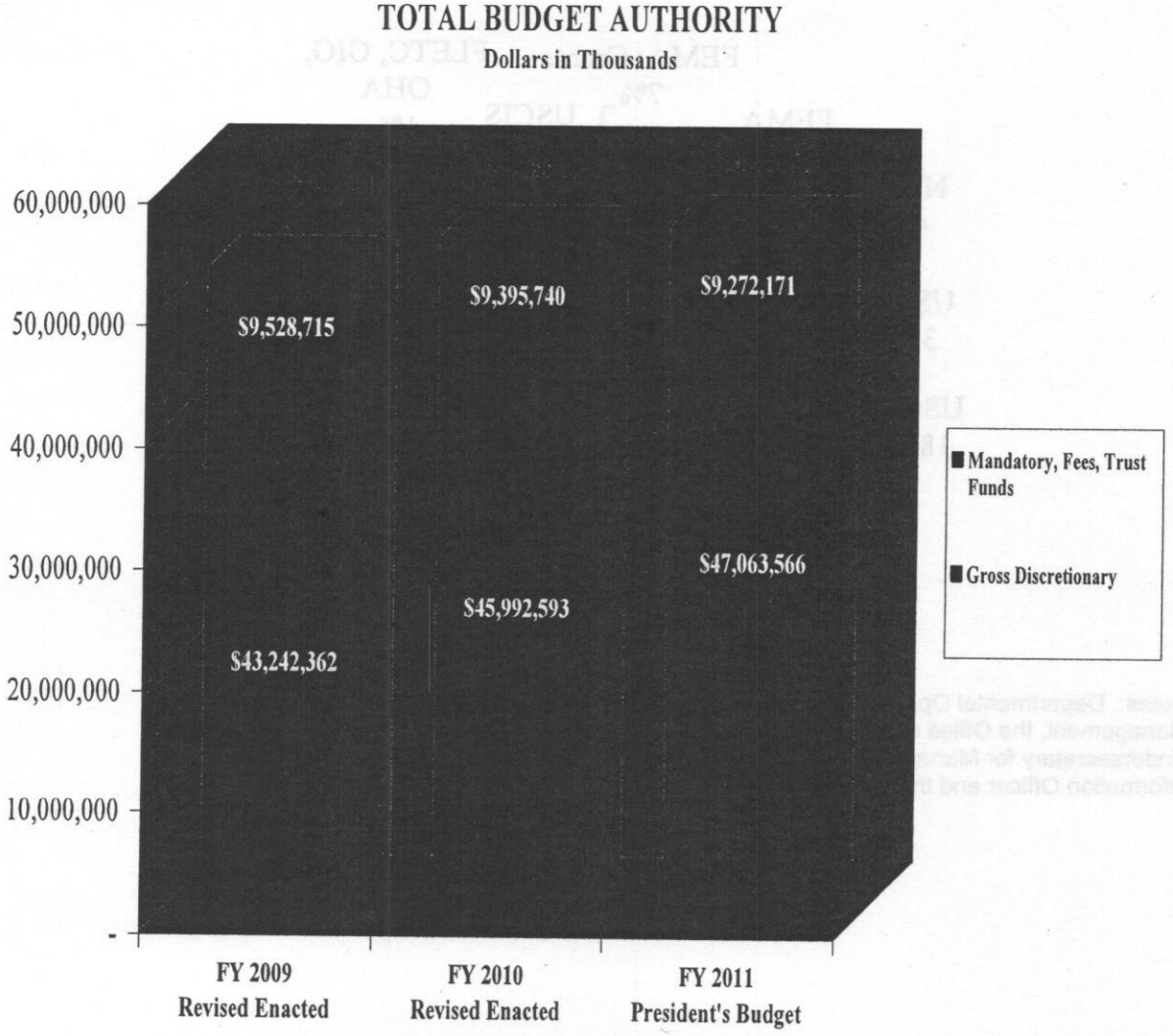
- *Lease Consolidation – Mission Support*: A total of $75M is requested to align the Department's real estate portfolio in the NCR to enhance mission performance and increase management efficiency in conjunction with St. Elizabeths Headquarters Consolidation.

- *Data Center Migration*: A total of $192.2M is requested for the continuation of system and application migration of legacy data centers to two enterprise-wide DHS Data Centers to meet current and anticipated data service requirements. Funding will also be utilized for upgrading infrastructure requirements.

- *Acquisition Workforce*: The FY 2011 request includes an increase of $24.2M to strengthen the Department's acquisition workforce capacity and capabilities. The increase is requested to mitigate the risks associated with skill gaps of the acquisition workforce, ensure that the Department achieves the best terms possible in major acquisitions and improve the effectiveness of the workforce.

- *Science and Technology (S&T) Safe Container (SAFECON)/Time Recorded Ubiquitous Sensor Technology (TRUST) R&D*: A total of $8M is requested for the S&T SAFECON and TRUST programs. These initiatives develop high reliability, high-throughput detection technologies to scan cargo containers entering the country for weapons of mass destruction, explosives, contraband and human cargo.

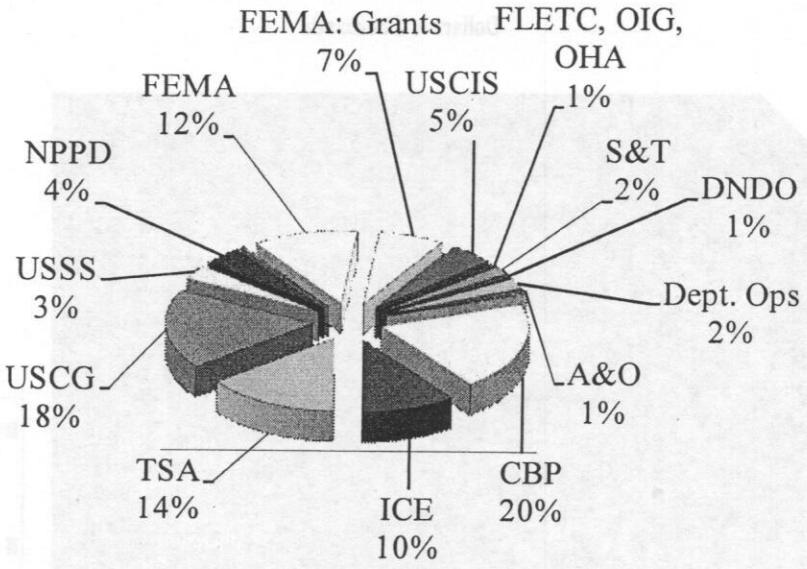
- *Grants*: A total of $4B is requested for grant programs to support our nation's first responders. This funding assists state and local governments in the prevention of, protection against, response to and recovery from incidents of terrorism and other events.



- FY 2011 Gross Discretionary funding increases by $1.1 billion, or 2 percent, over FY 2010.
- There is an decrease of $123 million, or 1 percent, in estimated budget authority for Mandatory, Fees, and Trust Funds over FY 2010.
- Excludes supplemental funding and rescissions of prior-year carryover funds.

AR 001155

FY 2011
Percent of Total Budget Authority by Organization
$56,335,737,000



Notes: Departmental Operations is composed of the Office of the Secretary & Executive Management, the Office of the Federal Coordinator for Gulf Coast Rebuilding, the Office of the Undersecretary for Management, the Office of the Chief Financial Officer, the Office of the Chief Information Officer and the National Special Security Event Fund.

TOTAL BUDGET AUTHORITY BY ORGANIZATION

Gross Discretionary & Mandatory, Fees, Trust Funds

	FY 2009 Revised Enacted [1]	FY 2010 Revised Enacted [2]	FY 2011 President's Budget	FY 2011 +/- FY 2010 Enacted	FY 2011 +/- FY 2010 Enacted
	$000	$000	$000	$000	%
Departmental Operations [3]	$ 659,109	$ 802,931	$ 1,270,821	$ 467,890	58%
Analysis and Operations	327,373	335,030	347,930	12,900	4%
Office of the Inspector General	114,513	113,874	129,806	15,932	14%
U.S. Customs & Border Protection	11,250,652	11,449,283	11,180,018	(269,265)	-2%
U.S. Immigration & Customs Enforcement	5,968,015	5,741,752	5,835,187	93,435	2%
Transportation Security Administration	6,992,778	7,656,066	8,164,780	508,714	7%
U.S. Coast Guard	9,624,179	10,122,963	10,078,317	(44,646)	0%
U.S. Secret Service	1,640,444	1,702,644	1,811,617	108,973	6%
National Protection and Programs Directorate	1,188,263	2,432,755	2,361,715	(71,040)	-3%
Office of Health Affairs	157,621	139,250	212,734	73,484	53%
Federal Emergency Management Agency	5,971,159	6,194,268	6,527,406	333,138	5%
FEMA: Grant Programs	4,220,858	4,165,200	4,000,590	(164,610)	-4%
U.S. Citizenship & Immigration Services	2,876,348	2,859,997	2,812,357	(47,640)	-2%
Federal Law Enforcement Training Center	332,986	282,812	278,375	(4,437)	-2%
S&T Directorate	932,587	1,006,471	1,018,264	11,793	1%
Domestic Nuclear Detection Office	514,191	383,037	305,820	(77,217)	-20%
TOTAL:	$ 52,771,076	$ 55,388,333	$ 56,335,737	$ 947,404	1.71%
Less Rescission of Prior Year Carryover Funds: [4]	(61,373)	(40,474)	-	40,474	-100%
ADJUSTED TOTAL BUDGET AUTHORITY:	$ 52,709,703	$ 55,347,859	$ 56,335,737	$ 987,878	2%
SUPPLEMENTAL: [5]	$ 3,354,503	$ 295,503	$ -	$ (295,503)	$ -
Less Rescission of Prior Year Carryover Funds: [5]	$ (100,000)	$ -	$ -	$ -	

1/ FY 2009 revised enacted reflects:
- Net reprogramming/transfer adjustments for OSEM ($17.4 million); OIG ($16.0 million); CBP ($-24.1 million); ICE ($16.4 million); TSA (14.4 million); USCG ($.400 million); USSS ($ 2.5 million); NPPD ($30 million); OHA ($.430 million); FEMA ($-39.5 million).
- Technical adjustments to revise fee/trust fund estimates for ICE - Immigration Inspection User Fee ($7.0 million); ICE - Detention and Removal Examination Fee ($1.4 million); ICE - Breached Bond/Detention Fund ($15.0 million); TSA - Transportation Threat and Credentialing - Registered Traveler (-$10.0 million), TSA - Transportation Threat and Credentialing - Transportation Worker Identification Credentials ($22.7 million); TSA - Transportation Threat and Credentialing - HAZMAT (-$3.0 million); TSA - Transportation Threat and Credentialing - Alien Flight School ($1.0 million); CIS ($185.4 million); USCG ($7.9 million).
- Realignment of USCG Operating Expenses funding and Pursuant to P.L. 110-53 reflects TSA realignment of funds for 9/11 Commission Act implementation ($3.675 million - Aviation Security, 13.825 million - Surface, $2.5 million - Support).
- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$20.0 million).

2/ FY 2010 revised enacted reflects:
- Technical adjustments for TSA Aviation Security Fees of ($128.9 million); USCG Health Care Fund ($5.0 million).
- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$.800 million).
- For comparability purposes, excludes USCG Overseas Contingency Operations ($241.5 million) and National Science Foundation transfer to USCG of $54.0 million.

3/ Departmental Operations is comprised of the Office of the Secretary & Executive Management, the Office of the Federal Coordinator for Gulf Coast Rebuilding, the Office of the Undersecretary for Management, the Office of the Chief Financial Officer, the Office of the Chief Information Officer, and the National Special Security Events Fund (NSSE).

4/ Pursuant to P.L. 110-329, reflects FY 2009 rescissions of prior year unobligated balances: Analysis and Operations (-$21.373 million); TSA (-$31.0 million); FEMA - Cerro Grande (-$9.0 million).
Pursuant to P.L. 111-83, reflects FY 2010 rescissions of prior year unobligated balances: Analysis and Operations (-$2.4 million); TSA (-$4.0 million); Counter-Terrorism Fund (-$5.6 million); FEMA ($-5.6 million); S&T ($-6.9 million); DNDO (-$8.0 million).

5/ In order to obtain comparable figures, Net Discretionary, Gross Discretionary, and Total Budget Authority excludes:
- FY 2009 supplemental funding pursuant to P.L. 110-252: USCG ($112 million).
- FY 2009 supplemental funding pursuant to P.L. 111-5 (ARRA): USM ($200 million); OIG ($5 million); CBP ($680 million); ICE ($20 million); TSA ($1.0 Billion); USCG ($240 million); FEMA ($610 million),.
- FY 2009 supplemental funding pursuant to P.L. 111-8: USSS ($100 million).
- FY 2009 supplemental funding pursuant to P.L. 111-32: CBP ($51.2 million); ICE ($66.8 million); USCG ($139.5 million); FEMA ($130.0 million).
- Pursuant to P.L. 111-32 reflects FY 2009 rescissions of prior year unobligated balances: FEMA (-$100.0 million).
- FY 2010 Overseas Contingency Operations funding provided in P.L. 111-83: USCG ($241.5 million);
- FY 2010 Supplemental funding pursuant to P.L. 111-117: USCG ($54.0 million);

AR 001157

NET DISCRETIONARY AUTHORITY BY ORGANIZATION
Excludes Discretionary Offsetting Fees & Mandatory, Non-Offsetting Fees, & Trust Funds

	FY 2009 Revised Enacted [1]	FY 2010 Revised Enacted [2]	FY 2011 President's Budget	FY 2011 +/- FY 2010 Enacted	FY 2011 +/- FY 2010 Enacted
	$000	$000	$000	$000	%
Departmental Operations [3]	$ 659,109	$ 802,931	$ 1,270,821	$ 467,890	58%
Analysis and Operations	327,373	335,030	347,930	12,900	4%
Office of the Inspector General	114,513	113,874	129,806	15,932	14%
U.S. Customs & Border Protection	9,803,667	10,134,554	9,817,117	(317,437)	-3%
U.S. Immigration & Customs Enforcement	5,005,615	5,436,952	5,523,800	86,848	2%
Transportation Security Administration	4,369,358	5,129,505	5,724,000	594,495	12%
U.S. Coast Guard	8,104,707	8,541,749	8,466,537	(75,212)	-1%
U.S. Secret Service	1,415,444	1,482,644	1,571,617	88,973	6%
National Protection and Programs Directorate	1,188,263	1,317,755	1,246,715	(71,040)	-5%
Office of Health Affairs	157,621	139,250	212,734	73,484	53%
Federal Emergency Management Agency	2,777,560	2,963,268	3,292,860	329,592	11%
FEMA: Grant Programs	4,220,858	4,165,200	4,000,590	(164,610)	-4%
U.S. Citizenship & Immigration Services	152,490	224,000	385,800	161,800	72%
Federal Law Enforcement Training Center	332,986	282,812	278,375	(4,437)	-2%
S&T Directorate	932,587	1,006,471	1,018,264	11,793	1%
Domestic Nuclear Detection Office	514,191	383,037	305,820	(77,217)	-20%
TOTAL:	$ 40,076,342	$ 42,459,032	$ 43,592,786	$ 1,133,754	2.67%
Less Rescission of Prior Year Carryover Funds: [4]	(61,373)	(40,474)	-	40,474	-100%
Mandatory, Fees, and Trusts	12,694,734	12,929,301	12,742,951		
ADJUSTED TOTAL BUDGET AUTHORITY:	$ 52,709,703	$ 55,347,859	$ 56,335,737	$ 987,878	2%
SUPPLEMENTAL: [5]	$ 3,354,503	$ 295,503	$ -	$ (295,503)	$ -
Less Rescission of Prior Year Carryover Funds: [5]	$ (100,000)	$ -	$ -	$ -	

1/ FY 2009 revised enacted reflects:

- Net reprogramming/transfer adjustments for OSEM ($17.4 million); OIG ($16.0 million); CBP ($-24.1 million); ICE ($16.4 million); TSA (14.4 million); USCG ($.400 million); USSS ($ 2.5 million); NPPD ($30 million); OHA ($.430 million); FEMA ($-39.5 million).

- Technical adjustments to revise fee/trust fund estimates for ICE - Immigration Inspection User Fee ($7.0 million); ICE - Detention and Removal Examiniation Fee ($1.4 million); ICE - Breached Bond/Detention Fund ($15.0 million); TSA - Transportation Threat and Credentialing - Registered Traveler (-$10.0 million), TSA - Transportation Threat and Credentialing - Transportation Worker Identification Credentials ($22.7 million); TSA - Transportation Threat and Credentialing - HAZMAT (-$3.0 million); TSA - Transportation Threat and Credentialing - Alien Flight School ($1.0 million); CIS ($185.4 million); USCG ($7.9 million).

- Realignment of USCG Operating Expenses funding and Pursuant to P.L. 110-53 reflects TSA realignment of funds for 9/11 Commission Act implementation ($3.675 million - Aviation Security, 13.825 million - Surface, $2.5 million - Support).

- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$20.0 million).

2/ FY 2010 revised enacted reflects:

- Technical adjustments for TSA Aviation Security Fees of ($128.9 million); USCG Health Care Fund ($5.0 million).

- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$.800 million).

- For comparability purposes, excludes USCG Overseas Contingency Operations ($241.5 million) and National Science Foundation transfer to USCG of $54.0 million.

3/ Departmental Operations is comprised of the Office of the Secretary & Executive Management, the Office of the Federal Coordinator for Gulf Coast Rebuilding, the Office of the Undersecretary for Management, the Office of the Chief Financial Officer, the Office of the Chief Information Officer, and the National Special Security Events Fund (NSSE).

4/ Pursuant to P.L. 110-329, reflects FY 2009 rescissions of prior year unobligated balances: Analysis and Operations (-$21.373 million); TSA (-$31.0 million); FEMA - Cerro Grande (-$9.0 million).

Pursuant to P.L. 111-83, reflects FY 2010 rescissions of prior year unobligated balances: Analysis and Operations (-$2.4 million); TSA (-$4.0 million); Counter-Terrorism Fund (-$5.6 million); FEMA ($-5.6 million); S&T ($-6.9 million); DNDO (-$8.0 million).

5/ In order to obtain comparable figures, Net Discretionary, Gross Discretionary, and Total Budget Authority excludes:

- FY 2009 supplemental funding pursuant to P.L 110-252: USCG ($112 million).

- FY 2009 supplemental funding pursuant to P.L. 111-5 (ARRA): USM ($200 million); OIG ($5 million); CBP ($680 million); ICE ($20 million); TSA ($1.0 Billion); USCG ($240 million); FEMA ($610 million);

- FY 2009 supplemental funding pursuant to P.L. 111-8: USSS ($100 million).

- FY 2009 supplemental funding pursuant to P.L. 111-32: CBP ($51.2 million); ICE ($66.8 million); USCG ($139.5 million); FEMA ($130.0 million).

- Pursuant to P.L. 111-32 reflects FY 2009 rescissions of prior year unobligated balances: FEMA (-$100.0 million).

- FY 2010 Overseas Contingency Operations funding provided in P.L. 111-83: USCG ($241.5 million);

- FY 2010 Supplemental funding pursuant to P.L. 111-117: USCG ($54.0 million);

KEY FY 2009 ACCOMPLISHMENTS & REFORMS

In 2009, our 230,000 employees strengthened existing efforts and launched new initiatives to meet our five key responsibilities: guarding against terrorism; securing our borders; engaging in smart, effective enforcement of immigration laws; preparing for, responding to and recovering from disasters of all kinds; and building a mature and unified Department.

DHS has emphasized three cross-cutting approaches to achieve these aims—increasing cooperation with federal, state, tribal, local, private sector, and international partners; deploying the latest science and technology to support our mission; and maximizing efficiency and streamlining operations across the Department.

As a result, we have made major advances in addressing new and emerging threats to keep our homeland safe, fostering lawful trade and travel and continuing to build a ready and resilient nation able to meet the challenges of the 21st century. The following are some key initiatives accomplished this past year.

Guarding Against Terrorism and Threats to Cyber Networks and Critical Infrastructure

Protecting the American people from terrorist threats is the founding purpose of the Department and a top priority. Over the past year, DHS has continued to guard against terrorism by enhancing explosives detection and other protective measures in public spaces and transportation networks, working with the private sector to protect critical infrastructure and cyber networks from attack, improving detection of chemical, biological, radiological, and nuclear materials, and building information-sharing partnerships with state and local law enforcement that enable law enforcement to better mitigate threats.

- Fulfilling a key 9/11 Commission recommendation, TSA began implementing Secure Flight, which prescreens passenger name, date of birth and gender against government watch lists for domestic and international flights.

- TSA achieved the 9/11 Act requirement of screening 50 percent of air cargo transported on domestic passenger aircrafts by February 3, 2009. Currently, 100 percent of cargo is screened on more than 95 percent of flights originating in the United States and 100 percent of all baggage is screened for explosives

- The Domestic Nuclear Detection Office directly trained more than 3,600 federal, state and local officers and first responders in radiological and nuclear detection and began demonstrating the first-of-its-kind Cargo Advanced Automated Radiography System, which aims to detect special nuclear materials and shielding material in cargo at ports of entry.

- DHS opened the new National Cyber Security and Communications Integration Center—a 24-hour, DHS-led coordinated watch and warning center that will improve national efforts to address threats and incidents affecting the Nation's critical IT and cyber infrastructure.

- DHS worked with the Office of Personnel Management to attain new authority to recruit and hire up to 1,000 cyber security professionals across the Department over the next 3 years to

help fulfill DHS' broad mission to protect the Nation's cyber infrastructure, systems and networks.

- S&T partnered with the U.S. Secret Service, industry and academia to digitize more than 9,000 ink samples to expedite the investigation of criminal and terrorist activities by reducing matching times from days to minutes.

- DHS held the 5-day National Level Exercise 2009—the first national level exercise to focus on terrorism prevention—in conjunction with federal, state, local, tribal, private sector and international partners.

- In accordance with the Chemical Facilities Anti-Terrorism Standards Act (CFATS), which allows DHS to regulate the security measures at high-risk chemical facilities, DHS is working with 2,300 facilities on strengthening security measures. In 2009, DHS received Site Security Plans from over 900 regulated facilities.

- DHS signed agreements to prevent and combat crime with Italy, Greece, Portugal and Spain. These agreements allow for the exchange of biometric and biographic data to bolster counterterrorism and law enforcement efforts while emphasizing privacy protections.

- DHS and Spanish Interior Minister Perez Rubalcaba signed a Declaration of Principles formalizing the Immigration Advisory Program—which identifies high-risk travelers at foreign airports before they board aircraft bound for the United States.

- DHS forged partnerships with Germany and Spain to facilitate scientific research and collaboration to combat transnational threats.

- DHS and Canadian Public Safety Minister Peter Van Loan announced a series of cooperative initiatives between the United States and Canada to address terrorism and organized crime while expediting the lawful flow of travel and trade—including a biometric data sharing initiative also involving Australia, the United Kingdom and, eventually, New Zealand.

Securing our Borders while Facilitating Lawful Travel and Trade

In 2009, DHS continued to strengthen security on the Southwest border through additional manpower and new technology to disrupt the flow of illegal drug, cash and weapon smuggling that fuels cartel violence in Mexico. The Department also reinforced security on the northern border while facilitating lawful travel and trade.

- The Obama administration announced the Southwest Border Security Initiative, a joint effort of the Departments of Homeland Security, Justice and State to crack down on Mexican drug cartels by enhancing border security through additional personnel, increased intelligence capability and better coordination with state, local and Mexican law enforcement authorities. As of December 8, 2009, CBP has seized more than $38.3 million in southbound currency—an increase of more than $29.3 million compared to the same period in 2008. In total thus far in 2009, CBP and ICE have seized more than $101.7 million and nearly 1.59 million

kilograms of drugs—an increase of more than $48.2 million and more than 423,167 kilograms of drugs compared to the same period in 2008.

- DHS implemented the Western Hemisphere Travel Initiative for land and sea travel to the United States, increasing border security while facilitating lawful travel and trade by requiring U.S. and Canadian citizens to present a passport or other approved secure document that denotes identity and citizenship when crossing the border.

- DHS and the Department of Justice joined with the Office of National Drug Control Policy to release the National Southwest Border Counternarcotics Strategy, the Obama administration's strategy to stem the flow of illegal drugs and their illicit proceeds across the southwest border and reduce associated crime and violence.

- The Department announced the expansion of Global Entry—a CBP pilot program that streamlines the screening process at airports for trusted travelers through biometric identification—as a permanent voluntary program at airports across the United States. Global Entry reduces average wait times by more than 70 percent and more than 75 percent of travelers using Global Entry are admitted in less than five minutes.

- DHS launched a joint Coast Guard-CBP effort to use Predator Unmanned Aerial Systems (UAS) to provide improved surveillance of the United States' maritime borders. DHS will conduct the first UAS operations along maritime borders in 2010.

- DHS, the Department of Justice and the Government of Mexico signed a Letter of Intent to develop a coordinated and intelligence-driven response to the threat of cross-border smuggling and trafficking of weapons and ammunition. This first-of-its-kind arrangement leverages the combined investigative capabilities of ICE, the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Attorney General of Mexico to combat violence and criminal activity along the U.S.-Mexico border.

- Through Global Entry, DHS launched a first-of-its-kind initiative with the Netherlands to open membership in U.S. and Dutch expedited air travel programs to citizens of both countries in an effort to streamline entry processes for pre-screened fliers.

Engaging in Smart, Effective Immigration Law Enforcement

Over the past year, DHS has strengthened its immigration enforcement activities, targeting criminal aliens and employers who violate the nation's immigration laws, while making improvements to the legal immigration system.

- DHS implemented a new, comprehensive strategy to reduce the demand for illegal employment and protect employment opportunities for the Nation's lawful workforce by targeting employers who knowingly hire illegal workers through investigations, prosecution and civil and criminal penalties. Since January 2009, DHS' new worksite enforcement policies have led to 1,897 cases and 2,069 Form I-9 inspections targeting employers, 58 companies and 62 individuals debarred, and 142 Notices of Intent to Fine totaling $15,865,181 issued.

- DHS is reforming the immigration detention system, enhancing security and efficiency nationwide while prioritizing the health and safety of detainees. New initiatives include creating an Office of Detention Policy and Planning to ensure uniform conditions of confinement, medical care and design; implementing a medical classification system; centralizing all detention facility contracts under ICE headquarters' supervision; developing a plan for alternatives to detention; more than doubling the number of federal personnel providing onsite oversight at the facilities where the majority of detainees are housed; creating two advisory boards comprised of community and immigration advocacy groups; and establishing an independent Office of Detention Oversight reporting directly to the ICE Assistant Secretary.

- DHS expanded the Secure Communities initiative—which uses biometric information to target criminal aliens in U.S. correctional facilities—from 14 to 107 locations in 2009, reflecting an increased emphasis on identifying and removing criminal aliens who pose the greatest threat to public safety. To date, the program has identified more than 111,000 aliens in jails and prisons who have been charged with or convicted of criminal offenses.

- USCIS and the FBI cleared the backlog of a year or more for background checks on people seeking to work and live in the United States or become citizens—reflecting DHS' commitment to quick, thorough and fair adjudication of immigration applications. The vast majority of these checks are now answered within 30 days. At the end of fiscal year 2009, USCIS also reduced the backlog of pending immigration applications and petitions by more than 90 percent and reduced average processing times for naturalization applicants by nearly 5 months as compared to FY 2008.

- USCIS launched a redesigned website—available in English and Spanish—which provides a one-stop location for immigration services and information, including real-time alerts on the status of immigration applications via text message and e-mail.

- USCIS increased employer participation in E-Verify, the nation's preeminent employment eligibility verification system, from 88,000 companies at the end of FY 2008 to more than 177,000 employers today.

Preparing for, Responding to and Recovering from Disasters

In the event of a terrorist attack, natural disaster or other large-scale emergency, the Department provides a coordinated, comprehensive federal response and works with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. This year, DHS increased efforts to build a ready and resilient nation by providing grants and training to our homeland security and law enforcement partners, coordinating the federal government's response to H1N1, and streamlining rebuilding and recovery along the Gulf Coast.

- DHS led the federal response to the H1N1 outbreak, creating regional coordination teams comprised of representatives from DHS and the Departments of Defense and Health and Human Services to oversee, coordinate and execute national incident management responsibilities. DHS also coordinated outreach efforts to congressional, state, local, tribal, private sector and international officials regarding the H1N1 outbreak.

AR 001162

- Since January 20, 2009, Louisiana and Mississippi have received more than $2.1 billion in public assistance from DHS, including $125 million for debris removal and emergency protective measures, $935.5 million in public works and infrastructure projects, $258 million for mitigation activities to increase resilience and more than $542 million for K-12 education. In addition, more than 6,000 displaced households in Louisiana and Mississippi have been transitioned to permanent housing.

- To cut through red tape and streamline and expedite the decision-making process for public assistance for recovery efforts in the Gulf Coast, DHS established two joint public assistance teams and a new arbitration process to resolve longstanding issues over public assistance funding. Over the past 10 months, the Joint Expediting Team and the Unified Public Assistance Project Decision Team have resolved 156 projects, distributing more than $100 million dollars to support the repair and replacement of fire and police stations, schools like the Southern University of New Orleans and Holy Cross School, libraries and other infrastructure critical to the recovery of Gulf Coast communities.

- FEMA has responded to 47 declared disasters since January 21, 2009, including the Red River flooding in North Dakota and Minnesota, the September flooding in Georgia and the earthquake and tsunami that struck American Samoa.

Unifying and Maturing DHS

Six years since the Department's creation, DHS' goal remains the same: one enterprise dedicated to a shared vision for homeland security. Over the past year, DHS implemented a series of wide-ranging efficiency initiatives that leverage the economies of scale in DHS in order to recover millions of dollars and create a culture of responsibility and fiscal discipline. At the same time, the Department leveraged new technology to improve DHS operations, coordination and outreach.

- DHS broke ground on its new headquarters at the St. Elizabeths Campus. While DHS currently operates in more than 40 offices around the National Capitol Region, the consolidated headquarters will unify DHS' many components into one cohesive department and is expected to save taxpayers $163 million over the next 30 years.

- DHS launched the Efficiency Review Initiative to improve efficiency, streamline operations and promote greater accountability, transparency and customer satisfaction through a series of initiatives—including eliminating non-mission critical travel, renegotiating contracts, utilizing government facilities instead of private rentals, reducing printing and postal mail and maximizing the use of web-based communication, training and meetings, implementing energy efficiencies in DHS facilities and maximizing DHS' buying power to receive the lowest price possible when acquiring office supplies and software licenses. These initiatives collectively are expected to lead to hundreds of millions of dollars in cost avoidances. This past year, DHS identified more than $100 million in cost savings including $22 million by eliminating non-mission critical travel; $16 by utilizing software licensing agreements DHS-wide; $7 million through the mandatory review of contracts; $9 million by eliminating redundancy in processing mariner credentials; $8 million by consolidating the DHS sensitive-but-unclassified portal system; almost $4 million by posting documents online or using e-mail in lieu of printing and postal mail; $2 million by streamlining boat maintenance and support schedules; $2 million by utilizing government facilities instead of private

rentals; almost $2 million by increasing energy efficiencies at facilities and many more examples across the Department.

- S&T launched the Virtual USA initiative, an innovative, information-sharing initiative that helps federal, state, local and tribal first responders communicate during emergencies by linking disparate tools and technologies in order to share the location and status of critical assets and information—such as power and water lines, flood detectors, helicopter-capable landing sites, emergency vehicle and ambulance locations, weather and traffic conditions, evacuation routes and school and government building floor plans—across federal, state, local and tribal governments.

Selected DHS High Priority Performance Goals

Preventing Terrorism and Enhancing Security

- **Improve security screening of passengers, baggage, and employees while expediting the movement of the traveling public (aviation and surface transportation security).**

  FY2011 Initiatives include deploying new technology, law enforcement and canine assets at domestic airports, enhancing checkpoint technology, implementing the Transportation Workers Identification Credential (TWIC) program—which requires transportations workers to obtain a biometric identification card to gain access to secure areas of transportation facilities, and strengthening our Visible Intermodal Prevention and Response (VIPR) teams— which use unpredictability to deter, detect, and disrupt potential terrorist activities, will help us to achieve these goals.

Securing and Managing Our Borders

- **Prevent terrorist movement at land ports of entry and maritime borders through enhanced screening while expediting the flow of legitimate travel.**

  FY2011 initiatives include implementing the Western Hemisphere Travel Initiative by deploying new technology, upgrading our processing capabilities at border checkpoints, and enhancing information sharing among law enforcement, as well as continuing recapitalization of aging Coast Guard surface and air assets to quickly and effectively respond to emerging threats.

Enforcing and Administering Our Immigration Laws

- **Improve the efficiency of the process to detain and remove illegal immigrants from the United States.**
- **Improve the delivery of immigration services.**

  FY2011 initiatives include increasing our targets for detaining and removing dangerous criminal aliens from the United States through our Secure Communities program—which uses biometrics to identify and remove criminal aliens incarcerated in state and local jails—by four percent per

year. Additionally, we will improve the delivery of immigration services by modernizing our adjudication process for new immigrants and potential citizens.

Ensuring Resilience to Disasters

- **Strengthen disaster preparedness and response by improving FEMA's operational capabilities and enhancing State, local and private citizen preparedness**

  In FY2011, FEMA will continue to enhance its training programs to help state and local entities prepare for all types of disasters. FEMA is also developing a national strategy to house up to half a million households within sixty days of a disaster—increasing current capacity by 200 percent.

Maturing and Strengthening the Homeland Security Enterprise

- **Mature and unify the Homeland Security Enterprise through effective information sharing.**

- **Improve acquisition execution across the DHS acquisition portfolio, by ensuring key acquisition expertise resides in major program office and acquisition oversight staffs throughout the Department.**

  In FY2011, our efforts will focus on information sharing across all departmental components. Additionally, the department is undertaking an initiative to enhance the capability and capacity of its acquisition workforce to ensure that major acquisition projects do not exceed cost, schedule, and performance objectives.

We will focus on these goals over the next two years and continue to work closely with the Office of Management and Budget in the monitoring and reporting of milestones and performance measures associated with them. As we continue the Bottom-Up Review associated with the QHSR, we may update these goals and associated measures.

CONCLUSION

The FY 2011 budget proposal reflects this administration's continued commitment to protecting the homeland and the American people through the effective and efficient use of DHS resources. As outlined in my testimony today, the Department will build on past successes in several areas including information sharing with our partners, aviation and port security measures and immigration reform efforts.

Thank you for inviting me to appear before you today. I look forward to answering your questions and to working with you on the FY 2011 Budget Request and other issues.

AR 001165

Statement for the Record

The Honorable Janet Napolitano

Secretary
United States Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security

AR 001166

Mr. Chairman, Representative King, and Members of the Committee:

Let me begin by saying thank you for the strong support you have provided me and the Department this past year. I look forward to another year working with you to make certain that we have the right resources to protect the homeland and the American people and that we make the most effective and efficient use of those resources.

I am pleased to appear before the Committee today to present President Obama's Fiscal Year (FY) 2011 Budget Request for the Department of Homeland Security (DHS).

As you know, the attempted attack on Northwest Flight 253 on December 25 was a powerful illustration that terrorists will go to great lengths to try to defeat the security measures that have been put in place since September 11, 2001. This Administration is determined to thwart those plans and disrupt, dismantle and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This effort involves not just DHS, but also many other federal agencies as well as state, local, tribal, territorial, private sector and international partners. As President Obama has made clear, this Administration is determined to find and fix the vulnerabilities in our systems that allowed this breach to occur – and the FY 2011 Budget Request prioritizes these security enhancements.

The Department is also working hand-in-hand with our federal partners to respond to the devastation and loss of life in Haiti following the January 12 earthquake. Collaboration within DHS among our many components has allowed us to leverage unprecedented resources and personnel to assist with the humanitarian efforts in Haiti, once again demonstrating what these offices can accomplish together. The FY2011 Budget Request strengthens the ongoing work in each of our Department's offices to fulfill our unified mission.

I will now summarize the FY 2011 budget request along with some of our key accomplishments from last year.

FY 2011 BUDGET REQUEST

The FY 2011 DHS budget will strengthen efforts that are critical to the Nation's security, bolster the Department's ability to combat terrorism and respond to emergencies and potential threats, and allow DHS to tackle its responsibilities to protect the Nation and keep Americans safe.

DHS executes a wide array of responsibilities in its unified security mission. To bolster these efforts, DHS collaborates and coordinates with many partners—state, local and tribal governments and law enforcement agencies, international allies, the private sector and other federal departments. These partnerships are essential to DHS' ability to fulfill its security mission.

The FY 2011 budget continues efforts to use our resources as efficiently and effectively as possible. We must exercise strong fiscal discipline, making sure that we are investing our resources in what works, cutting down on redundancy, eliminating ineffective programs and making improvements across the board.

To institutionalize a culture of efficiency across the Department, DHS launched the Department-wide Efficiency Review Initiative in March 2009. One major element of the Efficiency Review is

AR 001167

the Balanced Workforce Strategy, a three-pronged approach to ensuring that the right workforce balance is achieved. First, we are taking steps to ensure that no inherently governmental functions are performed by contractors. Second, we put in place rigorous review procedures to ensure that future activities do not increase our reliance on contractors. Third, we are coordinating workforce assessments across the Department to seek economies and service improvements and reduce our reliance on contractors. In FY 2011, the Department will continue executing the Balanced Workforce Strategy by converting contractor positions to federal jobs.

DHS secures the United States against all threats through five main missions, each of which is strengthened by this budget:

- *Preventing Terrorism and Enhancing Security*: Guarding against terrorism was the founding mission of DHS and remains our top priority today. A key element of preventing terrorism is recognizing the evolving threats posed by violent extremists and taking action to ensure our defenses continue to evolve to deter and defeat them.
- *Securing and Managing Our Borders*: DHS monitors our air, land and sea borders to prevent illegal trafficking that threatens our country, while facilitating lawful travel and trade. We will continue to strengthen security efforts on the southwest border to combat and disrupt cartel violence and provide critical security upgrades—through infrastructure and technology—along the northern border.
- *Enforcing and Administering our Immigration Laws*: DHS is responsible for enforcing the Nation's immigration laws while streamlining and facilitating the legal immigration process. In FY 2011, we will continue to strengthen enforcement activities while targeting criminal aliens who pose a threat to public safety and employers who knowingly violate the law.
- *Safeguarding and Securing Cyberspace*: The Department defends against and responds to attacks on the cyber networks through which Americans communicate with each other, conduct business and manage infrastructure. DHS analyzes and reduces cyber threats and vulnerabilities, distributes threat warnings, coordinates the response to cyber incidents and works with the private sector and our state, local, international and private sector partners to ensure that our computers, networks and cyber systems remain safe.
- *Ensuring Resilience to Disasters*: The Department provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergencies while working with federal, state, local and private sector partners to ensure a swift and effective recovery effort. DHS will continue its increased efforts to build a ready and resilient nation by bolstering information sharing, providing grants and training to our homeland security and law enforcement partners and further streamlining rebuilding and recovery along the Gulf Coast.

Ensuring shared awareness of risks and threats, increasing resilience in communities and enhancing the use of science and technology underpin these national efforts to prevent terrorism, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace and ensure resilience to disasters.

The total FY 2011 budget request for DHS is $56.3 billion in total funding; a 2 percent increase over the FY 2010 enacted level. The Department's FY 2011 gross discretionary budget request[1] is $47.1 billion, an increase of 2 percent over the FY 2010 enacted level. The Department's FY 2011 net discretionary budget request is $43.6 billion,[2] an increase of 3 percent over the FY 2010 enacted level. For purposes of comparison the Overseas Contingency Operation funding and transfer from the National Science Foundation are not included in the FY 2010 enacted level.

The following are highlights of the FY 2011 Budget Request:

PREVENTING TERRORISM AND ENHANCING SECURITY

- *Advanced Imaging Technology (AIT)*: An increase of $214.7M is requested to procure and install 500 advanced imaging technology machines at airport checkpoints to detect dangerous materials, including non-metallic materials. This request, combined with units the Transportation Security Administration (TSA) plans to install in 2010, will mean that 1,000 AIT scanners, will total AIT coverage at 75 percent of Category X airports and 60 percent of the total lanes at Category X through II airports.

- *Transportation Security Officers (TSOs) to Staff AITs*: An increase of $218.9M is requested for additional Transportation Security Officers (TSOs), managers and associated support costs to operate additional AITs at airport checkpoints. Passenger screening is critical to detecting and preventing individuals carrying dangerous or deadly objects and materials from boarding planes.

- *Federal Air Marshals (FAMs)*: An increase of $85M is requested for additional FAMs to increase international flight coverage. FAMs help detect, deter and defeat terrorist and other criminal hostile acts targeting U.S. air carriers, airports, passengers and crew.

- *Portable Explosive Trace Detection (ETD)*: An increase of $60M is requested to purchase approximately 800 portable ETD machines ($39M) and associated checkpoint consumables ($21M).

- *Canine Teams*: An increase of $71M and 523 positions (262 Full-Time Equivalents, or FTE) is requested to fund an additional 275 proprietary explosives detection canine teams, 112 teams at 28 Category X airports and 163 teams at 56 Category I airports.

- *Behavior Detection Officers (BDOs)*: An increase of $20M and 350 BDOs (210 FTE) is requested to further enhance TSA's Screening Passengers by Observation Techniques program. The FY 2011 request includes a total of 3,350 officers to enhance coverage at

---

[1] Gross Discretionary funding does not include funding such as Coast Guard's retirement pay account and fees paid for immigration benefits

[2] This does not include fee collections such as funding for the Federal Protective Service (NPPD), aviation security passenger and carrier fees (TSA), credentialing fees (such as TWIC – TSA), and administrative costs of the National Flood Insurance Fund (FEMA).

lanes and shifts at high risk Category X and I airports and expand coverage to smaller airports.

- *Domestic Nuclear Detection Office Systems Engineering and Architecture*: An increase of $13.4M is requested to fund systems engineering efforts to address vulnerabilities in the Global Nuclear Detection Architecture, the multi-layered system of detection technologies, programs and guidelines designed to enhance the Nation's ability to detect and prevent a radiological or nuclear attack.

- *Radiological/Nuclear Detection Systems*: An increase of $41M is requested for the procurement and deployment of radiological and nuclear detection systems and equipment to support efforts across the Department.

- *Law Enforcement Detachment Teams*: An increase of $3.6M is requested to bring deployable U.S. Coast Guard Law Enforcement Detachment (LEDET) teams to full capacity. LEDETs help prevent terrorism, secure U.S. borders, disrupt criminal organizations and support counter drug missions overseas. In FY 2009, for example, LEDETs aboard U.S. naval and partner nation assets accounted for more than 50 percent of total maritime cocaine removals.

- *2012 Presidential Campaign*: Total funding of $14M is requested for startup costs associated with the 2012 Presidential Campaign including training for candidate/nominee protective detail personnel. The Secret Service will also begin to procure and pre-position equipment, services and supplies to support candidate/nominee protective operations throughout the country.

- *Secret Service Information Technology*: Total funding of $36M is requested for the Information Integration and Transformation program. This funding will allow the Secret Service to successfully continue its comprehensive Information Technology (IT) transformation and provide a multi-year, mission-integrated program to engineer a modernized, agile and strengthened IT infrastructure to support all aspects of the Secret Service's mission.

SECURING AND MANAGING OUR BORDERS

- *Journeyman Pay Increase*: In the spring of 2010, DHS will implement the journeyman pay increase, raising the journeyman grade level for frontline Customs and Border Protection (CBP) Officers (including Border Patrol agents and Agricultural Specialists) from GS-11 level to the GS-12 level. An adjustment to the base of $310.4M will fund the full-year impact of the salary and benefit requirements associated with this implementation

- *CBP Officers*: An increase of $44.8M is requested to fund 318 CBP Officer FTEs within the Office of Field Operations and 71 support FTEs for CBP. The decline in the number of passengers and conveyances entering the United States in FY 2009 resulted in an almost 8 percent decrease in revenues from inspection user fees. CBP, therefore, has fewer resources to maintain critical staffing levels for CBP officers. The proposed funding will

allow CBP to maintain staffing for critical positions to protect the United States at its ports of entry.

- *Border Enforcement Security Task Forces (BESTs)*: An additional $10M is requested to establish BESTs in three additional locations: Massena, NY; San Francisco, CA and Honolulu, HI. These multi-agency teams work to identify, disrupt and dismantle criminal organizations posing significant threats to border security, including terrorist groups, gang members, and criminal aliens.

- *Intellectual Property Rights (IPR) Enforcement*: An increase of $30M is requested to support CBP and ICE IPR enforcement efforts. This includes information technology systems that support IPR activities and implementation of the 5-year IPR Plan. An increase of $5M is also requested for the Immigration and Customs Enforcement (ICE)-led National Intellectual Property Rights Coordination Center (IPR Center). The IPR Center brings key U.S. government agencies together to combat IPR violations that threaten our economic stability, restrict the competitiveness of U.S. industry and endanger the public's health and safety. ICE will also use these funds to focus on disrupting criminal organizations through the internet and support for anti-counterfeiting efforts.

- *Intelligence Analysts*: An increase of $10M is requested to fund 103 Intelligence Analysts for CBP. This staffing increase will support 24/7 operations of CBP Intelligence Watch, Operations Coordination and the Commissioner's Situation Room.

- *Coast Guard Asset Recapitalization*: A total of $1.4B is requested to continue recapitalization of aging Coast Guard surface and air assets. Included in this request is $538M for production of the Coast Guard's fifth National Security Cutter to continue replacement of the 378-foot High Endurance Cutters fleet. Also included is $240M for production of four Fast Response Cutters to continue replacement of the 110-foot Class Patrol Boat fleet. The Fast Response Cutters have enhanced capability, high readiness, speed, and endurance, which will allow them to quickly and effectively respond to emerging threats. Additionally, $40M is requested to purchase one Maritime Patrol Aircraft (MPA) HC-144A. The HC-144A will address the Coast Guard's MPA flight hour gap by providing 1,200 hours every year per aircraft. Finally, $13.9M is requested for improvement and acquisition of housing to support military families.

ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

- *E-Verify*: A total of $103.4M and 338 FTEs is requested for the E-Verify Program. In FY 2011, U.S. Citizenship and Immigration Services (USCIS) will develop and implement an E-Verify portal that will provide a single-user interface for the program's products and services. In addition, USCIS will enhance E-Verify's monitoring and compliance activities through analytical capabilities that will support more robust fraud detection and improved analytic processes and will continue developing system enhancements in response to customer feedback, surveys, mission requirements and capacity needs.

- *Secure Communities*: Total funding of $146.9M is requested to continue FY 2010 progress toward nationwide implementation of ICE's Secure Communities program—which involves

the identification, apprehension and removal of all Level 1 criminal aliens in state prisons and local jails through criminal alien biometric identification capabilities. Secure Communities, in cooperation with federal, state and local law enforcement agencies, will provide a safeguard to American communities by removing those criminal aliens from the United States who represent the greatest threats to public safety and by deterring their re-entry through aggressive prosecution.

- *Immigrant Integration*: A total of $18M is requested to fund USCIS Office of Citizenship initiatives, including expansion of the competitive Citizenship Grant Program to support national and community-based organizations preparing immigrants for citizenship, promoting and raising awareness of citizenship rights and responsibilities, and enhancing English language education and other tools for legal permanent residents. The Office of Citizenship will support the implementation of the Immigration Integration program and lead initiatives to educate aspiring citizens about the naturalization process, monitor and evaluate the administration and content of the new naturalization test, and develop educational materials and resources for immigrants and the organizations that serve them.

SAFEGUARDING AND SECURING CYBERSPACE

- *National Cyber Security Division (NCSD)*: Total funding of $379M is requested for the NCSD to support the development of capabilities to prevent, prepare for and respond to incidents that could degrade or overwhelm the Nation's critical information technology infrastructure and key cyber networks. These funds will identify and reduce vulnerabilities, mitigate threats and ensure that cyber intrusions and disruptions cause minimal damage to public and private sector networks.

- *National Cyber Security Center (NCSC)*: A total of $10M is requested for the NCSC to enhance cyber security coordination capabilities across the Federal Government including mission integration, collaboration and coordination, situational awareness and cyber incident response, analysis and reporting, knowledge management, and technology development and management.

ENSURING RESILIENCE TO DISASTERS

- *Disaster Relief Fund (DRF)*: The budget seeks funding of $1.95B, an increase of $350M for the DRF. The DRF provides a significant portion of the total federal response to victims in declared major disasters and emergencies.

- *Federal Emergency Management Agency (FEMA) Facilities*: An additional $23.3M is requested to address critical FEMA real estate needs. By FY 2011, the capacity of FEMA facilities will be unable to accommodate key mission responsibilities and staff. FEMA also faces a critical need to maintain and repair aging and deteriorating national facilities. To address these needs, FEMA has developed a 5-year capital plan to begin critical regional facility acquisitions and repairs.

- *Pre-Disaster Mitigation Grants*: Total funding of $100M is requested to provide program support and technical assistance to state, local and tribal governments to reduce the risks

associated with disasters, support the national grant competition and provide the required $500,000 per state allocation. Resources will support the development and enhancement of hazard mitigation plans, as well as the implementation of pre-disaster mitigation projects.

- *Flood Map Modernization*: A total of $194M is requested to analyze and produce flood hazard data and map products and communicate flood hazard risk. The funding will support the review and update of flood hazard data and maps to accurately reflect flood hazards and monitor the validity of published flood hazard information.

- *Rescue 21*: A total of $36M is requested for the Rescue 21 system, enabling the U.S. Coast Guard to enhance preparedness, ensure efficient emergency response and rapidly recover from disasters. The Rescue 21 system replaces the U.S. Coast Guard's legacy National Distress and Response System and improves communications and command and control capabilities in the coastal zone. The system is the foundation for coastal Search and Rescue and enhances maritime situational awareness through increased communications ability with mariners and other responders.

MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

- *St. Elizabeths Headquarters Consolidation*: To streamline the Departments core operations, $287.8M is requested to consolidate executive leadership, operations coordination and policy and program management functions in a secure setting at St. Elizabeths. The Department's facilities are currently dispersed over more than 40 locations throughout the National Capital Region (NCR). This consolidation at St. Elizabeths will reduce the fragmentation of components and will improve communications, coordination and cooperation across all DHS headquarters organizations.

- *Lease Consolidation – Mission Support*: A total of $75M is requested to align the Department's real estate portfolio in the NCR to enhance mission performance and increase management efficiency in conjunction with St. Elizabeths Headquarters Consolidation.

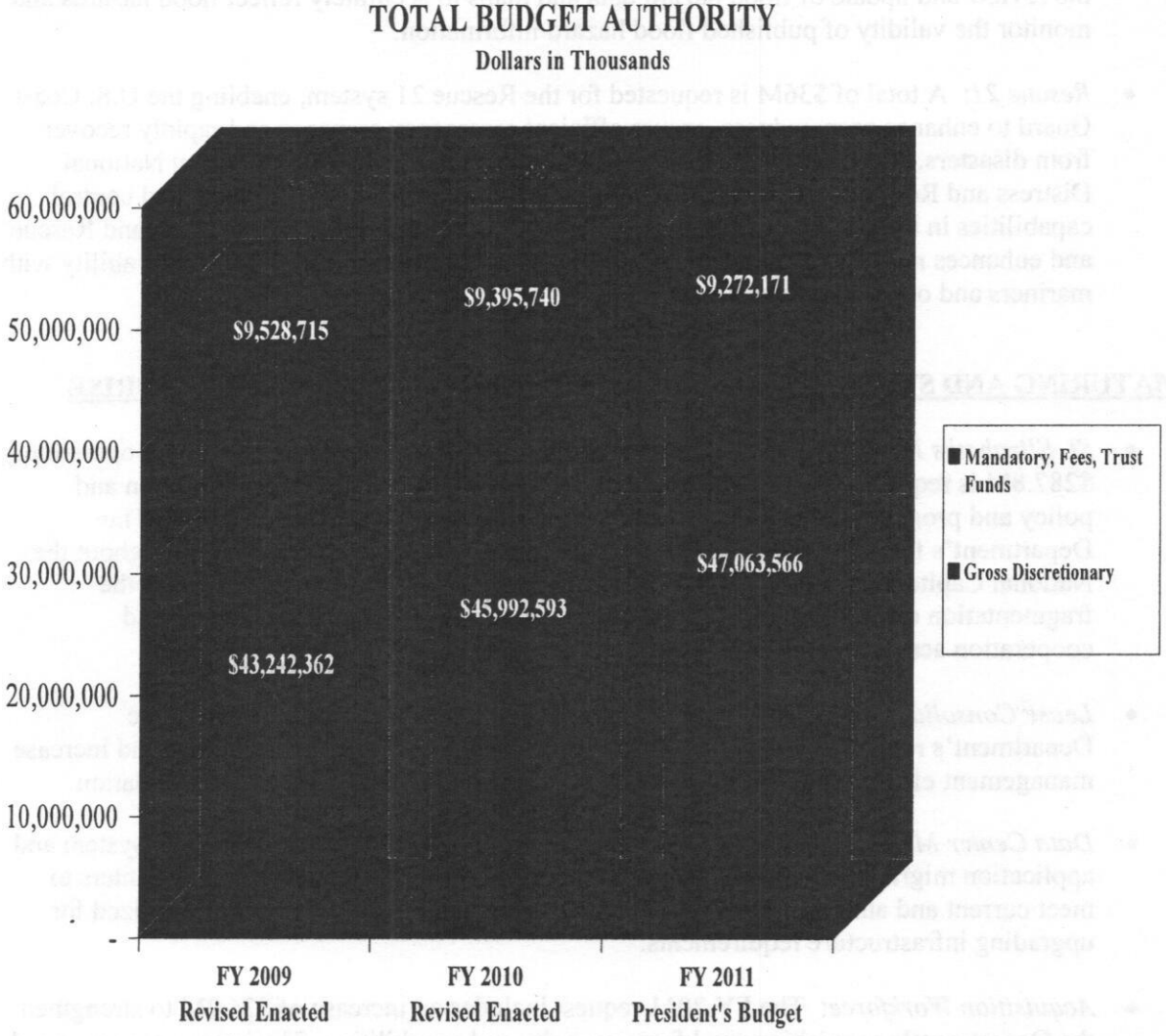
- *Data Center Migration*: A total of $192.2M is requested for the continuation of system and application migration of legacy data centers to two enterprise-wide DHS Data Centers to meet current and anticipated data service requirements. Funding will also be utilized for upgrading infrastructure requirements.

- *Acquisition Workforce*: The FY 2011 request includes an increase of $24.2M to strengthen the Department's acquisition workforce capacity and capabilities. The increase is requested to mitigate the risks associated with skill gaps of the acquisition workforce, ensure that the Department achieves the best terms possible in major acquisitions and improve the effectiveness of the workforce.

- *Science and Technology (S&T) Safe Container (SAFECON)/Time Recorded Ubiquitous Sensor Technology (TRUST) R&D*: A total of $8M is requested for the S&T SAFECON and TRUST programs. These initiatives develop high reliability, high-throughput detection technologies to scan cargo containers entering the country for weapons of mass destruction, explosives, contraband and human cargo.

AR 001173

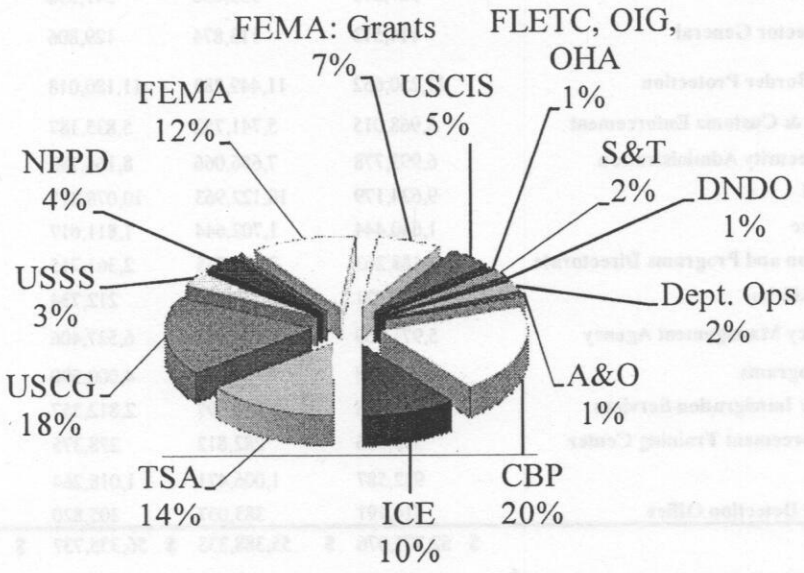
- *Grants*: A total of $4B is requested for grant programs to support our nation's first responders. This funding assists state and local governments in the prevention of, protection against, response to and recovery from incidents of terrorism and other events.



- FY 2011 Gross Discretionary funding increases by $1.1 billion, or 2 percent, over FY 2010.
- There is an decrease of $123 million, or 1 percent, in estimated budget authority for Mandatory, Fees, and Trust Funds over FY 2010.
- Excludes supplemental funding and rescissions of prior-year carryover funds.

AR 001174

FY 2011
Percent of Total Budget Authority by Organization
$56,335,737,000



Notes: Departmental Operations is composed of the Office of the Secretary & Executive Management, the Office of the Federal Coordinator for Gulf Coast Rebuilding, the Office of the Undersecretary for Management, the Office of the Chief Financial Officer, the Office of the Chief Information Officer and the National Special Security Event Fund.

AR 001175

TOTAL BUDGET AUTHORITY BY ORGANIZATION

Gross Discretionary & Mandatory, Fees, Trust Funds

	FY 2009 Revised Enacted [1]	FY 2010 Revised Enacted [2]	FY 2011 President's Budget	FY 2011 +/- FY 2010 Enacted	FY 2011 +/- FY 2010 Enacted
	$000	$000	$000	$000	%
Departmental Operations [3]	$ 659,109	$ 802,931	$ 1,270,821	$ 467,890	58%
Analysis and Operations	327,373	335,030	347,930	12,900	4%
Office of the Inspector General	114,513	113,874	129,806	15,932	14%
U.S. Customs & Border Protection	11,250,652	11,449,283	11,180,018	(269,265)	-2%
U.S. Immigration & Customs Enforcement	5,968,015	5,741,752	5,835,187	93,435	2%
Transportation Security Administration	6,992,778	7,656,066	8,164,780	508,714	7%
U.S. Coast Guard	9,624,179	10,122,963	10,078,317	(44,646)	0%
U.S. Secret Service	1,640,444	1,702,644	1,811,617	108,973	6%
National Protection and Programs Directorate	1,188,263	2,432,755	2,361,715	(71,040)	-3%
Office of Health Affairs	157,621	139,250	212,734	73,484	53%
Federal Emergency Management Agency	5,971,159	6,194,268	6,527,406	333,138	5%
FEMA: Grant Programs	4,220,858	4,165,200	4,000,590	(164,610)	-4%
U.S. Citizenship & Immigration Services	2,876,348	2,859,997	2,812,357	(47,640)	-2%
Federal Law Enforcement Training Center	332,986	282,812	278,375	(4,437)	-2%
S&T Directorate	932,587	1,006,471	1,018,264	11,793	1%
Domestic Nuclear Detection Office	514,191	383,037	305,820	(77,217)	-20%
TOTAL:	$ 52,771,076	$ 55,388,333	$ 56,335,737	$ 947,404	1.71%
Less Rescission of Prior Year Carryover Funds: [4]	(61,373)	(40,474)	-	40,474	-100%
ADJUSTED TOTAL BUDGET AUTHORITY:	$ 52,709,703	$ 55,347,859	$ 56,335,737	$ 987,878	2%
SUPPLEMENTAL: [5]	$ 3,354,503	$ 295,503	$ -	$ (295,503)	$ -
Less Rescission of Prior Year Carryover Funds: [5]	$ (100,000)	$ -	$ -	$ -	

1/ FY 2009 revised enacted reflects:
- Net reprogramming/transfer adjustments for OSEM ($17.4 million); OIG ($16.0 million); CBP ($-24.1 million); ICE ($16.4 million); TSA (14.4 million); USCG ($.400 million); USSS ($ 2.5 million); NPPD ($30 million); OHA ($.430 million); FEMA ($-39.5 million).
- Technical adjustments to revise fee/trust fund estimates for ICE - Immigration Inspection User Fee ($7.0 million); ICE - Detention and Removal Examination Fee ($1.4 million); ICE - Breached Bond/Detention Fund ($15.0 million); TSA - Transportation Threat and Credentialing - Registered Traveler (-$10.0 million), TSA - Transportation Threat and Credentialing - Transportation Worker Identification Credentials ($22.7 million); TSA - Transportation Threat and Credentialing - HAZMAT (-$3.0 million); TSA - Transportation Threat and Credentialing - Alien Flight School ($1.0 million); CIS ($185.4 million); USCG ($7.9 million).
- Realignment of USCG Operating Expenses funding and Pursuant to P.L. 110-53 reflects TSA realignment of funds for 9/11 Commission Act implementation ($3.675 million - Aviation Security, 13.825 million - Surface, $2.5 million - Support).
- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$20.0 million).

2/ FY 2010 revised enacted reflects:
- Technical adjustments for TSA Aviation Security Fees of ($128.9 million); USCG Health Care Fund ($5.0 million).
- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$.800 million).
- For comparability purposes, excludes USCG Overseas Contingency Operations ($241.5 million) and National Science Foundation transfer to USCG of $54.0 million.

3/ Departmental Operations is comprised of the Office of the Secretary & Executive Management, the Office of the Federal Coordinator for Gulf Coast Rebuilding, the Office of the Undersecretary for Management, the Office of the Chief Financial Officer, the Office of the Chief Information Officer, and the National Special Security Events Fund (NSSE).

4/ Pursuant to P.L. 110-329, reflects FY 2009 rescissions of prior year unobligated balances: Analysis and Operations (-$21.373 million); TSA (-$31.0 million); FEMA - Cerro Grande (-$9.0 million).
Pursuant to P.L. 111-83, reflects FY 2010 rescissions of prior year unobligated balances: Analysis and Operations (-$2.4 million); TSA (-$4.0 million); Counter-Terrorism Fund (-$5.6 million); FEMA ($-5.6 million); S&T ($-6.9 million); DNDO (-$8.0 million).

5/ In order to obtain comparable figures, Net Discretionary, Gross Discretionary, and Total Budget Authority excludes:
- FY 2009 supplemental funding pursuant to P.L. 110-252: USCG ($112 million).
- FY 2009 supplemental funding pursuant to P.L. 111-5 (ARRA): USM ($200 million); OIG ($5 million); CBP ($680 million); ICE ($20 million); TSA ($1.0 Billion); USCG ($240 million); FEMA ($610 million);.
- FY 2009 supplemental funding pursuant to P.L. 111-8: USSS ($100 million).
- FY 2009 supplemental funding pursuant to P.L. 111-32: CBP ($51.2 million); ICE ($66.8 million); USCG ($139.5 million); FEMA ($130.0 million).
- Pursuant to P.L. 111-32 reflects FY 2009 rescissions of prior year unobligated balances: FEMA (-$100.0 million).
- FY 2010 Overseas Contingency Operations funding provided in P.L. 111-83: USCG ($241.5 million);
- FY 2010 Supplemental funding pursuant to P.L. 111-117: USCG ($54.0 million);

NET DISCRETIONARY AUTHORITY BY ORGANIZATION

Excludes Discretionary Offsetting Fees & Mandatory, Non-Offsetting Fees, & Trust Funds

	FY 2009 Revised Enacted [1]	FY 2010 Revised Enacted [2]	FY 2011 President's Budget	FY 2011 +/- FY 2010 Enacted	FY 2011 +/- FY 2010 Enacted
	$000	$000	$000	$000	%
Departmental Operations [3]	$ 659,109	$ 802,931	$ 1,270,821	$ 467,890	58%
Analysis and Operations	327,373	335,030	347,930	12,900	4%
Office of the Inspector General	114,513	113,874	129,806	15,932	14%
U.S. Customs & Border Protection	9,803,667	10,134,554	9,817,117	(317,437)	-3%
U.S. Immigration & Customs Enforcement	5,005,615	5,436,952	5,523,800	86,848	2%
Transportation Security Administration	4,369,358	5,129,505	5,724,000	594,495	12%
U.S. Coast Guard	8,104,707	8,541,749	8,466,537	(75,212)	-1%
U.S. Secret Service	1,415,444	1,482,644	1,571,617	88,973	6%
National Protection and Programs Directorate	1,188,263	1,317,755	1,246,715	(71,040)	-5%
Office of Health Affairs	157,621	139,250	212,734	73,484	53%
Federal Emergency Management Agency	2,777,560	2,963,268	3,292,860	329,592	11%
FEMA: Grant Programs	4,220,858	4,165,200	4,000,590	(164,610)	-4%
U.S. Citizenship & Immigration Services	152,490	224,000	385,800	161,800	72%
Federal Law Enforcement Training Center	332,986	282,812	278,375	(4,437)	-2%
S&T Directorate	932,587	1,006,471	1,018,264	11,793	1%
Domestic Nuclear Detection Office	514,191	383,037	305,820	(77,217)	-20%
TOTAL:	$ 40,076,342	$ 42,459,032	$ 43,592,786	$ 1,133,754	2.67%
Less Rescission of Prior Year Carryover Funds: [4]	(61,373)	(40,474)	-	40,474	-100%
Mandatory, Fees, and Trusts	12,694,734	12,929,301	12,742,951		
ADJUSTED TOTAL BUDGET AUTHORITY:	$ 52,709,703	$ 55,347,859	$ 56,335,737	$ 987,878	2%
SUPPLEMENTAL: [5]	$ 3,354,503	$ 295,503	$ -	$ (295,503)	$ -
Less Rescission of Prior Year Carryover Funds: [5]	$ (100,000)	$ -	$ -	$ -	

1/ FY 2009 revised enacted reflects:

- Net reprogramming/transfer adjustments for OSEM ($17.4 million); OIG ($16.0 million); CBP ($-24.1 million); ICE ($16.4 million); TSA (14.4 million); USCG ($.400 million); USSS ($ 2.5 million); NPPD ($30 million); OHA ($.430 million); FEMA ($-39.5 million).
- Technical adjustments to revise fee/trust fund estimates for ICE - Immigration Inspection User Fee ($7.0 million); ICE - Detention and Removal Examiniation Fee ($1.4 million); ICE - Breached Bond/Detention Fund ($15.0 million); TSA - Transportation Threat and Credentialing - Registered Traveler (-$10.0 million), TSA - Transportation Threat and Credentialing - Transportation Worker Identification Credentials ($22.7 million); TSA - Transportation Threat and Credentialing - HAZMAT (-$3.0 million); TSA - Transportation Threat and Credentialing - Alien Flight School ($1.0 million); CIS ($185.4 million); USCG ($7.9 million).
- Realignment of USCG Operating Expenses funding and Pursuant to P.L. 110-53 reflects TSA realignment of funds for 9/11 Commission Act implementation ($3.675 million - Aviation Security, 13.825 million - Surface, $2.5 million - Support).
- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$20.0 million).

2/ FY 2010 revised enacted reflects:

- Technical adjustments for TSA Aviation Security Fees of ($128.9 million); USCG Health Care Fund ($5.0 million).
- Scorekeeping adjustment for a rescission of prior year unobligated balances from USCG - AC&I (-$.800 million).
- For comparability purposes, excludes USCG Overseas Contingency Operations ($241.5 million) and National Science Foundation transfer to USCG of $54.0 million.

3/ Departmental Operations is comprised of the Office of the Secretary & Executive Management, the Office of the Federal Coordinator for Gulf Coast Rebuilding, the Office of the Undersecretary for Management, the Office of the Chief Financial Officer, the Office of the Chief Information Officer, and the National Special Security Events Fund (NSSE).

4/ Pursuant to P.L. 110-329, reflects FY 2009 rescissions of prior year unobligated balances: Analysis and Operations (-$21.373 million); TSA (-$31.0 million); FEMA - Cerro Grande (-$9.0 million).

Pursuant to P.L. 111-83, reflects FY 2010 rescissions of prior year unobligated balances: Analysis and Operations (-$2.4 million); TSA (-$4.0 million); Counter-Terrorism Fund (-$5.6 million); FEMA ($-5.6 million); S&T ($-6.9 million); DNDO (-$8.0 million).

5/ In order to obtain comparable figures, Net Discretionary, Gross Discretionary, and Total Budget Authority excludes:

- FY 2009 supplemental funding pursuant to P.L 110-252: USCG ($112 million).
- FY 2009 supplemental funding pursuant to P.L. 111-5 (ARRA): USM ($200 million); OIG ($5 million); CBP ($680 million); ICE ($20 million); TSA ($1.0 Billion); USCG ($240 million); FEMA ($610 million);.
- FY 2009 supplemental funding pursuant to P.L. 111-8: USSS ($100 million).
- FY 2009 supplemental funding pursuant to P.L. 111-32: CBP ($51.2 million); ICE ($66.8 million); USCG ($139.5 million); FEMA ($130.0 million).
- Pursuant to P.L. 111-32 reflects FY 2009 rescissions of prior year unobligated balances: FEMA (-$100.0 million).
- FY 2010 Overseas Contingency Operations funding provided in P.L. 111-83: USCG ($241.5 million);
- FY 2010 Supplemental funding pursuant to P.L. 111-117: USCG ($54.0 million).

AR 001177

KEY FY 2009 ACCOMPLISHMENTS & REFORMS

In 2009, our 230,000 employees strengthened existing efforts and launched new initiatives to meet our five key responsibilities: guarding against terrorism; securing our borders; engaging in smart, effective enforcement of immigration laws; preparing for, responding to and recovering from disasters of all kinds; and building a mature and unified Department.

DHS has emphasized three cross-cutting approaches to achieve these aims—increasing cooperation with federal, state, tribal, local, private sector, and international partners; deploying the latest science and technology to support our mission; and maximizing efficiency and streamlining operations across the Department.

As a result, we have made major advances in addressing new and emerging threats to keep our homeland safe, fostering lawful trade and travel and continuing to build a ready and resilient nation able to meet the challenges of the 21st century. The following are some key initiatives accomplished this past year.

Guarding Against Terrorism and Threats to Cyber Networks and Critical Infrastructure

Protecting the American people from terrorist threats is the founding purpose of the Department and a top priority. Over the past year, DHS has continued to guard against terrorism by enhancing explosives detection and other protective measures in public spaces and transportation networks, working with the private sector to protect critical infrastructure and cyber networks from attack, improving detection of chemical, biological, radiological, and nuclear materials, and building information-sharing partnerships with state and local law enforcement that enable law enforcement to better mitigate threats.

- Fulfilling a key 9/11 Commission recommendation, TSA began implementing Secure Flight, which prescreens passenger name, date of birth and gender against government watch lists for domestic and international flights.

- TSA achieved the 9/11 Act requirement of screening 50 percent of air cargo transported on domestic passenger aircrafts by February 3, 2009. Currently, 100 percent of cargo is screened on more than 95 percent of flights originating in the United States and 100 percent of all baggage is screened for explosives

- The Domestic Nuclear Detection Office directly trained more than 3,600 federal, state and local officers and first responders in radiological and nuclear detection and began demonstrating the first-of-its-kind Cargo Advanced Automated Radiography System, which aims to detect special nuclear materials and shielding material in cargo at ports of entry.

- DHS opened the new National Cyber Security and Communications Integration Center—a 24-hour, DHS-led coordinated watch and warning center that will improve national efforts to address threats and incidents affecting the Nation's critical IT and cyber infrastructure.

- DHS worked with the Office of Personnel Management to attain new authority to recruit and hire up to 1,000 cyber security professionals across the Department over the next 3 years to

help fulfill DHS' broad mission to protect the Nation's cyber infrastructure, systems and networks.

- S&T partnered with the U.S. Secret Service, industry and academia to digitize more than 9,000 ink samples to expedite the investigation of criminal and terrorist activities by reducing matching times from days to minutes.
- DHS held the 5-day National Level Exercise 2009—the first national level exercise to focus on terrorism prevention—in conjunction with federal, state, local, tribal, private sector and international partners.
- In accordance with the Chemical Facilities Anti-Terrorism Standards Act (CFATS), which allows DHS to regulate the security measures at high-risk chemical facilities, DHS is working with 2,300 facilities on strengthening security measures. In 2009, DHS received Site Security Plans from over 900 regulated facilities.
- DHS signed agreements to prevent and combat crime with Italy, Greece, Portugal and Spain. These agreements allow for the exchange of biometric and biographic data to bolster counterterrorism and law enforcement efforts while emphasizing privacy protections.
- DHS and Spanish Interior Minister Perez Rubalcaba signed a Declaration of Principles formalizing the Immigration Advisory Program—which identifies high-risk travelers at foreign airports before they board aircraft bound for the United States.
- DHS forged partnerships with Germany and Spain to facilitate scientific research and collaboration to combat transnational threats.
- DHS and Canadian Public Safety Minister Peter Van Loan announced a series of cooperative initiatives between the United States and Canada to address terrorism and organized crime while expediting the lawful flow of travel and trade—including a biometric data sharing initiative also involving Australia, the United Kingdom and, eventually, New Zealand.

Securing our Borders while Facilitating Lawful Travel and Trade

In 2009, DHS continued to strengthen security on the Southwest border through additional manpower and new technology to disrupt the flow of illegal drug, cash and weapon smuggling that fuels cartel violence in Mexico. The Department also reinforced security on the northern border while facilitating lawful travel and trade.

- The Obama administration announced the Southwest Border Security Initiative, a joint effort of the Departments of Homeland Security, Justice and State to crack down on Mexican drug cartels by enhancing border security through additional personnel, increased intelligence capability and better coordination with state, local and Mexican law enforcement authorities. As of December 8, 2009, CBP has seized more than $38.3 million in southbound currency—an increase of more than $29.3 million compared to the same period in 2008. In total thus far in 2009, CBP and ICE have seized more than $101.7 million and nearly 1.59 million

kilograms of drugs—an increase of more than $48.2 million and more than 423,167 kilograms of drugs compared to the same period in 2008.

- DHS implemented the Western Hemisphere Travel Initiative for land and sea travel to the United States, increasing border security while facilitating lawful travel and trade by requiring U.S. and Canadian citizens to present a passport or other approved secure document that denotes identity and citizenship when crossing the border.

- DHS and the Department of Justice joined with the Office of National Drug Control Policy to release the National Southwest Border Counternarcotics Strategy, the Obama administration's strategy to stem the flow of illegal drugs and their illicit proceeds across the southwest border and reduce associated crime and violence.

- The Department announced the expansion of Global Entry—a CBP pilot program that streamlines the screening process at airports for trusted travelers through biometric identification—as a permanent voluntary program at airports across the United States. Global Entry reduces average wait times by more than 70 percent and more than 75 percent of travelers using Global Entry are admitted in less than five minutes.

- DHS launched a joint Coast Guard-CBP effort to use Predator Unmanned Aerial Systems (UAS) to provide improved surveillance of the United States' maritime borders. DHS will conduct the first UAS operations along maritime borders in 2010.

- DHS, the Department of Justice and the Government of Mexico signed a Letter of Intent to develop a coordinated and intelligence-driven response to the threat of cross-border smuggling and trafficking of weapons and ammunition. This first-of-its-kind arrangement leverages the combined investigative capabilities of ICE, the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Attorney General of Mexico to combat violence and criminal activity along the U.S.-Mexico border.

- Through Global Entry, DHS launched a first-of-its-kind initiative with the Netherlands to open membership in U.S. and Dutch expedited air travel programs to citizens of both countries in an effort to streamline entry processes for pre-screened fliers.

Engaging in Smart, Effective Immigration Law Enforcement

Over the past year, DHS has strengthened its immigration enforcement activities, targeting criminal aliens and employers who violate the nation's immigration laws, while making improvements to the legal immigration system.

- DHS implemented a new, comprehensive strategy to reduce the demand for illegal employment and protect employment opportunities for the Nation's lawful workforce by targeting employers who knowingly hire illegal workers through investigations, prosecution and civil and criminal penalties. Since January 2009, DHS' new worksite enforcement policies have led to 1,897 cases and 2,069 Form I-9 inspections targeting employers, 58 companies and 62 individuals debarred, and 142 Notices of Intent to Fine totaling $15,865,181 issued.

- DHS is reforming the immigration detention system, enhancing security and efficiency nationwide while prioritizing the health and safety of detainees. New initiatives include creating an Office of Detention Policy and Planning to ensure uniform conditions of confinement, medical care and design; implementing a medical classification system; centralizing all detention facility contracts under ICE headquarters' supervision; developing a plan for alternatives to detention; more than doubling the number of federal personnel providing onsite oversight at the facilities where the majority of detainees are housed; creating two advisory boards comprised of community and immigration advocacy groups; and establishing an independent Office of Detention Oversight reporting directly to the ICE Assistant Secretary.

- DHS expanded the Secure Communities initiative—which uses biometric information to target criminal aliens in U.S. correctional facilities—from 14 to 107 locations in 2009, reflecting an increased emphasis on identifying and removing criminal aliens who pose the greatest threat to public safety. To date, the program has identified more than 111,000 aliens in jails and prisons who have been charged with or convicted of criminal offenses.

- USCIS and the FBI cleared the backlog of a year or more for background checks on people seeking to work and live in the United States or become citizens—reflecting DHS' commitment to quick, thorough and fair adjudication of immigration applications. The vast majority of these checks are now answered within 30 days. At the end of fiscal year 2009, USCIS also reduced the backlog of pending immigration applications and petitions by more than 90 percent and reduced average processing times for naturalization applicants by nearly 5 months as compared to FY 2008.

- USCIS launched a redesigned website—available in English and Spanish—which provides a one-stop location for immigration services and information, including real-time alerts on the status of immigration applications via text message and e-mail.

- USCIS increased employer participation in E-Verify, the nation's preeminent employment eligibility verification system, from 88,000 companies at the end of FY 2008 to more than 177,000 employers today.

Preparing for, Responding to and Recovering from Disasters

In the event of a terrorist attack, natural disaster or other large-scale emergency, the Department provides a coordinated, comprehensive federal response and works with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. This year, DHS increased efforts to build a ready and resilient nation by providing grants and training to our homeland security and law enforcement partners, coordinating the federal government's response to H1N1, and streamlining rebuilding and recovery along the Gulf Coast.

- DHS led the federal response to the H1N1 outbreak, creating regional coordination teams comprised of representatives from DHS and the Departments of Defense and Health and Human Services to oversee, coordinate and execute national incident management responsibilities. DHS also coordinated outreach efforts to congressional, state, local, tribal, private sector and international officials regarding the H1N1 outbreak.

- Since January 20, 2009, Louisiana and Mississippi have received more than $2.1 billion in public assistance from DHS, including $125 million for debris removal and emergency protective measures, $935.5 million in public works and infrastructure projects, $258 million for mitigation activities to increase resilience and more than $542 million for K-12 education. In addition, more than 6,000 displaced households in Louisiana and Mississippi have been transitioned to permanent housing.
- To cut through red tape and streamline and expedite the decision-making process for public assistance for recovery efforts in the Gulf Coast, DHS established two joint public assistance teams and a new arbitration process to resolve longstanding issues over public assistance funding. Over the past 10 months, the Joint Expediting Team and the Unified Public Assistance Project Decision Team have resolved 156 projects, distributing more than $100 million dollars to support the repair and replacement of fire and police stations, schools like the Southern University of New Orleans and Holy Cross School, libraries and other infrastructure critical to the recovery of Gulf Coast communities.
- FEMA has responded to 47 declared disasters since January 21, 2009, including the Red River flooding in North Dakota and Minnesota, the September flooding in Georgia and the earthquake and tsunami that struck American Samoa.

Unifying and Maturing DHS

Six years since the Department's creation, DHS' goal remains the same: one enterprise dedicated to a shared vision for homeland security. Over the past year, DHS implemented a series of wide-ranging efficiency initiatives that leverage the economies of scale in DHS in order to recover millions of dollars and create a culture of responsibility and fiscal discipline. At the same time, the Department leveraged new technology to improve DHS operations, coordination and outreach.

- DHS broke ground on its new headquarters at the St. Elizabeths Campus. While DHS currently operates in more than 40 offices around the National Capitol Region, the consolidated headquarters will unify DHS' many components into one cohesive department and is expected to save taxpayers $163 million over the next 30 years.

- DHS launched the Efficiency Review Initiative to improve efficiency, streamline operations and promote greater accountability, transparency and customer satisfaction through a series of initiatives—including eliminating non-mission critical travel, renegotiating contracts, utilizing government facilities instead of private rentals, reducing printing and postal mail and maximizing the use of web-based communication, training and meetings, implementing energy efficiencies in DHS facilities and maximizing DHS' buying power to receive the lowest price possible when acquiring office supplies and software licenses. These initiatives collectively are expected to lead to hundreds of millions of dollars in cost avoidances. This past year, DHS identified more than $100 million in cost savings including $22 million by eliminating non-mission critical travel; $16 by utilizing software licensing agreements DHS-wide; $7 million through the mandatory review of contracts; $9 million by eliminating redundancy in processing mariner credentials; $8 million by consolidating the DHS sensitive-but-unclassified portal system; almost $4 million by posting documents online or using e-mail in lieu of printing and postal mail; $2 million by streamlining boat maintenance and support schedules; $2 million by utilizing government facilities instead of private

rentals; almost $2 million by increasing energy efficiencies at facilities and many more examples across the Department.

- S&T launched the Virtual USA initiative, an innovative, information-sharing initiative that helps federal, state, local and tribal first responders communicate during emergencies by linking disparate tools and technologies in order to share the location and status of critical assets and information—such as power and water lines, flood detectors, helicopter-capable landing sites, emergency vehicle and ambulance locations, weather and traffic conditions, evacuation routes and school and government building floor plans—across federal, state, local and tribal governments.

Selected DHS High Priority Performance Goals

Preventing Terrorism and Enhancing Security

- **Improve security screening of passengers, baggage, and employees while expediting the movement of the traveling public (aviation and surface transportation security).**

  FY2011 Initiatives include deploying new technology, law enforcement and canine assets at domestic airports, enhancing checkpoint technology, implementing the Transportation Workers Identification Credential (TWIC) program—which requires transportations workers to obtain a biometric identification card to gain access to secure areas of transportation facilities, and strengthening our Visible Intermodal Prevention and Response (VIPR) teams— which use unpredictability to deter, detect, and disrupt potential terrorist activities, will help us to achieve these goals.

Securing and Managing Our Borders

- **Prevent terrorist movement at land ports of entry and maritime borders through enhanced screening while expediting the flow of legitimate travel.**

  FY2011 initiatives include implementing the Western Hemisphere Travel Initiative by deploying new technology, upgrading our processing capabilities at border checkpoints, and enhancing information sharing among law enforcement, as well as continuing recapitalization of aging Coast Guard surface and air assets to quickly and effectively respond to emerging threats.

Enforcing and Administering Our Immigration Laws

- **Improve the efficiency of the process to detain and remove illegal immigrants from the United States.**

- **Improve the delivery of immigration services.**

  FY2011 initiatives include increasing our targets for detaining and removing dangerous criminal aliens from the United States through our Secure Communities program—which uses biometrics to identify and remove criminal aliens incarcerated in state and local jails—by four percent per

AR 001183

year. Additionally, we will improve the delivery of immigration services by modernizing our adjudication process for new immigrants and potential citizens.

Ensuring Resilience to Disasters

- **Strengthen disaster preparedness and response by improving FEMA's operational capabilities and enhancing State, local and private citizen preparedness**

  In FY2011, FEMA will continue to enhance its training programs to help state and local entities prepare for all types of disasters. FEMA is also developing a national strategy to house up to half a million households within sixty days of a disaster—increasing current capacity by 200 percent.

Maturing and Strengthening the Homeland Security Enterprise

- **Mature and unify the Homeland Security Enterprise through effective information sharing.**

- **Improve acquisition execution across the DHS acquisition portfolio, by ensuring key acquisition expertise resides in major program office and acquisition oversight staffs throughout the Department.**

  In FY2011, our efforts will focus on information sharing across all departmental components. Additionally, the department is undertaking an initiative to enhance the capability and capacity of its acquisition workforce to ensure that major acquisition projects do not exceed cost, schedule, and performance objectives.

We will focus on these goals over the next two years and continue to work closely with the Office of Management and Budget in the monitoring and reporting of milestones and performance measures associated with them. As we continue the Bottom-Up Review associated with the QHSR, we may update these goals and associated measures.

CONCLUSION

The FY 2011 budget proposal reflects this administration's continued commitment to protecting the homeland and the American people through the effective and efficient use of DHS resources. As outlined in my testimony today, the Department will build on past successes in several areas including information sharing with our partners, aviation and port security measures and immigration reform efforts.

Thank you for inviting me to appear before you today. I look forward to answering your questions and to working with you on the FY 2011 Budget Request and other issues.

AR 001184

Advanced Imaging Technologies: Passenger Privacy Protections

Fiscal Year 2010 Report to Congress

February 25, 2010

Transportation Security Administration

Message from the Acting Administrator

February 25, 2010

I am pleased to present the following report, "Advanced Imaging Technologies: Passenger Privacy Protections," prepared by the Transportation Security Administration. The report was compiled pursuant to the language set forth in the Joint Explanatory Statement that accompanies the Fiscal Year 2010 Department of Homeland Security Appropriations Act (P.L. 111-83). The report provides details and strategy for a comprehensive program to ensure passenger privacy related to advanced imaging technologies.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at (571) 227-2801 or to the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely,

Gale D. Rossides
Acting Administrator
Transportation Security Administration

Executive Summary

Advanced Imaging Technology (AIT) is a passenger screening capability that is used at airport checkpoints to screen passengers for concealed weapons (metal and non-metal), explosives and other prohibited items. AIT affords Transportation Security Officers (TSOs) the opportunity to review anomalies on an individual and to determine whether additional screening procedures are required to clear passengers through the screening process. AIT functions as a primary passenger screening technology instead of a Walk-Through Metal Detector. The use of AIT for passenger screening is voluntary, and the Transportation Security Administration (TSA) has implemented substantial privacy protections in the design and implementation of AIT.

TSA has assessed multiple types of AIT systems, including backscatter x ray and millimeter wave. Both offer safe and effective screening for weapons, explosives and other prohibited items concealed on a person's body. The backscatter system uses x rays that penetrate clothing, but not skin, to create an image of a person's body. Millimeter wave technology uses non-ionizing radio frequency energy in the millimeter wave spectrum to generate an image based on the energy reflected from the body. TSA implemented both technology and process protections to ensure that passenger privacy and anonymity are maintained during screening.

For example, TSA required manufacturers to include software algorithms in AIT systems that enhance privacy by blurring the face or the image of the body. All AIT machines are delivered to airports without the capability to store, print or transmit images and cannot be modified. TSA required AIT machines to have the capability to retain and export imagines *only* for use in the testing mode for training and evaluation purposes; testing is done at the TSA Systems Integration Facility and the Transportation Security Laboratory. TSOs operating in the airport environment are not capable of putting AIT into the test mode. Further, to avoid the possibility that a specific individual may be associated with an image, TSA physically separates from the screening location the TSO who views the AIT image. Finally, AIT screening is voluntary. The passenger may choose whether to undergo screening by this technology or undergo a pat down. In our operational testing of the technology, more than 98 percent of passengers opt for AIT screening.

TSA continues to explore additional privacy protections in the use of AIT systems. An important objective of the AIT program is to enhance these systems with automated threat detection capability. Automated threat detection software will address many privacy concerns because there will be no need to view images of passengers who do not alarm the system. Automated threat detection will require extensive software development and testing to ensure effective detection with minimal false alarms. TSA is working actively with the Department of Homeland Security's Science and Technology Directorate, the security industry and international government partners to develop an automated threat detection capability that can be installed on deployed U.S. AIT systems.

Advanced Imaging Technologies: Passenger Privacy Protections

Table of Contents

I. Legislative Language 1

II. Background 2

III. Technology Overview 4

IV. Protecting Passenger Privacy 5

V. Appendix A—List of Abbreviations/Acronyms 8

AR 001188

I. Legislative Language

This document complies with the directive set forth in the Joint Explanatory Statement that accompanies the Fiscal Year 2010 Department of Homeland Security (DHS) Appropriations Act (P.L. 111-83). The directive states:

> Within 60 days after the date of enactment of this Act, TSA shall report to the Committees on the details and strategy for a comprehensive program to ensure passenger privacy related to the whole body imaging (WBI) program. At a minimum, this strategy should include: off-site monitoring; adequate privacy safeguards by software or other means; procedures to prohibit storing, transferring, or copying any images produced by the machines; and a concept of operations plan for those passengers that choose a physical search rather than WBI screening.

II. Background

Established in the immediate aftermath of September 11, 2001, the Transportation Security Administration (TSA) is charged with protecting the Nation's transportation systems to ensure the freedom of movement for people and commerce. To that end, TSA's Passenger Screening Program identifies, field tests, procures, deploys and sustains equipment that detects threats concealed on people and in their carry-on items as they enter the airport terminal sterile area.

The emphasis on developing new technologies for passenger screening is codified in 49 U.S.C. § 44925. Pursuant to 49 U.S.C. § 44925(a), the DHS Secretary has an ongoing responsibility to "give a high priority to developing, testing, improving, and deploying, at airport screening checkpoints, equipment that detects nonmetallic, chemical, biological, and radiological weapons, and explosives, in all forms, on individuals and in their personal property." This equipment must detect, under realistic operating conditions, the types of weapons and explosives that terrorists would most likely attempt to smuggle onto an aircraft.

Congress also required the Secretary to develop a strategic plan for the optimal deployment of explosive detection equipment at airport screening checkpoints, specifically citing the use of walk-through explosive detection portals, shoe scanners and backscatter x ray scanners. An updated version of this strategic plan was provided to the Appropriations Committees on September 29, 2008 (see Passenger Checkpoint Screening Program Strategic Plan, Aviation Security, Report to Congress in Response to Conference Report 109-699 to the Fiscal Year 2007 Department of Homeland Security Appropriations Act, August 2008).

Historically, checkpoints have been configured with Walk-Through Metal Detectors (WTMDs) that scan passengers and are positioned in conjunction with x ray technology to scan passengers' associated baggage. While currently deployed x ray technology is able to detect both metallic and non-metallic threats concealed in carry-on luggage, WTMDs for passengers, including the enhanced metal detector, are limited to the detection of metallic threats only.

Threats to aviation are dynamic and constantly evolving to include non-metallic threat objects and liquids (for example, explosives) carried on persons. With the exception of six pilot Advanced Imaging Technology (AIT) units, there are no other currently deployed technologies in the primary passenger screening position that can detect non-metallic items on the passenger's body. Additional intrusive screening methods, such as a full body pat-down, are effective but are time-intensive and cannot be practically applied to all passengers.

To mitigate the non-metallic threat, TSA began evaluating available AIT in 2007. To better assess the application of these technologies to the checkpoint environment, the agency conducted limited field trials of different vendor solutions at multiple airports. Throughout 2007 and 2008, AIT units were utilized in the secondary screening position only (for example, for passengers who set off alarms when going through the WTMD). In 2009, TSA began to evaluate using AIT systems in the primary screening position as an alternative to the WTMD. Deploying AIT systems in a primary position and screening all passengers for both metallic and non-metallic threats allows TSA to utilize the technology to its full capacity. Because of the successful results

observed in these tests, TSA has elected to award contracts for 200 additional AIT units. In the future, continued evaluations will be conducted on other vendors to assess the capabilities of the systems and collect lessons learned to refine the concept of operations and the procedures utilized by the AIT.

III. Technology Overview

AIT options are designed to facilitate the detection of metallic and non-metallic weapons, explosives and other contraband material concealed under multiple layers of clothing by creating images that can be examined to discern these items. TSA is evaluating various types of AIT options, including backscatter x ray, millimeter wave and infrared (IR) technology. All of the technologies generate a computer image of the scanned individual that is displayed on a remote monitor for analysis to determine whether anomalies are present. The effectiveness of these technologies depends on how distinctly the threat objects can be made to stand out against the background and how much of the body can be screened. A Transportation Security Officer (TSO) reviews the image for anomalies that may represent concealed weapons (metallic and non-metallic) and explosives that are placed or carried on the body. The following is an overview of the AIT screening solutions TSA has evaluated:

Backscatter

Backscatter technology relies on a narrow, low-intensity x ray beam scanned over the body's surface at high speed, a portion of which is reflected back from the body and other objects placed or carried on the body, where it is converted into a computer image of the subject and displayed on a remote monitor. For comparison purposes, the x ray dose received from the backscatter system is equivalent to the radiation received in 2 minutes of airplane flight at altitude (.02 millirem for two scans by backscatter compared to .0276 millirem for 2 minutes of flight). Newer technologies require less scanning time, reducing individual x ray exposure to .002 millirem for the entire process. The backscatter AIT meets or exceeds the American National Standards Institute standard for personnel security screening systems using x rays.

Millimeter wave

Millimeter wave technology uses non-ionizing radio frequency energy in the millimeter wave spectrum to generate an image based on the energy reflected from the body. The frequency for millimeter wave technology ranges between 30-300 gigahertz. The three-dimensional image of the body is displayed on a remote monitor for analysis. The energy projected by the system is roughly 10,000 times less than a cell phone transmission.

IR technology

IR-based systems scan for temperature differences on the body's surface or for temperature imbalances between the body, clothes and any hidden objects. IR equipment's effectiveness is a result of its capability to detect minute temperature differences of hidden objects regardless of the organic or inorganic nature of the substance.

IV. Protecting Passenger Privacy

The AIT project addresses the twin goals of ensuring that prohibited items, such as weapons and explosives, do not enter airports' sterile areas while minimizing privacy intrusions. In evaluating privacy protections required of this technology, TSA considered the eight Fair Information Practice Principles (FIPPs) that inform the Privacy Act of 1974 and other privacy laws and regulations within the United States and around the world. TSA addressed the Data Minimization, Purpose Specification, Use Limitation, Data Quality and Integrity, Security and Accountability FIPPs by not retaining passenger images once anomalies are resolved. This procedure also addressed the possibility that images could be hacked, stolen, lost or otherwise misused. The remaining FIPPs were addressed by permitting passengers to decline AIT screening in favor of physical screening (Individual Participation FIPP) and by providing notice to the passenger (Transparency FIPP) at the checkpoint, as well as through extensive information on the TSA website and in published Privacy Impact Assessments. To further ensure passenger privacy, TSA also implemented operational procedures to completely separate the TSO image reviewer from the passenger (making the passenger anonymous to the TSO reviewer) and to address passenger privacy perception issues (in other words, how does this feel for the passenger).

Remote Viewing

The TSO viewing the passenger image created by the AIT is located in a separate room and cannot see the passenger being screened. Likewise, the TSO assisting the passenger at the AIT machine is not permitted to see the AIT image. AIT image data are transmitted in one direction between the checkpoint to the image viewer via a non-networked physical wire and cannot be lost, modified or disclosed. Image data are encrypted and transmitted in a proprietary format that cannot be deciphered without the proprietary technology.

No Image Retention

AIT image storage functions are disabled by the AIT manufacturer before the devices are delivered to TSA and cannot be activated by the TSOs operating the equipment in the airport. Software-based controls are in place to restrict such activation. Images are maintained on the screen only long enough to resolve any anomalies. If a TSO viewing the passenger image created by the AIT sees a suspicious area or prohibited item, the image remains on the screen until the item is cleared either by the TSO recognizing the item on the screen or by a separate TSO at the AIT machine physically patting down the passenger. The image cannot be retained on the computer and is removed from the monitor to permit the next passenger to be screened. Once the TSO goes to the next image, the image from the previous passenger is automatically and permanently deleted. In addition, TSOs are prohibited from bringing any device into the viewing area that has any photographic capability, including cell phone cameras. Rules governing the use of this AIT equipment are documented in standard operating procedures, and compliance with these procedures is routinely reviewed. By not storing images, TSA effectuates six of the eight FIPPs. Because no data are stored, data storage security risks, such as data minimization, secondary use, sharing, quality, security and accountability, are eliminated. In

addition, the computers used to process and present the images are locked with both physical and software controls to prevent the insertion of any storage media or other communication devices.

New Algorithms

Although the current AIT images are anonymous and individuals already are unrecognizable even in a raw state, vendors have placed a blur over the face on the image to address public perceptions regarding privacy or have used software algorithms to alter the image of the entire body to address privacy concerns. AIT vendors are continuing to develop new algorithms that would provide automated threat detection capabilities for passengers who use AIT screening. Acceptable levels of detection and false positive/false negative results must be addressed before such algorithms can be implemented. TSA is working actively with DHS' Science and Technology Directorate, the security industry and international government partners to develop an automated threat detection capability that could be installed on U.S.-deployed AIT systems.

Alternative Screening

AIT screening is optional; passengers may decline AIT screening. Passengers who decline AIT screening must undergo equivalent screening consisting of a physical pat-down to provide an appropriate level of security. This level of choice effectuates the Individual Participation FIPP by permitting the individual to exercise choice to the extent possible.

TSO Training

TSOs operating AITs are given extensive training both in detection of threat items revealed by the AITs and in the operational protocols that protect the privacy of individuals undergoing AIT screening. Specifically, TSOs operating AITs undergo mandatory initial and annual privacy training. TSO supervisors ensure that policies and procedures designed to enhance privacy protections are fully enforced.

Public Messaging

TSA posts signs at each AIT checkpoint to educate the passenger on the technology. The signage includes a sample of the image created by the AIT device, informs passengers that AIT screening is optional and provides safety information about the relative impact of the technology in comparison to everyday activities. In addition, TSA published a Privacy Impact Assessment, provided extensive information on AIT technologies on its Web site[1] (www.TSA.gov) and blog[2] and conducted extensive outreach with press; privacy groups; industry and consumer groups; academics with expertise in security; and cultural, religious, disability and other groups whose

[1] See Imaging Technology, www.tsa.gov/approach/tech/imaging_technology.shtm; TSA Continues Millimeter Wave Passenger Imaging Technology Pilot, www.tsa.gov/press/happenings/at_mmwave_purchase.shtm; TSA to Begin Testing Imaging Technology at George Bush Intercontinental Airport, www.tsa.gov/press/releases/2009/0731.shtm; and TSA to Begin Testing Imaging Technology at Cleveland Hopkins International Airport, www.tsa.gov/press/releases/2009/0730.shtm.

[2] See Imaging Technology: The Bigger Picture, www.tsa.gov/blog/2009/08/imaging-technolgy-bigger-picture.html; Safety & Privacy Concerns Regarding the Millimeter Wave Whole Body Imager, www.tsa.gov/blog/2008/04/safety-privacy-concerns-regarding.html; and Pilot Program Tests Millimeter Wave for Primary Passenger Screening, www.tsa.gov/blog/2009/02/pilot-program-tests-millimeter-wave-for.html.

members may have specific concerns regarding airport checkpoint screening. These efforts effectuate the Transparency FIPP by providing notice to potentially affected individuals about AIT.

V. Appendix A—List of Abbreviations/Acronyms

AIT	Advanced Imaging Technology
DHS	Department of Homeland Security
FIPP	Fair Information Practice Principles
IR	Infrared
TSA	Transportation Security Administration
TSO	Transportation Security Officer
WBI	Whole Body Imaging
WTMD	Walk -Through Metal Detector

AR 001196

U.S. Department of Homeland Security
Washington, DC 20528

FEB 2 6 2010

Homeland Security

ACQUISITION DECISION MEMORANDUM

MEMORANDUM FOR: Gale Rossides
Acting Administrator
Transportation Security Administration

FROM: Elaine C. Duke
Under Secretary for Management

SUBJECT: Passenger Screening Program Acquisition Review

The Department of Homeland Security (DHS) Acquisition Review Board (ARB) reviewed selected projects comprising the Transportation Security Administration's (TSA) Passenger Screening Program (PSP) on September 8 and 11, 2009. This Acquisition Decision Memorandum (ADM) confirms the decisions made by this Deputy Secretary chaired ARB. The attachment to this ADM contains the details of the meeting and the resulting action items.

An Acquisition Decision Event (ADE) 3 approval was granted for the following projects to enter production, deployment and sustainment, and to achieve Full Operational Capability (FOC) consistent with the program's current Acquisition Plan, subject to satisfaction of the action items noted in the attachment to this ADM:

- Advanced Imaging Technology (AIT), and
- Bottled Liquid Scanner (BLS) Project.

ADE 2A/2B approval was granted to proceed with continued development, including securing sufficient vendor units to satisfy testing and evaluation resource requirements for the following technologies:

- Enhanced Metal Detector-2 (EMD-2),
- Shoe Scanner Detection (SSD) for up to 50 units, and
- Advanced Technology (AT) 2.

Due to the quantities and dollar amounts involved in their procurement, the FOC (ADE 3) Decision is delegated to the TSA's Component Acquisition Executive (CAE) for both AT 2 and EMD 2 contingent upon there being at least two vendors on the Qualified Products List, and that the Director, Operational Test and Evaluation was satisfied with Operational Test results.

Authority to proceed into production, deployment, and sustainment for the Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) was removed from consideration during discussion at this ARB at the request of the TSA. The TSA will arrange to return to the ARB when TSA determines this project is ready to proceed to the next ADE.

It is the responsibility of the TSA and the PSP Office to ensure that the results of this ADM and its attachment are promulgated to the affected activities. The Acquisition Program Management Division (APMD) will provide support and assistance to the PSP Program Office. Please send action items, status and supporting documentation to APMD.CAD@hq.dhs.gov. Should you have any questions, please contact W. Page Glennie, APMD, at (202) 447-5492.

Attachment

cc:
Under Secretary for Management
Assistant Secretary for Policy
Deputy Assistant Secretary for Policy
General Counsel
Chief Administrative Officer
Chief Human Capital Officer
Chief Information Officer
Chief Security Officer
Acting Chief Financial Officer
Acting Chief Procurement Officer
Director, Acquisition Program Management Division, OCPO
Director, Cost Analysis Division, OCPO
Head of Contracting Activity, TSA
Component Acquisition Executive, TSA
Director, Test Evaluation and Standards, S&T
Director, Operational Test and Evaluation, S&T
Screening Coordination Office, SCO
Director, Acquisition Program Management Support Division, TSA
Program Manager, PSP, TSA

Acquisition Review Board Discussions and Action Items for Transportation Security Administration Passenger Screening Program September 8 and 11, 2009

The Passenger Screening Program (PSP) identifies, tests, procures, deploys, and sustains equipment that assist detection of explosive threats and prohibited items concealed on people and in their carry-on items as they enter the airport terminal sterile area through the passenger screening checkpoint. The TSA has received $311 million in American Reinvestment and Recovery Act (ARRA) funds to accelerate planned acquisition and deployment of security equipment. The funds will expedite deployment of qualified systems for passenger screening projects to achieve Full Operational Capability (FOC) on an accelerated basis, including the Advanced Technology (AT) carry-on screening systems and Bottled Liquid Scanners (BLS). ARRA funding will also allow TSA to accelerate procurement of Advanced Imaging Technology (AIT) systems (to screen passengers on a non-invasive basis), Universal Conveyor Systems, and Explosive Trace Detectors (ETD). Once these systems are qualified, anticipated benefits include an enhanced threat detection capabilities and improved efficiency of checkpoint operation.

The ARB discussed several areas of the program in depth on September 8, 2009 including:

- Acquisition Strategy. Procurements are being conducted using full and open competition, evaluating the capabilities of multiple vendors against technical and operational requirements for potential placement on a Qualified Products List (QPL). The Program Office is currently pursuing a rolling QPL process to maximize potential vendor participation and to incentivize vendors to develop additional capabilities to thus improve both system effectiveness and efficiency. Although only one vendor had qualified a BLS system, many vendors were given the opportunity to compete, so no sole source Justification and Approval will be required for that project.
- Capabilities Sought. The Program Manager (PM) clarified the capabilities provided by the Enhanced Metal Detector (EMD 2) and the Whole Body Imager (WBI) (which is now designated as AIT) for the Board.
- Technology Selection. The use of non-material solutions was discussed, given the potential for changes in doctrine, organization, training, leadership, and personnel to address identified screening deficiencies that might mitigate the costs and complexity of purely material/technology or facility solutions. The PM noted that these options were being considered but also conveyed the need to minimize the complexity of current screening operations for Transportation Security Officers (TSOs) and other aviation security personnel, while ensuring that screening operations remain compliant with both regulatory and statutory requirements.
- Information Technology. The TSA's Security Technology Integrated Program (STIP) will develop and deploy the capability to remote monitor and maintain aviation security equipment, and is a portion of TSA's Office of Security Technology's acquisition portfolio that is Information Technology (IT) intensive. The various projects comprising the PSP will be initially deployed as non-networked, stand-alone systems. The Office of the Chief Information Officer (OCIO) will conduct an in depth review of STIP as part of its Enterprise Architecture Board process.

The ARB reconvened on September 11, 2009 to continue the review of the PSP. Additional discussion included:

- FOC quantities required and projected timeline for incremental procurements;

- The status of vendors seeking qualification and placement on the QPL, and the remaining portion of FOC quantities; and
- The challenges associated with maximizing vendor participation in the QPL process, specifically, the extent to which vendors were able to satisfy qualification requirements.

An Acquisition Decision Event (ADE) 3 approval was granted for the following projects to enter production, deployment and sustainment, and to achieve FOC consistent with the program's current Acquisition Plan, subject to satisfaction of the action items noted in the attachment to this ADM:

- Advanced Imaging Technology (AIT), and
- Bottled Liquid Scanner (BLS) Project.

ADE 2A/2B approval was granted to proceed with continued development, including securing sufficient vendor units to satisfy testing and evaluation resource requirements for the following technologies:

- Enhanced Metal Detector-2 (EMD-2),
- Shoe Scanner Detection (SSD) for up to 50 units, and
- Advanced Technology (AT) 2.

Authority to proceed into production, deployment, and sustainment for the Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) was removed from consideration during discussion at this ARB at the request of the TSA. The TSA will arrange to return to the ARB when TSA determines this project is ready to proceed to the next ADE.

Due to the quantities and dollar amounts involved in their procurement, the FOC (ADE 3) Decision is delegated to the TSA's Component Acquisition Executive (CAE) for both AT 2 and EMD 2 contingent upon there being at least two vendors on the Qualified Products List, and that the Director, Operational Test and Evaluation was satisfied with Operational Test results.

The following actions must also be completed:

- Action Item. *Documentation Update*. The AIT and the EMD-2 are to update their Life Cycle Cost Estimate (LCCE) and Integrated Logistics Support Plan (ILSP). This action is due within sixty days of the date of the ARB.
- Action Item. *Conduct Testing and Evaluation.* The PSP will ensure that required operational capabilities are demonstrated for the CAT/BPSS and AT 2 projects, as verified and validated through sufficient, credible, and objective testing and evaluation, prior to scheduling the ARB for the ADE 3 review. The Director, Operational Test and Evaluation (DOT&E) will provide a Letter of Assessment (LOA) for each vendor system in support of the ARB, and will work with the program office to develop an integrated master schedule that supports development of the LOAs.
- Action Item. *Complete Oversight of Test and Evaluation Activities.* Consistent with the above action item and those actions from a prior ADM dated September 10, 2009, the PSP, in conjunction with the DHS Testing & Evaluation and Standards Division and DOT&E, will jointly propose a process to ensure continued oversight of testing and evaluation activities throughout the qualification process for subsequent vendor submissions under current projects. To fulfill this, the PSP will submit a Test and Evaluation Master Plan (TEMP) for DOT&E approval no later than January 31, 2010, along with supporting appendices, as required,

documenting this process. In addition, the DOT&E will prepare a separate LOA for each vendor system under test for consideration by the acquisition executive, in support of placement on the applicable QPL.

- Action Item. *Technology Updates and Changes in Key Performance Parameters.* If technologies being used result in the program having to change the Acquisition Program Baseline (APB) or if there are substantial changes in the overall acquisition approach and strategy, including capabilities sought and overarching testing and evaluation strategy, the Program Office must ensure DHS is informed in accordance with the Breach policy in Acquisition Directive 102-01. Additionally, if changes in Key Performance Parameters occur due to added capability for the CAT/BPSS, a review by the ARB will be required to ensure proper adherence to DHS' Credentialing Policy.
- Action Item. *Develop and Reconcile Cost Estimates.* The CAD will work with the PSP Program Office to develop appropriate cost estimates to include a reconciliation with the PSP Program Office's LCCE. These estimates will include Research and Development, Procurement, and Operations and Maintenance costs. This action item is due at the next scheduled ARB, currently anticipated to be in the Fourth Quarter, Fiscal Year 2010 and will be reported by the CAD at that ARB.

It is the responsibility of the TSA and the PSP Office to ensure that the results of the ADM and this attachment are promulgated to the affected activities. The Acquisition Program Management Division (APMD) will provide support and assistance to the PSP Program Office. Please send action items, status and supporting documentation to APMD.CAD@hq.dhs.gov. Should you have any questions, please contact W. Page Glennie, APMD, at (202) 447-5492.

AR 001201

Office of the Chief Procurement Officer
Acquisition Program Management Division

List of Individuals who received the draft Acquisition Decision Memo for **TSA PSP ARB held on September 8 and 14, 2009.**

Core Recipients: Acquisition Review Team Members. Where "No" appears in the Comments column, concurrence is implied. The individual received the document, was aware of the associated deadline, and understood that no response would imply concurrence.

Name	Title	Office	Provided Comments?
Donald Bathurst	Chief Administrative Officer	CAO	No
Gary Carter	Test & Evaluation and Standards	S&T	Yes
Theodore Chuang	Assistant General Counsel	OGC	No
Alan Cohn	Assistant Secretary for Policy	OSO	No
Mark Dayton	Counselor	MGMT	No
Richard Gunderson	Chief Procurement Officer (Acting)	CPO	No
John Higbee	Director, Acquisition Program Management Division	OCPO	No
Jeffery Neal	Chief Human Capital Officer	CHCO	No
George Ryan	Operational Test and Evaluation	S&T	No
Peggy Sherry	Chief Financial Officer (Acting)	CFO	No
Richard Spires	Chief Information Officer	OCIO	No
Jerry Williams	Chief Security Officer	CSO	No

Additional Recipients: Program Office Representatives and Others

Name	Title	Office	Provided Comments?
Cheryl Bumblis	Mgmt & Prgm Analyst	OCIO	No
Bradley Buswell	Chief Of Staff	S&T	No
David Capitano	Director, Oversight and Strategic Support	OCPO	No
Patricia Cogswell	Associate Director	PLCY/SCO	No
Soraya Correa	Director, Office of Procurement Operations	OCPO	No
Mitch Crosswait	Deputy Director, Requirements, Capabilities and Assessments	PLCY/OSP	No
Shawn Flinn	Director, Human Capital Policy	OCHCO	No
Morgan Geiger	Asst. Director	CFO/PA&E	No
Page Glennie	Deputy Director (Acting)	OCPO/APMD	
Margie Graves	Deputy, Chief Information Officer	CIO	No
Paul Grim	Senior Ops Research Analyst	OCPO	No

Stephen Heifetz	Deputy Asst Secretary	PLCY/PDEV	No
Donna Jenkins	Director, Acquisition Workforce	OCPO	No
Kirk Johnson	Senior Program Analyst	PLCY/OSP	No
Michael Karau	Senior Asset Manager	OCAO	No
Jim Manzo	Director, Cost Analysis Division	OCPO	Yes
Kathleen Martin	Deputy General Counsel	OGC	No
Thomas Mason	Director, Strategic Initiatives	OCPO	No
Deirdre McAllister	Project Manager	OCIO/OAT	No
Daniel McLaughlin	Deputy Director	OCPO/OPO	No
Wendy Molzahn	Director, Office of Special Acquisitions	OCPO/OSA	No
Scott Myers	Director, Assets and Logistics Management	OCAO/ALM	No
William Randolph	Director, Procurement Oversight	OCPO	No
Michael Shirk	Program Analyst	CFO/PAE	No
Cedric Sims	Executive Director, Enterprise Business Management	OCIO/EBMO	No
Lee Smith	Director, Enterprise Architecture	EACOE	No
Keith Trippie	Portfolio Manager	OCIO/EBMO	No
Kelli Walther	Director	PLCY/SCO	No
John Whitley	Director	CFO/PAE	No
Dominic Bianchini	Program Manager	TSA	Yes
Dominico Cipicchio	Component Acquisition Exec.	TSA	Yes
Larry Nee	Director, APMSD	TSA	Yes

Homeland Security

Testimony of Gale D. Rossides, Acting Administrator, Transportation Security Administration Before the United States House Subcommittee on Homeland Security Committee on Appropriations

Release Date: March 4, 2010

Washington, D.C.
(Remarks as Prepared)

Good morning Chairman Price, Ranking Member Rogers, and distinguished Members of the Subcommittee. Thank you for the opportunity to appear today to discuss the President's Fiscal Year (FY) 2011 budget request for the Transportation Security Administration (TSA) and the steps the TSA is taking to enhance transportation security.

I want to thank the Subcommittee for consistently ensuring that TSA has the resources to carry out its critical security mission and express my appreciation for your continued partnership in meeting the changing and challenging security threats that confront us. Today I will outline TSA's plans to protect the transportation sector and ask for your support of the President's FY 2011 budget request of $8.2 billion for TSA to help us meet these challenges.

Since 9/11, TSA has employed multiple layers to secure the aviation system and ensure the safety of the traveling public. Long before passengers reach the airport, TSA uses the latest intelligence to influence our daily operational decisions and to provide security information to public and private partners. Passengers are vetted against the No-Fly List to determine who should not receive a boarding pass for a flight to, from, or within the United States and the Selectee List to determine who must go through additional security measures. At the airport, our layered approach to security employs measures both seen and unseen by travelers. The 48,000 Transportation Security Officers (TSOs) at hundreds of airports across the United States screen 1.8 million passengers and their baggage every day using advanced technology X-Ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines, Bottled Liquid Scanners, Advanced Imaging Technology (AIT), full-body pat-downs, and explosives detection systems both at the checkpoint and at other key locations in the airport. Bomb Appraisal Officers (BAOs), and Behavior Detection Officers (BDOs) also assist in the screening process. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security along the airport perimeter and in limited access areas of airports. The $1 billion in the American Recovery and Reinvestment Act of 2009 (ARRA) funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

To support in-flight security, Federal Air Marshals (FAMs) are deployed on domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more pilots volunteer to serve as armed, deputized Federal Flight Deck Officers on domestic flights.

While we have made enormous strides to improve aviation security, terrorists continue to pose a threat to the United States; there is no silver bullet, nor any single measure that provides a 100 percent guarantee of security. Therefore, we cannot afford to become complacent.

The attempted attack on Northwest Flight 253 on Dec. 25, 2009, 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 Department of Homeland Security (DHS) Secretary Janet Napolitano has testified at recent hearings, this Administration is determined to thwart terrorist plots and disrupt, dismantle, and defeat terrorist networks by employing and enhancing the multiple layers of defense that work in concert with one another to secure our country. This effort involves not just TSA, but

components across the DHS and many other Federal agencies as well as State, local, tribal, territorial, private sector, and international partners. TSA works closely with other DHS agencies, such as U.S. Customs and Border Protection (CBP) and the U.S. Coast Guard (USCG), to continually evaluate and improve security programs and processes.

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on Dec. 25, 2009, DHS immediately put in place additional security measures. TSA requested that the Federal Aviation Administration apprise all 128 U.S.-bound international flights from Europe of the attempted attack and asked them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosives detection canine teams, state and local law enforcement, expanded presence of BDOs, and enhanced screening. TSA conducted calls with all major airlines and the Air Transport Association and issued Security Directives and Emergency Amendments for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

On Jan. 3, DHS/TSA issued a new Security Directive, effective on Jan. 4 and still operational today, which includes security measures developed in consultation with law enforcement officials and our domestic and international partners. This Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners.

These steps helped strengthen our security posture to face current threats to our country, yet as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this attack. At President Obama and Secretary Napolitano's direction, DHS and TSA are pursuing new initiatives to enhance the protection of air travel from acts of terrorism. The President's FY 2011 budget request would provide TSA with the resources it needs to carry out these critical new initiatives.

Enhanced Screening Technology

TSA is aggressively pursuing the deployment of enhanced screening technology to domestic airports and encouraging our international partners to do the same. While no technology is guaranteed to stop a terrorist attack, a number of technologies, when employed as part of a multi-layered security strategy, can increase our ability to detect dangerous materials.

To this end, TSA is accelerating deployment of AIT units to increase capabilities to identify materials such as those used in the attempted Dec. 25, 2009, attack. These efforts are already well underway. TSA has 40 machines deployed at 19 airports throughout the United States. Last September, TSA purchased 150 additional AIT units with ARRA funding, and this year, TSA expects to deploy these and at least 300 additional units across the country. The units purchased with ARRA funds are scheduled to be deployed to U.S. airports this summer, with the first units set to arrive at Boston Logan and Chicago O'Hare international airports next week. The President's FY 2011 budget requests $214.7 million to purchase and install an additional 500 AIT units at checkpoints, to bring the total number of AIT units to approximately 1,000. An additional $314.6 million is requested for 5,355 TSO positions to operate these AIT machines at their accelerated deployment pace.

TSA also continues to explore additional privacy protections for AIT machines through automated threat detection, which would transmit images only when an alarm is triggered. In collaboration with the DHS Science and Technology Directorate, 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.

TSA is also increasing assets in the area of explosives detection equipment and highly trained security personnel to strengthen our abilities to find dangerous materials and stop dangerous people from boarding aircraft.

TSA has expanded the random use of Explosives Trace Detection (ETD) machines, which are effective against a wide scope of explosives, to screen both passengers and bags. The President's FY 2011 budget requests $60 million to purchase and supply approximately 800 additional portable ETD machines.

Further, the President's budget seeks approximately $20 million in funding to increase the ranks of BDOs by 350, enhancing coverage of lanes and shifts at Category X, I, II, and III airports and expanding coverage to smaller airports. BDOs provide an extra layer of security based on proven behavior observation and analysis techniques to make timely security risk assessments of travelers. They add an additional measure of unpredictability in aviation security, which is an important feature for disrupting terrorists' ability to plan attacks.

TSA also has determined that critical TSA field locations would benefit from enhanced access to operational intelligence information by providing up-to-date guidance and context to TSA officials stationed in the field, as well as local stakeholders. The President's FY 2011 budget requests $7.1 million to expand TSA's Field Intelligence Officer program by 31 officers to enhance classified communications and information sharing. The more relevant information we can provide to our TSOs, the more equipped they will be to detect and prevent a range of threats.

Nearly 950 Advanced Technology X-Ray machines have been deployed to U.S. airports to enhance the screening of carry-on bags. Additional machines will follow this year and include automated detection software to improve their capability. With support provided by this Subcommittee, TSA will approach full operational capability of this explosives detection technology in FY 2010. As we make improvements in detection capabilities for carry-on bags, it will be important to proceed with AIT deployment for passenger screening to avoid a potential shift of vulnerabilities.

The Explosives Detection Systems (EDS) Strategic Plan outlined a process for achieving optimal screening solutions at 250 commercial airports. This number has been increased to 285 to now incorporate smaller airports. By the end of this fiscal year, it is projected that 200 airports will have one or more operational in-line systems, which provide greater efficiency and increased baggage throughput. TSA appreciates the Subcommittee's continuing support for EDS, which has allowed us to proceed aggressively with these multiyear projects and provide greater attention to medium and smaller airports as projects at larger airports are completed.

To further bolster security, DHS has established a new partnership with the Department of Energy (DOE) and its National Laboratories. The Deputy Secretaries of Homeland Security and Energy are leading the effort to bring the paramount capabilities and critical resources of the DOE National Laboratories to bear on developing advanced technical solutions to key aviation security challenges. This partnership will focus on advancing current technology, assessing system capabilities to determine gaps, and developing emerging technologies to fill those gaps in an efficient and effective manner.

Two years ago, DHS and DOE formed the National Explosive Engineering Sciences Security (NEXESS) Center, a consortium of National Laboratories including Sandia National Laboratory, Los Alamos National Laboratory, and Lawrence Livermore National Laboratory, to provide an agile and aggressive means to anticipate and understand explosive threats and to develop countermeasures to protect the homeland. The NEXESS Center provides informed scientific analysis for short- to mid-term priority assessments as well as mid- to long-term research and technology development. The Deputy Secretaries of both DHS and DOE are working collaboratively to strengthen these efforts in light of the December 25th attempted attack.

Aviation Law Enforcement

To strengthen the presence and capacity of aviation law enforcement, the President's budget requests an additional $85 million to support the costs of increasing the number of FAMs. As a result of threat mitigations put in place following the Northwest Flight 253 incident, FAMS increased coverage of international flights and, as an interim measure, DHS has deployed additional law enforcement officers from across the Department–including the U.S. Secret Service, CBP, U.S. Immigration and Customs Enforcement, and the USCG–to assist FAMs. In January 2010, these highly trained officers participated in an accelerated specialized Federal Air Marshal Service (FAMS)-led training program on the unique methods employed to protect and defend an aircraft. This augmentation program allows FAMS to continue the increased international operational tempo while maintaining appropriate domestic flight coverage. With the funding requested for FY 2011, TSA would sustain the higher level of international flight coverage while continuing domestic flight coverage at appropriate levels.

The President's FY 2011 budget also requests $71 million for an additional 275 proprietary explosives detection canine teams for Category X and I airports. TSA's National Explosives Detection Canine Team Program develops, trains, deploys, and certifies explosives detection canine teams to deter and detect the introduction of explosive devices into the transportation system.

International Partnerships

DHS and TSA will continue to work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in foreign airports and the commitment of our foreign partners to enhance security. DHS leadership has embarked upon an aggressive international outreach initiative to enhance international aviation security standards and practices – particularly for international flights bound for the United States. To build upon and sustain the vision achieved in these international efforts, the President's FY 2011 budget requests an additional $40 million for TSA to develop and promote enhanced global transportation security processes and structures worldwide and to ensure compliance with international and TSA standards. These funds would provide field and support personnel to manage

international programs at 15 existing offices and deploy additional personnel to the Middle East and Africa. TSA plans to add 34 international Transportation Security Specialists, 10 International Industry Representatives, and a 10-person Rapid Response Team. TSA will work proactively with foreign partners by representing TSA in a variety of international and domestic settings, including major transnational aviation-related organizations, regional bodies dealing with transportation security, bilateral cooperative efforts, as well as interagency transportation security efforts.

Because TSA does not conduct screening at international airports, TSA works closely with our foreign partners to ensure international screening standards are followed, particularly for flights bound to the United States. TSA annually conducts approximately 300 airport assessments and inspections at foreign airports using International Civil Aviation Organization (ICAO) standards and inspections of foreign and U.S. air carriers that fly to the United States using TSA standards. If an airport does not meet these standards, TSA works with the host government to rectify the deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. If non-compliance with international standards continues long-term, TSA may recommend suspension of flight service from these airports to the United States.

TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport that is a last point of departure to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level.

Watchlists

As one critical layer of defense, DHS conducts pre-departure passenger screening in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. TSA uses the No-Fly List and the Selectee List, two important subsets within the Terrorist Screening Database managed by the FBI's Terrorist Screening Center, to determine who may board, who requires further screening, and who should be referred to appropriate law enforcement personnel. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, or within the United States. Individuals on the Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

I want to thank the Subcommittee for the support it has provided over the years for TSA's Secure Flight program. Through Secure Flight, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, TSA will fully assume this function in 2010. The transition for domestic carriers will be completed this spring and international carriers are targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination. When fully implemented, Secure Flight will screen more than 2.5 million passengers daily.

Air Cargo Screening

In FY 2009, TSA achieved its goals to require the screening of 50 percent of all cargo on passenger aircraft and 100 percent screening of cargo on all narrow body passenger aircraft. This year we are confident that we will achieve 100 percent screening of all cargo on passenger aircraft departing from U.S. airports by the August deadline mandated under the Implementing Recommendations of the 9/11 Commission Act of 2007. To help reach this goal, TSA developed and implemented the Certified Cargo Screening Program (CCSP), which allows screening of cargo early in the air cargo supply chain by a trusted, vetted, and validated facility. TSA certifies and regulates shippers, indirect air carriers, and other entities to screen cargo prior to its being tendered for transport on passenger aircraft. We are working with the supply chain industry to encourage maximum participation in the CCSP.

TSA air cargo inspectors facilitate air carrier and indirect air carrier implementation of the required security measures and promote compliance through outreach to industry. In FY 2009, TSA's air cargo inspectors completed more than double the number of inspections conducted in the preceding year. With additional resources provided in FY 2010, TSA is increasing inspector ranks by 50 to oversee the implementation of CCSP and validate new program entrants.

TSA also is working with ICAO to develop a "supply chain approach" to securing air cargo on passenger flights, similar to TSA's CCSP. This effort will go a long way toward enhancing the current level of international civil aviation security and in particular to raise the baseline of air cargo security on a global basis.

Finally, TSA is working with other key international partners, on both a bilateral and multilateral basis, to develop

common understandings and objectives for the enhancement of air cargo security standards and to ensure each country's air cargo security systems provide comparable levels of security, both across the air cargo supply chain and in international air transport.

Enhancing Security throughout the Transportation System

TSA's vetting responsibilities have grown significantly in recent years, and TSA has responded with the development and implementation of efficient, reliable, and cost-effective antiterrorism screening programs.

Almost 1.4 million workers–longshoremen, truck drivers, and port employees–requiring unescorted access to secure areas of ports have been enrolled in the Transportation Worker Identification Credential (TWIC) program since October 2007. In FY 2009, TSA's Hazardous Materials Endorsement Threat Assessment Program (HTAP) conducted threat assessments on 297,473 applicants, a continued increase from the program's inception. Operational costs for the TWIC program and the HTAP program are entirely funded by fee revenue.

TSA conducts Visible Intermodal Prevention and Response (VIPR) deployments in all modes of transportation to detect, deter, defeat, and disrupt potential terrorist or criminal activity. VIPR operations employing multi-disciplinary teams of FAMs, Surface Inspectors, BDOs, and TSOs are planned and implemented through a risk-based approach. In FY 2009, TSA completed the hiring and deployment of 10 additional VIPR teams.

Conclusion

In closing, Mr. Chairman, the President's FY 2011 budget request ensures TSA will have the human and technology resources it needs to take critical next steps to improve aviation and transportation sector security. We are expanding and improving the use of technology, strengthening aviation security protocols with our foreign partners, developing long-term law enforcement capacities, and strengthening a TSA workforce that is highly trained, agile and dedicated to this mission. In all of these action areas to bolster security, we are also mindful of our obligations to safeguard the privacy and rights of travelers, and to ensure freedom of movement for people and commerce.

Thank you for your continued support to TSA and for the opportunity to discuss the President's budget request for TSA for Fiscal Year 2011. I would be pleased to respond to your questions.

This page was last reviewed/modified on March 4, 2010.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

CQ CONGRESSIONAL TRANSCRIPTS
Congressional Hearings
March 4, 2010

House Appropriations Subcommittee on Homeland Security Holds Hearing on President Obama's Fiscal 2011 Budget Request for the Transportation Security Administration

---

PRICE:

Subcommittee will come to order. Good afternoon.

We're pleased to welcome Acting Assistant Secretary Gale Rossides to her second budget hearing on transportation security issues before this subcommittee.

Ms. Rossides, at this point you've been Transportation Security Administration's acting assistant secretary for much longer than any of us anticipated.

We all look forward to having some certainty about the long-term leadership of the agency, but in the meantime you have stepped up admirably to the demands of your role. And we appreciate your strong and diligent leadership which I'm confident has made air travel in our country more secure.

So thank you for serving your country with distinction in what is sometimes a thankless job.

Created in the wake of the attacks of September 11th, the initial focus of the TSA was securing the aviation sector in this country. But soon thereafter attacks on London, Madrid and Mumbai pointed to other transportation vulnerabilities, especially in transit systems.

Based upon the threat environment, this subcommittee has worked diligently over the years to fill security gaps in all of our transportation networks.

Since 2003 we've appropriated over $8 billion to get TSA screeners better tools to detect weapons and explosives in luggage and on people. We have appropriated over $400 million for TSA to vet passengers for links to terrorism in order to prevent certain individuals from boarding an aircraft. Additionally Congress has set an August 2010 deadline for screening all cargo on passenger aircraft, appropriating $468 million to date (ph) to accomplish this task.

To address threats outside the aviation environment, Congress has provided $1.8 billion in grants to help local transit agencies and Amtrak secure rail and transit networks.

AR 001210

We worked with the new administration last year to place additional efforts on surface transportation security, with new special response teams or VIPRs, and funding to better coordinate security efforts in non-aviation posts, such as pipelines, highways, motor carriers, mass transit, rail and shipping.

This subcommittee has also encouraged research and development of technologies to thwart threats that have yet to materialize. Well before the Christmas Day bomb plot, TSA had been working to field a solution to the non-metallic explosives threat by testing and evaluating advanced imaging technology -- which this subcommittee supported.

On December 25th when Umar Farouk Abdulmutallab attempted to detonate an explosive device on board a Northwest Airlines flight from Amsterdam to Detroit, our fears about this threat were realized.

As a result, TSA ramped up its procurement and deployment plan for the new screening capacity. For that, you should be commended.

However the failure of Dutch screeners to detect the explosive on Christmas Day was just one piece of the breakdown in our intelligence and aviation security systems that permitted the would-be bomber to get as far as he did.

After ordering a top-down review of all aviation security procedures, including our terrorist watch list system, President Obama initiated a number of reforms, including enhanced screening for passengers flying into the U.S. from or flying through nations on our list of state sponsors of terrorism and other counties of interest; the deployment of additional law enforcement at airports, air marshals on flight, and explosives detection canine teams to keep our air traffic safe; ramped up deployment of passenger screening technologies that can better detect hidden explosives; and, importantly, improvements to the terrorist watch list system, including placing more individuals on the no-fly list.

We will want to discuss your efforts since the announcement of these reforms and of course how your 2011 budget builds on these measures to create a lasting security solution for the American people.

The high-threat environment that we face makes plain the need to close critical gaps in the aviation sector. The 2011 request which totals $7.87 billion overall includes an additional $946 million above the 2010 level for increased measures to secure the nation's airports and flights on the heels of Christmas Day's botched attack.

We would need to closely scrutinize your request today, bearing in mind that the enemy is constantly watching and evolving and that no single tool is a fool-proof solution to the threat.

We will also be watching TSA to ensure that the agency itself is evolving to thwart potential attackers. One thing we rely on to give us perspective on the agency's strategic vision is your annual expenditure plan for checkpoint systems, checked baggage and air cargo.

This plan is our guidebook, indicating how funds will be allocated within various programs. It is routinely updated to address changes in the threat environment or to revise estimates for technology development.

Without knowing what you plan to procure in 2010 for airport checkpoints, we cannot make complete sense of your 2011 budget request for such items as advanced imaging technologies or portable explosive trace machines. We need to know what you're requesting for 2011 is the best use of resources and not just a response to the latest incident.

Today I look forward to learning more about this cohesive strategy. As part of this discussion, we expect you to be able to answer not only why a 9 percent increase in aviation security is a smart investment in 2011, but also whether we're devoting the correct amount of resources to domestic versus international activities.

After all aviation security does not start at our borders. We need to work across the globe to make sure the threats identified are identified at their originating point, not when a terrorist boards an aircraft headed to the United States.

So we'll also want to hear about how TSA and the department are cooperating with foreign authorities to secure air travel worldwide, as well as discuss the optimal mix of manpower and screening technology for the 2011 fiscal year.

I want to thank you again for your service to the country. Look forward to continuing to work with you to ensure our transportation security professionals are equipped with the resources they need to keep the American people safe.

We'll ask you, Ms. Rossides, to take five minutes to summarize your written statement, and we'll be happy to include that full statement in the record.

Let me -- now before you begin, I'd recognize our distinguished, ranking member, Mr. Rogers, for his comment.

ROGERS:

Thank you, Mr. Chairman.

And welcome to -- Ms. Rossides to what is perhaps your final appearance before the subcommittee -- regrettably.

When TSA was established in 2002, I've watched with strong concerns about the agency's inclination to become overly reliant on manpower as opposed to the smart use of effective technology in its efforts to bolster aviation security.

Today, some eight years later, in the wake of another terrorist attack, it feels like deja vu all over again as I review TSA's proposed response to the vulnerabilities exposed by the Christmas Day plot.

Back in 2002 just as today, Congress was presented a request for funds to support thousands upon thousands of screeners rather than a clearly articulated strategy for achieving meaningful aviation security. My concern back then as it is today is that we're not thinking through the proposed security enhancements in terms or portability, effectiveness and adaptability for the next threat (inaudible).

So as I look at the fiscal '11 budget request for more than 500 additional full body imagers and more than 5,300 additional screeners, I'm apprehensive. Because it's unclear whether such a costly and manpower-intensive approach is the absolute best course of action, especially when the initial deployment of these whole body imagers appears to be an iterant (ph) step toward use of even more (inaudible) technology.

My position on enhancing aviation security is one of cautious urgency. Far too often government overreacts in the wake of a crisis. And a reactionary posture is one that habitually leads us into overspending on solutions that don't pan out.

Let me be clear: I'm not saying there isn't some merit in what TSA's proposing for fiscal '11. Rather my concern is that this costly proposal appears to be a short-term fix not long-term, sustainable solution (inaudible) effectively balances legitimate travel, needed security and limited resources.

Unfortunately, these questions cannot be fully answered until we have a better understanding of the direction the TSA is heading in the current fiscal year, which is difficult to do. I know we received TSA's fiscal '10 spending plans as required by law, even though we're well into fiscal '10. But don't get me off on (inaudible).

As this subcommittee continues its oversight responsibilities, I intend to press DHS on the prioritization of its budget. I've made it very clear on previous hearings that I believe the fiscal '11 budget emphasizes aviation security and administration costs at the expense of virtually every other operational security program across the department.

While I do not dispute the need to enhance aviation security and to improve program management, it's important to recall that two very distinct Al Qaida plots were revealed this past year, the Christmas Day attack and the Zazi plot to reportedly detonate an explosive in New York City.

So what this means to me is that we cannot exclusively focus upon the aviation sector at the expense of other areas. (inaudible) must remain vigilant on the entire spectrum of threats facing the country.

Now, having said all that, I would be remiss if I did not take a moment to recognize the notable efforts of all the TSA personnel, who've worked tirelessly to identify solutions to very difficult challenges since the Christmas Day attack.

And finally, Mr. Chairman, I think we need to highlight, as you have, Ms. Rossides' noteworthy service since the establishment of TSA. She's one of the six original employees at TSA -- as young as she is. And she has endured the full range of challenges facing aviation security in the post-9/11 era.

She will be taking up other pursuits but we want to thank you for your service to your country, many years in this chore.

To put it mildly, this subcommittee and our nation owes you a debt of gratitude for your dedicated service.

PRICE:

Thank you very much.

Ms. Rossides, please proceed?

ROSSIDES:

(OFF-MIKE) before you today to ask, on behalf of the Transportation Security Administration, to ask for your support of the president's fiscal year 2011 total budget request of $8.2 billion for TSA, an increase of $512 million over fiscal year '10.

I also thank you both personally for your very kind words. Having been with TSA since its first days, I have witnessed and appreciate our enduring partnership with this subcommittee as we have achieved and continue to strive to meet important objectives toward securing our nation's vital transportation system.

I also greatly appreciate the work we have done with partners at all levels of government, industry representatives, our international partners, the private sector and especially the traveling public we serve.

This year we expect to fully implement our Secure Flight program, a key security vetting measure effected (ph) before airline passengers ever arrive at the airport. GAO as now certified that we have generally met all 10 program certification requirements set by this committee.

We will also screen 100 percent of air cargo on domestic flights by August, and make substantial progress on screening air cargo on international in-bound passenger flights.

We will obligate all $1 billion provided under the Recovery Act, accelerating important passenger and baggage screening enhancements. We will further initiate over $1.3 billion in checkpoint and explosive detections systems with funds provided in fiscal year '10.

We will stand up 15 new VIPR teams dedicated to surface transportation security and serve as the executive agent for decisions on $300 million in FEMA (ph) public transportation and railroad security grants.

TSA operates in a high threat environment, day in and day out. This drives us to be ever vigilant.

The attack on Northwest Flight 253 on Christmas Day was a stark reminder that there are still those who wish to do us harm. They are studying our security measures and will exploit our social norms to their advantage. The men and women of TSA lived with that reality everyday.

I truly appreciate the time that you, Mr. Chairman and Ranking Member Rogers, took to visit our Transportation Security Integration Facility, the TSIF, last week to discuss many of the advancements we are seeking in fiscal year '11, most notably, our advanced imagining technology.

For years TSA has recognized the threat of improvised explosive devices and focused our efforts there. We began testing advanced imaging technology in 2007 to detect both metallic and non-metallic threats hidden in the body. Because of the nearly three years of work we've put into this, we currently have 40 machines already in place at 19 airports. We will field approximately 500 units system-wide by the end of this year, and our F.Y. '11 request of $215 million doubles that equipment capability.

The almost 1,000 units will allow us to screen over 60 percent of all airline passengers with AIT. This requires also 5,000 TSOs which are also requested in our budget along with supporting costs.

I want to emphasize that TSA is the world leader in the marketplace for this advanced imaging technology. And the work we have done to date has paved the way for other countries to follow suit in the wake of the December 25th incident.

TSA does not screen passengers in other countries, but we are committed to helping our foreign partners enhance the security of flights coming into the United States. We have built strong relationships with our international partners, proven by the high level of cooperation we received in December.

Within five hours of TSA issuing new security directives, 95 percent of foreign partners were in compliance. TSA seeks an additional $40 million for our international programs.

Our request also seeks to better equip our TSOs to identify threats with operational intelligence by expanding our field intelligence officer program. We are also requesting $60 million for 800 additional portable explosives trace detection machines, which have proven to be very successful at detecting a wide array of explosives.

We propose to add 350 behavior detection officers. And with an additional $71 million, TSA is requesting to add 275 proprietary canine teams.

The president's budget also requests an additional $85 million for FAMS to sustain domestic and international flight coverage on our highest risk flights.

In closing, I would like to state that TSA's core mission is one of counterterrorism. We continue the work we began eight years ago to close vulnerabilities with new technology and with new processes in a very complex security regime.

As this will likely be my final appearance before the subcommittee as acting assistant secretary, I am extremely grateful for your support of TSA, for our programs, and for the everyday heroes I have been honored to serve alongside with. I appreciate your support in achieving our shared security goals.

And I am happy to respond to your questions.

PRICE:

Thank you very much.

And I'll ask the first such question having to do with the advanced imaging technology.

Over the past two years, the TSA has worked, developed and tested advanced imaging technologies for use in airport screening checkpoints, with an eye toward replacing metal detectors at primary screening checkpoints.

This -- this replacement effort has been well under way, actually, well over a year before the Christmas Day bombing. Because of your efforts TSA was quickly able to develop plans to screen 100 percent of passengers both with AITs and primary, or to use an equivalent method to detect non-metallic threats after the Christmas Day incident.

Unlike pat-downs or traditional metal detectors, DHS believes that AITs, which see beyond the passenger's clothes and identifies threat objects on the body, could've detected the explosive powers that Abdulmutallab smuggled inside his underwear when he went through security in Amsterdam.

AR 001216

Budget request notes that if funded, the 1,000 AITs purchased in 2010 and 2011 would allow this technology to be in place at 75 percent of the country's largest airports.

(inaudible) remains unclear as how you deploy this systems since they have a much larger footprint than metal detectors and a slower processing time. For example, AITs take much longer to scan a single passenger through that metal detector -- a 1.3 seconds versus 22 seconds.

In a briefing with staff, TSA stated that they do not expect increased processing times with AITs because current passengers have to wait on the X-ray to scan their carry-on bags and shoes.

According to TSA, this 20-second X-ray is about the same time -- 22 seconds -- that it takes for an AIT to scan a passenger. I wonder if you could just help us -- help us figure this out.

I really wonder if the AITs will -- will increase wait times. Just give a little more detail there. And -- and if wait times begin growing, how are you going to alleviate the lines of passengers backing up and the potential security threat as they wait to be screened by an AIT?

And what's your deployment plan for the AITs? Is it your intention to deploy AIT equipment within the existing screening checkpoint footprint at all airports? Do you plan on doing a one-on-one replacement for metal detectors? How is this going to move forward?

And then finally, let me just recall the situation we faced when we -- we wanted quickly to be able to screen checked baggage after 9/11. You will recall, TSA placed explosive detection machines in less than ideal locations in a number of airports on a temporary basis, which created a series of problems; ultimately made permanent solutions more costly and more time consuming.

I'm sure that experience is on your mind as you look forward here to how we're going to do the AIT project. How are you going to avoid repeating these same mistakes as you deploy the AIT equipment at already existing screening checkpoints?

ROSSIDES:

Yes, sir. So let me start by talking about the work that's been done to date. We gained a tremendous amount of knowledge from the pilots that we've ran over the last couple of years, in terms of how to process the passengers through, how to measure the wait times.

And from the time the passenger enters the queue to the time that they actually leave the checkpoint, there are multiple processes going on, one of which is walking through the advanced imaging technology, but the other is screening of their carry-on bags.

And it is the combination of those processes working in parallel for the passengers they go through that tells us that we do not believe that deploying these AIT is going to significantly increase the wait times for the passengers.

We also believe that deploying the TSOs in the right positions in the checkpoint to inform the passengers how to properly divest to go into the AIT is going to contribute to keeping those wait times down.

The integration of the AIT equipment into the checkpoint has been something that we have looked at as part of our piloting and as we're looking (inaudible) deployment. We have airports around the country now that have raised their hands and said they are ready to take this technology and put it in their existing checkpoint.

We are confident that those that we're rolling out this year can be done and put in the existing checkpoint and not have to go through major construction issues, not have the kinds of things we had where we had the checked baggage technologies in lobby areas, et cetera.

We're also very much focused on how do we educate the traveling publics so that when they show up at the checkpoint, they understand exactly what they can expect as they go through the AIT machine.

So it's the combination of looking at the entire process within the checkpoint, looking at the public education element, making sure that we have the TSOs properly stationed in front of the equipment so that they can make sure that the passengers are properly divested.

This technology gives us -- gives us such an improvement in the detection capability that we are -- we are looking to make sure that the processes, the technology and the people are all well-integrated so that it is both a very effective screening process as well as very efficient.

PRICE:

The footprint of these machines, though, is greater than the metal detectors.

ROSSIDES:

Yes, it is sir. And what we've found is that in a lot of these airports, as the checkpoints were built, they actually had more room in them -- you know, more room in -- within the checkpoint's footprint itself. And so the initial deployment is to look at those checkpoints that are ready right now to handle this equipment.

PRICE:

And the idea is that the carry-on baggage will still go down the line and be screened...

ROSSIDES:

Yes.

PRICE:

... but that the time the individual stands in the AIT machine will parallel...

ROSSIDES:

Correct.

PRICE:

... or be concurrent with that time used for carry-on screening. And so that's how you come up with a very little net increase in (inaudible) spent.

ROSSIDES:

Right. Correct.

And it is something that we will be very, very focused on, frankly, as travel -- passenger loads increase over the next couple of years. We will look to make sure that we are properly managing, you know, both the queue line. We will also have -- as we're setting these machines up, we will also have the ability to direct the passengers into the advanced imaging technology or through the walk- through (ph) metal detector and receive alternate screening. So we can manage the process that way as well.

PRICE:

And these pilot -- pilot efforts that you've made in the last -- last couple of years to check out this technology, has that also included extensive work on what we're talking about right now, the deploying (inaudible), the way the passenger flow works...

ROSSIDES:

Yes.

PRICE:

... and for that matter, passenger acceptance of the new technology in general?

ROSSIDES:

Yes. Yes. And I am -- I am very, very pleased to be able to report to you that the passenger response to this technology has been overwhelmingly positive. And that was part of our pilot. I believe that we have over 90 percent acceptance rate by the traveling public when they opted to go (inaudible) the equipment.

This has been a great piece of technology for persons with disabilities going through checkpoints.

And so during our pilots we looked at both configuration, we looked at our officer training requirements, we looked at the passenger throughput (ph), and we looked at passenger acceptance.

PRICE:

And by "passenger acceptance," you're also referring to the measures taken to protect privacy?

ROSSIDES:

Yes, sir. And we have signage up in the checkpoint area that informs the passengers that, first of all, that this is optional. They do not have to go through the advanced imaging technology if they choose not to.

It also informs them that the officer that is guiding them through this technology will never see the image that the officer in a remote location is viewing for the detection purposes. And we have made sure that those privacy -- those privacy concerns have been addressed with the public.

We have had a privacy impact statement out during the deployment of the technology and pilot phase. And again we have worked very hard with privacy groups, as well as the traveling public to ensure that they accept and understand the privacy measures that are in place.

PRICE:

Thank you.

Mr. Rogers?

ROGERS:

AR 001220

So continuing on the privacy aspect, the machine makes an image which is telecasted, if you will, to a room where just one person is located, correct? And that's the only place where this image is shown?

ROSSIDES:

Correct.

ROGERS:

The one person in the closed room (inaudible) an employee?

ROSSIDES:

That's right.

ROGERS:

And the face is blurred?

ROSSIDES:

Correct.

ROGERS:

Now you say that this is optional (inaudible) passenger. Suppose they say, "No, I don't want to do that." What do you do then?

ROSSIDES:

Then they are directed through the walk-through metal detector. They could be subjected to hand-wanding and a full-body pat-down so that we are ensuring that an alternative and comparable form of screening is applied to that passenger if they choose not to go (inaudible) the technology.

ROGERS:

So would that -- every person that refuses the whole body imager scan would be patted down?

ROSSIDES:

Possibly. They could be either patted down. They could have a review of their carry-on luggage. And there's a variety of alternative measures that we would have that would be applied depending upon, again, you know, that particular technology that's available in the checkpoint.

ROGERS:

Now is -- this new machine, is it as effective as a pat- down?

ROSSIDES:

From an effectiveness standpoint and an efficiency standpoint it's better because it allows us to view the images quickly, it identifies anomalies on the body, it identifies anomalies that may be in sensitive parts of the body, and it's also very -- it's much faster than doing a full-body pat-down on somebody.

ROGERS:

Well, considering the Christmas Day bomber, would this machine have detected the bomb on that person?

ROSSIDES:

Without going into the specifics of that because of the ongoing criminal investigation, I will tell you that the experience we have had both in the labs and in our pilots, our officers are identifying objects on the body that are comparable to what that threat was.

ROGERS:

Every time?

ROSSIDES:

Our officers are doing a very good job and the...

ROGERS:

Every time?

ROSSIDES:

I'd have to -- I'd have to get back to you, but, you know -- we have very, very good measures in place for evaluating our officers.

ROGERS:

Well, the contrary-wise, if you had patted this man down, would we have found the bomb?

ROSSIDES:

Today we do not do a full-body pat-down that goes into the sensitive parts of the body where that bomb was secreted.

ROGERS:

Now, this machine is not fool-proof, correct? I mean, it's not 100 percent.

ROSSIDES:

It requires the experience of the operator as well, yes.

ROGERS:

We may be getting into some confidential matters here. But what I need to know is, as well you can state it in these circumstances, is this machine the end all?

ROSSIDES:

This machine gives us an increased detection capability that is significantly greater than what we have at the checkpoint today. And what we've been working with industry and these manufacturers -- we are driving these manufacturers to continue to improve this technology because of the demands that we have for aviation security.

ROGERS:

Now, if a bomb were secreted in an oracle of the body, the machine would not detect that of course, would it?

ROSSIDES:

Inside the body?

ROGERS:

Yes.

ROSSIDES:

Correct.

ROGERS:

Correct?

ROSSIDES:

Correct.

ROGERS:

Now on the footprint, the machine would not replace the magnetometers, correct?

ROSSIDES:

Right now, we do not have plans to fully replace all the walk-through metal detectors, that's correct.

ROGERS:

So you would have the metal detectors as well as the full-body imager?

ROSSIDES:

Correct. Right now.

ROGERS:

Why would you need both?

ROSSIDES:

Well, part of it is to manage the flow of the passengers so that we would be able to have an alternative, first, if a passenger says they don't want to go through the advanced imaging technology we would still have the walk-through metal detector. And couple that with, you know, other security measures.

But also what we're looking at right now is, as we're deploying these, maximize the use of the advanced imaging technology but also direct passengers through the walk-through metal detector in checkpoint. So that when a passenger shows up, the security advantage we have, is that when a passenger shows up (inaudible) in the queue line, they will be directed by the officer to either the advanced imaging technology or the whole-body -- the walk-through metal detector, and they won't know. And so the advantage to us is somebody couldn't predict, "I'll get in this line and go through the advanced imaging technology," or "I'll get in this line and go through the walk-through metal detector."

Long term, we hope to drive the industry to actually provide us with the technology where the walk-through metal detector capabilities would be part of the advanced imaging technology equipment.

ROGERS:

So you have a combined machine?

ROSSIDES:

That would be -- that would be a great set-up for us down the road.

ROGERS:

Why haven't we done that?

ROSSIDES:

We are pushing the industry to do that. But we have not gotten -- the industry hasn't gotten to that point yet.

ROGERS:

I'll bet you if you put out a spec and ask for bids you would get some bids pretty quickly.

ROSSIDES:

And I -- I believe we're -- we're asking for that in the labs. And we're working with DHS's Science and Technology lab to actually help us, you know, push the industry toward that.

ROGERS:

That would save money, would it not, in the acquisition and deployment?

ROSSIDES:

I'm not sure that it would, sir. I'd have to get back to you.

ROGERS:

Let me know.

ROSSIDES:

I will.

ROGERS:

Now there's the machine, and then there's the separate room...

ROSSIDES:

Yes.

AR 001226

ROGERS:

... where the image is viewed by a -- an operator, which has to be fairly close to the machine, but not terribly close. Right?

ROSSIDES:

(inaudible)

ROGERS:

Nevertheless, it requires some space that is not now required with magnetometers or (inaudible) procedure, right?

ROSSIDES:

Right.

ROGERS:

Now does -- does your budget request cover the costs of installing machines and acquiring space for the room, and all of that?

ROSSIDES:

It -- what the budget request includes -- money for constructing a viewing room, you know, within the checkpoint area. What we're doing, for example, is in a lot of places we're taking a supervisor's office and we're using other, you know, pieces of the real estate there close by to the checkpoint to create that alternate viewing room.

But the budget does have some money in it to request -- to cover some of those infrastructure costs to build out the viewing room.

ROGERS:

So what about the airports? Will they -- what will be their financial involvement with this change (ph)?

AR 001227

ROSSIDES:

The airport's...

ROGERS:

Yes.

ROSSIDES:

... financial involvement?

ROGERS:

Yes.

ROSSIDES:

Some of them are providing us the room. And, you know, in some cases we're providing them nominal amounts of money to pay for this infrastructure cost. But I think for the most part -- it's the investment (inaudible) TSA that we're making in the checkpoint area.

ROGERS:

So -- but will -- will you pay the airports for taking more of their space?

ROSSIDES:

I don't believe we are. I'll get back to you on that, though. It's -- I have not seen that cost factor as we're looking at these deployments. But I will get back to you and double check.

ROGERS:

Thank you (inaudible).

PRICE:

Thank you.

Mr. Rodriguez?

RODRIGUEZ:

Thank you very much.

And Madam Secretary, for your service to our country. And thank you very much for the great work you've been doing.

We just had a -- a recent incident that occurred in -- in Texas -- in Austin, the IRS facility there.

ROSSIDES:

Yes.

RODRIGUEZ:

And he could have taken a lot more lives. It did take, you know, the life of a wonderful, you know, individual -- veteran who served our country well.

In -- in 2008, TSA had proposed a plan to propose new rules for some other -- some 15,000 planes, including requirements for jet operators to check passengers and their watch lists, and those kind of things. And this proposal was met with a great deal of opposition in the private pilot industry groups and others.

When -- when will the TSA's new proposal for regulating private aircraft be made available? And, number two, what changes if any will be taken in consideration as a result of the incident that occurred in Austin at the IRS facility?

ROSSIDES:

Yes, Mr. Congressman. In answer to your question first. We have our -- we are going to go out with a supplemental, or a second notice of (inaudible) on the general aviation large aircraft security program. And we're hoping to have that through the administration and posted by the end of the year. And we did receive a lot of comments on the first round. And we had a terrific collaboration with the industry, and with G.A. pilots on comments. And we're really looking at that.

In the aftermath of the Austin, Texas, crash, in that incident we actually went back to the Homeland Security Institute that had done the engineering studies for us. And asked them to take

a look at the specifics of that crash, and if it should formulate any change in that proposed rulemaking. And so we're waiting for the results of that study. And that will -- that may help us. And -- and it definitely will inform us as to any changes to be made -- need to make in the rule.

RODRIGUEZ:

What kind of security do we have if any in some of the small airports that we have, you know, in terms of any kind of assessments that we might make at the present time?

ROSSIDES:

Right now in most very small G.A. airports we really don't really have any.

RODRIGUEZ:

We don't have -- we don't have any at all?

ROSSIDES:

No, sir.

RODRIGUEZ:

OK. Do we have some kind of assessment of the number of fly -- I guess we do have the number of flights that go out of there. But we don't -- we don't have any way of checking to see who flies out of there, who doesn't, and those kind of things?

ROSSIDES:

Right now -- well, mostly the FAA knows who's flying. They would know who -- you know, they would know the registration of that -- of the small plane. And they would know generally who the pilots are. The pilots have to be certified by the FAA. So most of the regulation to date has been via the FAA's programs.

RODRIGUEZ:

And so we've -- not even once a year or twice a year do we go and check to see -- or any kind of spot check on any of those...

ROSSIDES:

We have done on occasion for national security events, for example, with the inauguration last year of President Obama, we actually went and visited every general aviation airport on the route from the train that he took from Philadelphia to D.C. When there are -- during the Olympics, the planning for the Olympics that just ended.

RODRIGUEZ:

OK.

ROSSIDES:

We did work looking at the general aviation airports. And we did that with, you know, state and local law enforcement in concert with our inspectors.

So depending upon national events, significant activities in an area, we will go and look at the general aviation airports. And if intel suggests something, we definitely then work in looking at them.

RODRIGUEZ:

If -- if I can just follow up on that one again. When you refer to intel do you -- are you in direct contact, for example, on the border with Border Patrol and others?

ROSSIDES:

Yes. Yes. We have a very close working relationship with (inaudible)...

(CROSSTALK)

RODRIGUEZ:

In terms of the number of flights coming...

ROSSIDES:

Yes.

RODRIGUEZ:

... over -- and Canadian border also?

ROSSIDES:

Yes.

RODRIGUEZ:

OK. Thank you very much. Thank you.

PRICE:

Thank you.

Ms. Lowey?

LOWEY:

Thank you.

In the American Recovery and Reinvestment Act, the committee provided TSA with $25 million for airport screening machines that have been discussed rather thoroughly to be deployed at airports across the country.

However, last Tuesday it was reported that not one of these devices has yet to be deployed. I was really shocked to read that, because we know the importance of quickly deploying this technology to our most traveled airports, including Kennedy, LaGuardia in New York.

Why did it take seven months just to purchase 150 advanced imaging technology machines? You mention a time frame for deploying this technology in Boston and Chicago. What about New York?

And if you struggled to spend the $25 million, what assurances can you give this committee that you can quickly and effectively spend the more than $214 million being proposed by the president to deploy nearly 1,000 machines across the country?

ROSSIDES:

AR 001232

Thank you. Yes, Congresswoman, we bought 150 of the machines last September. And we are in the process now of receiving those. And they will be disbursed (inaudible) to go out to the airport. The reason that it took some time is we put in the order in September, and the manufacturer has been delivering those. We have made sure that they are ready and equipped the way we need them to be for deployment to the airports.

We also have -- we're in the process of awarding a contract for -- what's called an "integration contract." And that will be a contractor that will be -- their -- their expertise is in deploying this kind of technology, and rolling this out, and supporting us to do that.

So we have two qualified vendors with this technology today. And as we make these purchases, we will be able to use that vendor's list. And in the meantime our lab is continuing to certify additional vendors. And that's why -- the industry is responding very quickly to this demand. And with our integration contract we believe we will be able to deploy these.

And we are -- it's -- it's going to take all of our energy and our commitment, but we are, you know, very, very committed to doing this.

LOWEY:

Now could you answer -- you mentioned Boston and Chicago. How about New York?

ROSSIDES:

I don't have the schedule in front of me, but I will be happy to provide it. Secretary Napolitano tomorrow will be announcing the deployment to 11 airports. And our team is working now on the deployment of all 150 machines, plus those that we will be receiving this year and -- and, hopefully, next.

LOWEY:

I hope it'll be -- the decisions are made according to threat.

ROSSIDES:

They are.

LOWEY:

Just wanted to check that out.

Another issue. Secretary Napolitano testified last week before the Authorizing Committee that DHS did in fact have the authority to grant TSOs collective bargaining rights administratively. Could you tell me what is holding up the department from taking this action when President Obama stated many times over during the campaign that he supported it?

I mean, it seems to me the threat to the traveling public is the terrorists, not the labor unions. And the fact that we can't even get someone to head up the agency because of this issue doesn't make any sense. Could you respond?

ROSSIDES:

Yes, Madam Congresswoman. The secretary has indicated that she wants to get a permanent TSA administrator in place before the final decision is made on collective bargaining.

LOWEY:

That's a good excuse, but what does she -- well, OK.

ROSSIDES:

But I will tell you what I have done in my tenure as the acting assistant secretary. I have held meetings with both NTU (ph) and AFGE in the last year, where the leadership of the unions have brought in officers from around the country that they have -- that are members of their respective unions. And we have sat down and had just great dialogue with those front line officers and the leadership of both unions on issues of mutual concern.

And I will tell you that you put me in a room with a bunch of TSOs, and it is a great, great exchange. And we've had -- I consider the leadership of TSA today to have a very good working relationship with both unions. And we will await the secretary's ultimate...

(CROSSTALK)

LOWEY:

I thank you for that response. But I see the chairman's about to crack the whip. And I just want to remind you that Customs and Border Protection, Immigration, Customs Enforcement, Capitol Police and the Pentagon Force Protection Agency grants collected for -- has -- have collective bargaining rights.

ROSSIDES:

Yes, ma'am (inaudible).

LOWEY:

You're away of that?

ROSSIDES:

Yes. Yes, ma'am.

LOWEY:

Thank you, Mr. Chairman.

PRICE:

Thank you.

Mr. Farr?

FARR:

Thank you, Mr. Chairman.

I probably fly more than anyone on this committee because of the distance from here, and I go home every weekend. So I have a lot of experience with TSA.

And, frankly, I've been very critical of air marshals; of wondering what the cost effectiveness of them are. It would be like us having to have a marshal to take us from this room to the floor.

After you've gotten into the building, the building secure, and after you get through airports should be secure. We've certainly got locked down cabins and cabins that are armed, and all kinds of things. And I don't think in the Christmas bomber it would have made a difference whether an air marshal was on that plane -- because air marshals sit in first class, and that incident happened in the -- in the back.

So we -- the committee last year asked for a report on essentially the cost effectiveness of the air marshal program. We have not received anything yet. In your request you want $85 million more dollars for air marshals. I don't think our committee ought to give it to you until we get that report back. I just wondered if you want to comment on what -- what we're getting out of that program?

I mean, there's a lot of -- you know, this is a priority of issues. And while I'm a big fan of law enforcement, I don't think this is the best I've -- actually, from what I understand talking to the air marshals, they have nothing to do when they're not flying. They're not reviewing rosters. They're not helping with the -- the no-fly list and things like that.

They have no access to the information of who's on the plane. They're always shocked to find out that I'm a Congress member. Only find that out till they sit next to me, and they can read my -- my material. And asking me afterwards when they go off, "Why didn't anybody tell me?"

I swear there were five other members of Congress on this plane, and he didn't -- probably didn't know who they were either.

I mean, it -- it is -- I guess that's what's led to this issue of wondering why we ought to keep beefing up this program.

ROSSIDES:

So Congressman, I would be happy to come myself and bring the leadership of the Federal Air Marshal Service to give you a briefing, including some of the issues that you questioned there that I don't want to talk about in an open setting.

I will tell you that the Air Marshal Service is an extremely well-trained law enforcement professionals. When they...

(CROSSTALK)

FARR:

I don't doubt that.

ROSSIDES:

And when they are not in mission status, they are doing other things, including training. They are supporting our operations in airports. And they have -- they work closely with the FBI. They're assigned to the JTTF in the interest of aviation security. So we do have a number of deployments when they are not in the air.

But they are...

FARR:

AR 001236

Well, why don't you submit the report that we asked for, and then we can have a meeting after that?

ROSSIDES:

We will do that. And I will follow up on where that report is.

FARR:

The other -- wondered how the TSA is addressing the language barriers in international field personnel in the Middle East and Africa? For -- this is -- what are you doing to train people in the native languages or hire those country nationals to work for you in -- on the -- in the -- with field personnel in sort of the risky -- risky areas of the world?

ROSSIDES:

So one of the things that we do look for as we deploy our TSA representatives around the globe is whether or not they have -- they are fluent in the language to which they are being deployed. And if they are not, then they are (inaudible) to the Department of State Language School; that they are at least have -- have some basic capability in the language.

FARR:

And who pays for the screening equipment in foreign countries?

ROSSIDES:

In the foreign countries, those -- the foreign countries pay for that equipment.

FARR:

The host country pays for it?

ROSSIDES:

(inaudible)

FARR:

What lessons did TSA learn from its involvement and cooperation with so many agencies and other countries during the Vancouver Olympics?

ROSSIDES:

During the Vancouver Olympics -- we're in the process of doing a lessons learned now. And the -- we had great cooperation both at the -- from the general aviation and the commercial airports back and forth to Vancouver. We had a great inter-governmental agency cooperative effort. And the lessons learned are being -- are being reviewed now just immediately in the aftermath of the Olympics.

FARR:

Can you report those to the committee?

ROSSIDES:

Happy to. Yes.

FARR:

And lastly, what do you do...

(CROSSTALK)

FARR:

... I'm sorry -- with private -- private aviation.

PRICE:

Very, very quickly. We -- we -- we have a vote coming up, so...

ROSSIDES:

As I -- as I mentioned to Congressman Rodriguez, we are in the process of preparing the Supplemental Notice of Proposed Rule Making for General Aviation, which will go out later this year.

(CROSSTALK)

FARR:

Thank you.

PRICE:

Thank you.

Mr. Culberson?

CULBERSON:

Thank you, Mr. Chairman. It -- it's -- we really appreciate your service. Thank you for the job you've been doing. We -- there is a lot of concern that the Christmas Day bomber was on a terror watch list, and was able to get on an airplane. How and why did that happen? And what can we do in the future to make sure if they're on the watch list, they don't get on the airplane?

ROSSIDES:

Sir, he was not on any terrorist watch list. He was neither a no-fly, nor a selectee. And so we did not have any visibility into him.

CULBERSON:

He had -- and of course had apparently a valid visa. But it was my understanding he was on a terror watch list. That's not correct?

ROSSIDES:

No, sir, he's not.

CULBERSON:

He was on a British terror watch list, my colleague, Mr. Kirk, tells me. Are we looking at watch lists from other countries?

ROSSIDES:

We -- right now, sir -- I probably shouldn't answer that in an open session. So -- but I will tell you that right now President Obama did direct that -- that the U.S. government, both the Department of Homeland Security and the intelligence community, look at the watch-listing process. And we're in the -- in -- that -- that review right now is ongoing to see how we can improve that.

CULBERSON:

That does some like, you know, and I'm glad you're doing it, but common sense, if they're on a watch list, you just -- just automatic pilot you shouldn't let them on an airplane with -- with -- with my wife and kids, anybody's wife and kids...

(CROSSTALK)

ROSSIDES:

And -- and one of the things that TSA will have implemented by the end of this year is the Secure Flight program, which will ensure that no-flies and selectees are properly screened, and no-flies are not permitted to fly.

CULBERSON:

One other thing that just I know frustrates all Americans -- I certainly hear a lot about it; I know my colleagues do from their constituents -- is again just common sense. That it is very frustrating to see the TSA apply these restrictions to all of us. And -- and frisking, and -- and searching, you know, 70-, 80-year-old women.

I remember a horrible case of a -- of a Medal of Honor winner, an 80-year-old gentleman who'd served his country, and the guy was pulled aside and harassed and searched. Yet young Muslim men who -- particularly like, you know, this guy had been traveling to Pakistan -- are not treated any differently. And what statute -- what federal regulation prevents you from signaling out young Muslim men and giving them a little more attention than an 80-year-old Medal of Honor winner?

ROSSIDES:

Well, sir, when I -- when I hear of circumstances like that as you've described, it -- it troubles us too. We want to make sure that our officers are respectful of all passengers. But in reality, the

law requires us to screen all passengers. And TSA does not profile, and -- and therefore we do not, you know...

(CROSSTALK)

CULBERSON:

Right.

ROSSIDES:

... single out different categories of individual...

(CROSSTALK)

CULBERSON:

Right.

ROSSIDES:

... passengers for...

(CROSSTALK)

CULBERSON:

That's what I was asking. Is it statute? Is there a federal statute that prohibits you from singling out a group of people or particular characteristics, or is there internal regulation? Is it a federal regulation or a federal statute that prohibits you from profiling?

ROSSIDES:

You know, I'd have to get back to you, but I know as a matter of policy we do not profile.

CULBERSON:

It is disturbing. I mean, it's something that needs to change. It just defies common sense. I remember -- I got here 2001, and the -- was on the Transportation Authorizing Committee before I joined this -- this wonderful committee. And right after 9/11 we brought in the head of -- I think

you were on there with me, Mark -- we brought in the head of the Israeli -- remember that? (inaudible) security? It was terrific.

(UNKNOWN)

(OFF-MIKE)

CULBERSON:

Yes. And we heard terrific input from the head of Israeli security. They just don't have this problem. I mean, if you're an -- you know, an 80-year-old grandmother, they don't bother you. And -- and they obviously are going to screen you and check you. But they've got a -- as I recall, Mark, a security professional that'll actually talk to them. And if you're a...

(UNKNOWN)

(OFF-MIKE)

CULBERSON:

Yes. You fit certain characteristics you're going to have a conversation with Officer Lewis here. You're going to have a little special visit.

It just defies common sense. What do we need to do to make that happen? Because this is -- we do not have a problem with Baptists or Hindus, or, you know, Buddhists blowing up airplanes. This is just common sense. Why are we -- what needs to happen so you can let your officers use their own common sense and good judgment and zero in on the population that's the problem?

ROSSIDES:

So let me -- let me answer that in a couple of ways. First of all we have consulted with the Israelis frequently on the security measures that they have there and what we can do here. We have also -- we have a behavior detection officer program that has officers looking for behaviors that would warrant us to give somebody additional screening.

The -- in terms of what legislative remedy would we possibly need for this, I'd have to get back to you.

CULBERSON:

Please do. Real specifically. Where is the problem? And let me if I could -- let Mr. Kirk, because he is very knowledgeable on this as a naval intelligence officer, Mr. Chairman.

Thank you.

PRICE:

Fine.

Mr. Kirk, we will try to get your question in before we have to go vote?

KIRK:

(OFF-MIKE)

I just got to ask since -- since the second busiest airport in the world is in my state. We just had the head of security at O'Hare, Jim Maurer, say that it was the least secure airport in America. This is in the front page of the Chicago Sun Times today.

Can you comment on his charges? And he's got some pretty specific complaints against O'Hare.

ROSSIDES:

Yes, Congressman. I'm -- I'm familiar with the statements he made. But I will tell you that O'Hare has an airport security plan. TSA inspects to that plan. They are in compliance with that plan. And any time that we have something reported to us or we notice through our inspections that they are not in compliance with we would take it up with any airport authority.

KIRK:

And just one specific thing that he had here that I want to raise with you is, he says, quote, "O'Hare is the only airport in the country that allows private vehicles to park on the secure side of the airfield."

ROSSIDES:

I saw that. And -- and I'm aware of the parking setup there. But we -- basically right now they have a security plan that they are in compliance with.

KIRK:

Right. Do you have regular liaison with your European counterparts?

ROSSIDES:

Yes, sir. We do.

KIRK:

So one of the things that I would hope that we would do -- and maybe with the initiative of this committee -- is if you're on a British no-fly list, at a minimum you should be on the selectee list for the United States.

ROSSIDES:

And I believe that that is part of what we are looking -- looking at in terms of how do we share information across governments, and how do we make sure that information gets to the United States so that we can properly act on it.

KIRK:

Now, this may take some money, some foreign liaison, some work. But I think especially the no-fly list of the NATO allies should immediately trigger membership on the selectee list for the United States.

ROSSIDES:

Thank you. And I -- I will take it back...

(CROSSTALK)

KIRK:

And I think we ought to...

ROSSIDES:

... and I will make...

(CROSSTALK)

KIRK:

We ought to pick that up. Because it would be expensive in liaison, but I think the public would...

(CROSSTALK)

ROSSIDES:

Thank you.

PRICE:

The recommendation the gentleman is making doesn't depend on this. But I'm -- I'm told that as a matter of fact Abdulmutallab was not on the British no-fly list. He...

(CROSSTALK)

KIRK:

He was actually even worse.

(CROSSTALK)

KIRK:

He was -- he was denied a visa.

PRICE:

He was denied a visa because of a -- of a -- of a related problem. He was...

KIRK:

That -- that even means that the foreign office even had its act together.

PRICE:

He -- he was -- he was on our TIDE list. But that didn't translate into no-fly list.

(CROSSTALK)

KIRK:

I think that...

PRICE:

For the record, we'll straight out -- we'll -- we'll straighten that out.

(CROSSTALK)

PRICE:

... recommendations independent of that.

KIRK:

Basic point is you ought to have the resources to -- when they update their list, they immediately go on the selectee list for us.

ROSSIDES:

And Congressman, if I'd just say...

KIRK:

Yes?

ROSSIDES:

... TSA actually does not nominate and maintain that list. And so -- but it is something that I will take back to the...

(CROSSTALK)

KIRK:

Thank you.

ROSSIDES:

... issue exactly.

PRICE:

I apologize for having to take a break. We'll make it as brief as possible. We'll -- we'll come back for one final round after two votes.

ROSSIDES:

OK. Thank you.

(RECESS)

PRICE:

The committee will come to order once again. We've -- we've had a little more delay than we anticipated, but we'll -- we'll have one more round.

And we appreciate your patience, Ms. Rossides.

I would have some questions for the record, following up on my first line of questioning having to do with how these AIT machines are going to be deployed, particularly with the manpower and womanpower aspect of that request.

I won't get into detail on that now, but we do have this request for -- for five screeners for each machine, and we'll want to explore with you just how hard and fast that -- that estimate is and what the possibilities might be for a less manpower-intensive operation.

Also want to ask you some questions about the plans for portable explosive trace machines. But I think in this -- in this exchange here, in this hearing I want to ask you about the goal that we all share and that we trust will be -- will be achieved, although there are some significant challenges. That is, the goal of 100 percent screening of cargo transported on -- on passenger aircraft.

The 9/11 Act requires that you establish a screen -- a system to screen 50 percent of cargo by -- by February of '09, and 100 percent by August of 2010. You met the 50 percent deadline last February, yet it's going to be significantly more difficult to achieve 100 percent screening as -- and as we understand it, the -- the difficulties lie in -- mainly in two areas. That is international cargo and -- and also cargo in these large pallets.

So let just ask you about the nature of those challenges and what -- what you're doing to overcome them.

I think you have estimated -- last year you estimated, Ms. Rossides, that TSA may reach 75 percent for international cargo by August of this year. So we -- we all want to meet this 100 percent screening requirement, but you've been working on the problem for over a year now (inaudible) years before that.

So I wonder if you would still stand by that estimate, and if -- if not, why not. What is the screening estimate for international air cargo now? Any possibility we can do better than that 75 percent? If not, when are we going to achieve this?

Now, the other problem is the pallets. There are no machines qualified to screen air cargo delivered as pallets in -- or in oversized containers. TSA and S&T have been working on this problem for multiple years. But it appears we do not have a -- a solution, at least in the near term, for this dilemma, well after the mandate has expired.

So the lack of technology means that screening air cargo will be more person-dependent and more canine-dependent in the -- in the near term. So here, too, can you help us understand the technical challenge we're facing and the likely timeline for achieving our goals.

ROSSIDES:

Yes, Mr. Chairman. So with respect to air cargo domestically, let's talk about that first, which is part of the requirement, by August. We are confident that we will meet the domestic requirement to screen 100 percent, which means that all passenger airplanes leaving the United States, lifting off from domestic airports, that that cargo on those passenger flights will be screened.

The challenge, and the really significant challenge, is the international inbound. There are 98 countries that you need to have gained compliance (inaudible) that requirement. And right now we are working with those country -- for example the U.K. -- that their procedures, their screening methods meet the standards that we've set. But we're looking at those countries that are going to be -- that we have literally got to look at air methods -- how are they screening, are they using a similar supply chain approach, and are we comfortable with those methods.

I do not believe that we will get to that 100 percent by August. The 75 percent that we -- that I testified to last year might even be optimistic. What the staff is telling me, it may be more like 65 percent by August.

We are aggressively looking at every country, and working with IKO (ph), and looking at our global strategies office. Our people that do work around the globe are working with these host governments and the air carriers to begin to address this.

But it is going to be quite a challenge. We have about 20 countries that account for about 84 percent of the volume coming in. And -- so those are obviously where we're focusing our attention the most so that we can get the biggest bang for our buck, so to speak, with those countries.

We've been asked before what's our timeline, you know, how much longer would it take. And our estimate is, you know, it could be a couple more years before -- beyond August 2010 that we would have 100 percent compliance with some of those foreign countries.

PRICE:

Before you turn to the pallet question, what's the nature of the -- of the issue with -- with the most difficult cases? Is it -- is simply the -- or mainly the technological capability that these countries possess, the resources with which to do this?

Are there more -- are their more intractable problems of -- of a diplomatic nature? What -- and -- and it does -- does lead one to wonder if -- if -- if the latter is the case, what -- what's going to be taken to overcome this?

ROSSIDES:

So most of the challenges are either their basic capability to do it. We have actually gotten great cooperation every place where we have visited and talking to the host governments and the foreign carriers. So it's more that they just simply lack the resources to make the investment in the technology or to build capability. The -- there -- there -- we are going to have to look at alternative measures if it comes down to that in terms of how do we enable these foreign governments to meet this challenge.

But right now what we're working with, in working with IKO (ph) -- which has supported our supply chain approach -- we're hoping that they, too, can assist some of these locations.

The issue with the pallets is that these -- these very large pallets, there just basically is not a good technology to screen in this huge configuration that some of these pallets are.

So we're looking at what kind of technology, in our labs, can look at that, and how do we first try to break down the commodity into smaller packages that we can use to address the compliance requirement. Go -- so we go and look at smaller packages versus the huge, large, palletized-size configuration for these shipments.

PRICE:

Let me quickly, and finally, refer to an item that will not surprise you, given the content of past hearings, especially last year's hearing. In fact, had two hearings last year with TSA and FEMA on what solutions could be implemented to improve the timeliness of transit grant drawdowns for fiscal years 2006 through 2008.

At that time, 93 percent of the 2006 transit grants remained -- remained unspent, and 99 percent unspent from '07.

For the '06 grants, it took about 285 days after DHS announced the awards for the actual projects to be approved; slightly less so in '07, 207 days. Last spring, TSA and FEMA announced that all tier 1 projects would be approved at the time the awards were announced. This was to be a significant change, allowing the transit entities to access these funds faster.

Yet one year later, despite this non-incremental change, it appeared, in the process for approving these -- this funding, it appears the disbursement of these funds has really -- has really not improved dramatically. Certainly for grants awarded in '06, there have been improvements. The 67 percent of the '06 grants remaining unspent, compared to 93 percent a year ago.

But there have been marginal improvements, at best, for '07, with only 90 -- with 93 percent of the grants unspent compared to 99 percent a year earlier. So -- so why have these changes, which certainly on paper appear to be major changes to expedite the disbursement of these grants, not -- not produce the results we all anticipated?

We had intense interest in this, as you know. We had a second hearing. We asked you to report on the progress by August of '09.

So we know you worked hard trying to solve this problem. We saw some improvement. But we still haven't seen the report. It's over six months late.

So, you know, the main -- the main concern here is the underlying problem. But at the same time, it's hard for us to get a handle on the -- on the problem when we -- when we don't have the kind of information we deemed necessary.

ROSSIDES:

AR 001250

Yes, Mr. Chairman. And first, let me apologize that the report is not to the committee yet. And we are working to get that through and to you.

What we have done, though, is look at the recipients of these grant funds. Because what we know is, regardless of the process between TSA and FEMA, we wanted to focus locally on the recipients of these funds and how were they spending those.

So TSA has actually met with the recipients of 80 percent of these funds. And what we are seeing is that, at the local level, these funds are being managed well. The challenge is, they do not necessarily invoice. And so the drawdown rates do not actually reflect the progress that is being made with each of the individual projects. So we're attempting to work with them so that they do actually invoice us in a way that would show higher -- higher percentage of the drawdown rates.

What most of these local recipients and agencies do is, they wait for the project to be completely over and then they submit their invoices for payment. And so it looks like projects are not moving along in due course when, in fact, our visits with them and our work with them locally is showing that they are actually making some progress.

But we will get you that report, and I again apologize it's not to the committee.

PRICE:

Well, that's -- that's the sort of -- I mean, what you've said really -- really underscores, I think, the need for an accounting of this. We have no way of assessing what you -- what you just said in terms of the -- or maybe this being an artifact of an accounting method. I suppose I, on the face of it, would wonder how much of the -- how much of the problem that -- that really explains.

But to the extent some other way of accounting for this would help -- help us understand what the -- what the real rate looks like we, of course, would -- would -- would like to see that. But we do need an accounting, and we -- we're -- we're still very concerned about the underlying problem. These are funds that are not getting out to our communities for vitally needed productions (ph), and so we will look for that report in very short order.

Mr. Rogers?

ROGERS:

Let me get back to the whole-body imaging machines with you. What -- tell me -- I read your statement (inaudible) schedule on it. Summarize that for us.

ROSSIDES:

So you asked before about -- about the -- our ability to deploy the technology and -- and install them in the checkpoints. And TSA has the designs for all the checkpoints across our U.S. airports. And what we're looking at right now is, we know what the two current manufacturers' technology requirements in terms of the size of these units, is. And we're looking at the airport configurations that we know, and where we can deploy this technology so that it has minimal impact on the configurations of these checkpoints.

And that process is ongoing between the TSA technology staff and the airports.

And we're very confident that these first 500 we can deploy very effectively and in a fairly accelerated manner when you (inaudible) time frame because we know what those checkpoints look like today. We've had airports volunteer because they know, as well, that they can take this checkpoint -- they can take the technology as the checkpoint is configured.

The -- as we look ahead and as we continue to press the industry, we are not going to just stop with this technology and the advancement and the capabilities that this technology promises. We want to see the industry get us to a kind of technology that has both the walk- through metal detector capability as well as the imaging technology capability.

But we're very confident right now, based on our planning, based on what we know about these checkpoints, and based upon the cooperation from the airport industry across the system that we can deploy these in a very, very effective fashion.

ROGERS:

Well, on the schedule you say in your statement, on page five, that 40 machines have been deployed at 19 airports already.

ROSSIDES:

That's correct.

ROGERS:

Last September you bought 150 additional units, and this year you expect to deploy those and at least 300 additional units across the country -- which would be 450 additional units.

ROSSIDES:

(inaudible)

ROGERS:

And that the first unit's set to arrive at Boston Logan and Chicago O'Hare next week.

ROSSIDES:

Right.

ROGERS:

And then, as you point out, the budget request $214 million-plus to buy and install an additional 500 units at checkpoints to bring the total number of units to about 1,000. So -- and so you're asking, then, on top of the money to acquire the machines, you're asking an additional $314 million-plus for 5,355 new positions to run these machines at their accelerated pace.

And assumedly, if these machines are working out well, assumedly you will increase the number even further, correct?

ROSSIDES:

The -- that is part of this ongoing assessment we're doing right now, is what would be the optimum, full operational capability across all airports in the country, beyond the 1,000. But we have not come to a final number on that.

ROGERS:

So your initial -- initial guesstimate -- guesstimate on the manpower to operate the 1,000 machines is 5,355 people -- five FTEs per machine, plus. Is there any hope that we can get that down?

ROSSIDES:

The -- this -- what we're looking at is that requirement for this initial 1,000 machines. I believe that as we continue to deploy additional machines across the whole system you'll have different requirements for the (inaudible) airports versus the smaller. And it's our commitment, as we're going forward to look at how do we get the maximum efficiencies and effectiveness out of both the resources of our people and the technology.

That 5,000 FTE per machine basically really represents a little over 1.25 to 1.5 FTE, but you're adding in three shifts, 24/7 operations. And that's where we get the five per machine.

ROGERS:

But some airports won't be open...

(CROSSTALK)

ROSSIDES:

That's right. And so it's an average across the whole system that that represents. So as we continue to move into more and more airports we will be looking at what that right combination and what that FTE would be, you know, once we're -- once we're at a full capability.

ROGERS:

Well, you're asking for a 12 percent increase in the -- in the money for the FTEs in one year. Now, as you recollect when we first started this organization, before this department ever existed or (inaudible), TSA, we capped the number of employee FTEs at 45,000. What is it now?

ROSSIDES:

Today, in the checked baggage and passenger screening checkpoint, we have about 38,000 FTEs working in those areas.

ROGERS:

Well, but for -- for total screeners.

ROSSIDES:

Total? It's about 44,000 -- yes, just under 45,000.

ROGERS:

Which you would bump up with these new ones to plus- 50,000, then?

AR 001254

I -- I -- I notice that there is some comment that there's a -- a -- some auto detect function which might be possible on these body scanner machines. What do -- what you make of this?

ROSSIDES:

The auto detections capability is where the machine actually identifies on the image the anomaly so that the operator doesn't have to study the image. The machine basically tells the operator that there's an anomaly here that requires further examination.

ROGERS:

Well, would that -- does that exist now?

ROSSIDES:

No. It -- it's in our labs being evaluated right now, that kind of technology.

ROGERS:

If that works out, would that help us reduce the FTEs per machine?

ROSSIDES:

No, sir. It really does not because the configuration for the staffing right now is to -- that staffing is to actually be in the checkpoint assisting with the (inaudible) process and the anomaly resolution process. So it would not necessarily save on the -- with the auto detection capability..

ROGERS:

Now, you have the magnetometer at the checkpoint, plus the whole-body imaging. Would the FTEs for the body imager, the five FTEs, would that also cover the magnetometer work?

ROSSIDES:

Well, the -- we look at it in terms of the whole checkpoint being a cell that requires staffing. And so the additional resources that we are asking for would accommodate the checkpoint with the advanced imaging technology as well as if we had the walk-through metal detector. So it -- we don't really save FTE if we get rid of the walk-through metal detectors. It's still the number of people required in that checkpoint, you know, unit.

AR 001255

ROGERS:

So the metal -- with or without the full-body imaging machine -- well, without the full-body imaging machine what is the manpower (ph) requirement for a checkpoint?

ROSSIDES:

I believe that the checkpoint configuration with the AIT in this design is 9.5 FTE (ph). And it's -- then you -- you normalize it across the whole system. And so the request that -- that you're seeing is for the increase, which is 1.25 to 1.5 FTE per machine. And then you multiply that by the shifts and by the -- the 24/7 operations in the major airports.

ROGERS:

Well, your estimate of five FTEs per machine per day looks to me like it's going to be conservative.

ROSSIDES:

Well, sir, we have looked at what we can do with our existing resources and with this technology. And that is a good faith estimate on our part of what our modeling shows.

ROGERS:

Well, I hope, Mr. Chairman, at some point in time, we can talk about, on the subcommittee, withholding some money in the later part of the year until we see, the practical application that we actually need five FTEs per machine per day. Because it very well may work out as they deploy these machines they will find some efficiencies that were not (inaudible).

But if we go ahead and hire these people, then we're stuck. So I would hope that we could talk about staging the manpower as time goes (inaudible).

ROSSIDES:

And -- and we will be happy to keep the committee informed as we are deploying these in terms of what we're seeing operationally.

ROGERS:

Thank you.

PRICE:

All right.

Mr. Ruppersberger, you can -- you can wrap up with today's...

(CROSSTALK)

RUPPERSBERGER:

Excuse me. We had a lot of hearings at the same time, but this is very important and relevant.

One of the issues I want to discuss about -- and if I'm repeating myself, let me know -- is your personnel, the training of your personnel, and looking at how there are techniques used in other parts of the world that might -- might work. And Israel is a perfect example.

I think we're not talking about profiling, but I think Israel talks about behavior. And -- and that's what we'd really like to talk about. But first, let me ask you this: From a training point of view, what standards do you have for your average TSA person? Are they -- do they have to have law enforcement experience, any education experience? Any -- any experience at all? What -- what are your standards as far as -- as far as hiring?

ROSSIDES:

So the standards for the transportation security officer are spelled out in law, and those require a high school degree or its equivalency. There are requirements once they are hired for expensive training. They must have a minimum of 80 hours of training. And that training is -- runs the gamut, from how to operate the technology that's in the checkpoint, how to deal with passengers properly, how to resolve alarms, how to conduct physical body pat- downs. So it's a variety of training.

The officers are also required, annually, to be certified, meaning that they have to demonstrate their proficiency to conduct those duties, and if they're not they're subject to dismissal.

The -- we have another group of officers called behavior detection officers. And they are trained -- and get to what you're talking about in terms of the Israelis with looking for anomalous behaviors of passengers as they're coming through the checkpoint. And then, you know, based on the behaviors that they observe they may refer the passenger for secondary or additional screening.

RUPPERSBERGER:

Right. Well, this is what I want to get into. I think a lot of times we do repetition because we've always done it. And yet, are we really wasting our personnel's time when they could be focusing in other areas that might create a better way of detecting?

Give you an example. I'm going to use myself personally. I have two artificial shoulders. My back's fused, and I have five screws in each foot. So I set off everything when I go through.

And so I -- automatically, I stand in line and let the officials know. You don't complain. You get in the back of the line. And then -- then every time you go in, you do the whole -- you wait for somebody to come. And you have maybe one or two people that are there.

Now, you know, eventually the -- there's got to be some judgment on, whether it's me or somebody that on a regular basis that -- that -- that does this type thing. Because I wonder if -- if that -- the people that are working on me because of my body, my artificial body parts -- I'm bionic, by the way.

But -- but if -- if -- if they would be looking at (inaudible) trained more in behavioral, but also there's an issue of the manifest. You know, in port security we look at manifests. We can't -- you know, we look at the port of embarkation.

If we're going to have airlines involved in this process, we have to be more open and get them more information and more intelligence. And I think that, if you look from the Israel system, it works. I mean, they're probably more exposed than any other country in the world right now from a terrorist point of view.

And whether you would consider evaluating, first thing, the standards of the people you hire. Do we need more law enforcement? I'm not saying this is what you need (inaudible) evaluate. And then if you do hire, you're -- and I'm not complaining about the people that are being hired because I don't -- I haven't judged them, I don't know their performance records, but then they need to be trained.

And are we really doing the same thing over and over, wasting time with certain individuals, even though we know Al Qaida might try to find more Caucasians, or whatever. Is -- is -- is it -- we're putting ourselves in a better position by that reevaluation and doing what -- what really might work better?

ROSSIDES:

Sir, you've actually described -- we -- part of the reasons why we're moving in this direction we're moving with the advanced imaging technologies. One of the great advantages that the

advanced imaging technology is going to give us is that persons like yourselves who have metal implants, going through that technology will now go through the machine and avoid the total pat-down and the time that that takes. We've actually had tremendous positive response from veterans, from persons with disabilities, going through that technology in the pilot phase.

RUPPERSBERGER:

But, you know, I'm not talking about somebody like me or that person. I'm talking about the system, and whether the -- the personnel that is wait -- spend their time with someone like a veteran or people that have...

ROSSIDES:

Right.

(CROSSTALK)

RUPPERSBERGER:

... that they could be doing something that would be making the system more safer and not just doing something that looks -- makes us feel good, but really what are -- what are we...

(CROSSTALK)

ROSSIDES:

Right. And -- and, in fact, what we do do is, in addition to our behavior detection officers, we actually utilize our TSOs I other parts of the airport to look for and do random unpredictable screening -- screening procedures. And that is exactly some of the lessons we've learned from the Israeli model, is to have multiple layers of security.

We actually have worked closely with the Israelis on a number of our programs besides behavior detection, but also our covert testing programs. And we did actually consult with them -- with them after the Christmas Day attack to talk about what might that have done in their system versus how it was carried out, you know, across the globe through the Amsterdam process that the suspect went through.

So our -- our approach to multiple layers of security, and utilizing our officers in those multiple layers is exactly what we're trying to do similar to the Israeli, where it isn't just focusing on the passenger who is coming through that is (inaudible) perfectly compliant.

RUPPERSBERGER:

I really -- I represent the BWI airport (inaudible) -- the BWI airport, and I've seen, I think, a lot of advancement in your personnel, the quality of the personnel, the way they treat the public. But again, I think some of the systems seem to be so repetitive and redundant you're wondering whether (ph) they're going to work. And a lot of what -- what you're talking about, which I agree with, is the technology.

(OFF-MIKE)

(LAUGHTER)

ROSSIDES:

Thank you.

RUPPERSBERGER:

Thank you.

PRICE:

Ms. Rossides, let me -- let me again thank you for a very useful afternoon of testimony -- good exchanges that are helpful to us. And beyond that, for the outstanding quality of your service.

ROSSIDES:

Thank you so much, Mr. Chairman. And I -- I appreciate tremendously the engagement with this committee. We enjoy, and really are appreciative, of the support you give to TSA. Thank you.

(UNKNOWN)

Mr. Chairman, in that vein, we sort of started out together in this business.

ROSSIDES:

Yes, sir.

(LAUGHTER)

(UNKNOWN)

When TSA was created, and the department was created, (inaudible) Department of Transportation. So we've been laboring over these things for a good while now, and we're going to miss your expertise.

ROSSIDES:

Well, thank you.

(UNKNOWN)

You have been a very competent manager. You've demonstrated today again your knowledge of these subjects, and we're going to miss you and we want to say thank you again for your long service.

ROSSIDES:

Thank you.

(UNKNOWN)

Where are you going?

ROSSIDES:

Well, right now I'm waiting for the administration to appoint a permanent administrator, sir.

(UNKNOWN)

Are you holding your breath?

(LAUGHTER)

ROSSIDES:

Thank you.

PRICE:

I think we best adjourn this hearing. Thank you very much.

ROSSIDES:

Thank you very much.

CQ Transcriptions, March 4, 2010

List of Panel Members and Witnesses

PANEL MEMBERS:

REP. DAVID E. PRICE, D-N.C. CHAIRMAN

REP. JOSE E. SERRANO, D-N.Y.

REP. CIRO D. RODRIGUEZ, D-TEXAS

REP. C.A. DUTCH RUPPERSBERGER, D-MD.

REP. ALAN B. MOLLOHAN, D-W.VA.

REP. NITA M. LOWEY, D-N.Y.

REP. LUCILLE ROYBAL-ALLARD, D-CALIF.

REP. SAM FARR, D-CALIF.

REP. STEVEN R. ROTHMAN, D-N.J.

REP. DAVID R. OBEY, D-WIS. EX OFFICIO

REP. HAROLD ROGERS, R-KY. RANKING MEMBER

REP. JOHN CARTER, R-TEXAS

REP. JOHN CULBERSON, R-TEXAS

REP. MARK STEVEN KIRK, R-ILL.

REP. KEN CALVERT, R-CALIF.

REP. JERRY LEWIS, R-CALIF. EX OFFICIO

WITNESSES:

GALE ROSSIDES, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Source: CQ Transcriptions

All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of CQ Transcriptions. You may not alter or remove any trademark, copyright or other notice from copies of the content.

© 2010 Congressional Quarterly Inc. All Rights Reserved.

Homeland Security

Readout of Secretary Napolitano's Meeting with Airline Industry CEOs on Strengthening International Aviation Security

Release Date: March 4, 2010

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Department of Homeland Security (DHS) Secretary Napolitano today met with CEOs of the member airlines of the Air Transport Association of America (ATA), the largest airline trade association in the United States, and the International Air Transport Association (IATA), which represents approximately 230 airlines and more than 90 percent of the world's air traffic—part of her ongoing efforts to bring together major domestic and foreign air carriers to work on ways to bolster international aviation security.

"Government and the private sector must work collaboratively to develop and implement enhanced international security measures and standards," said Secretary Napolitano. "Working together with our partners in the aviation industry, we can and will strengthen the global aviation network to protect the traveling public from terrorism and other threats."

During the meeting, Secretary Napolitano and airline CEOs from across the United States and Europe discussed the international airline industry's important role in implementing stronger and more effective international aviation security measures to protect the traveling public.

Secretary Napolitano also highlighted the Department's continued efforts to bolster security measures at domestic airports–including the accelerated deployment of state-of-the-art equipment such as Advanced Imaging Technology and Explosives Trace Detection units to enhance passenger screening–and reiterated DHS' commitment to working with airlines on the deployment of security measures and technology at U.S. and international airports.

Since January, Secretary Napolitano has met frequently with top representatives from airlines and airports from across Europe, Asia, Africa, the Middle East and North America on ways to strengthen the international aviation security system.

Today's meeting builds on recent international summits attended by Secretary Napolitano that have resulted in joint declarations to strengthen the international civil aviation system between the United States and Argentina, Brazil, Canada, Chile, the Dominican Republic, Mexico and Panama on Feb. 17, and between the United State and the European Union on Jan. 21.

For more information, visit www.dhs.gov.

###

This page was last reviewed/modified on March 4, 2010.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders

- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security
- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

Homeland Security

Secretary Napolitano Announces Deployments of Recovery Act-Funded Advanced Imaging Technology

Release Date: March 5, 2010

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Department of Homeland Security (DHS) Secretary Janet Napolitano today announced the first 11 airports to receive advanced imaging technology (AIT) units purchased with American Recovery and Reinvestment Act (ARRA) funds—strengthening security at airports throughout the country while boosting local economies.

"By accelerating the deployment of this technology, we are enhancing our capability to detect and disrupt threats of terrorism across the nation," said Secretary Napolitano. "These 11 airports will be the first of many to receive this enhanced technology as a result of the Recovery Act."

Based on security and operational needs, the Transportation Security Administration (TSA) will deploy AIT units to the following airports:

- Boston Logan International (BOS)
- Charlotte Douglas International (CLT)
- Chicago O'Hare International (ORD)
- Cincinnati/Northern Kentucky International (CVG)
- Fort Lauderdale-Hollywood International (FFL)
- Kansas City International (MCI)
- Los Angeles International (LAX)
- Mineta San José International (SJC)
- Oakland International (OAK)
- Port Columbus International (CMH)
- San Diego International (SAN)

AIT units are being installed today at Boston Logan International airport, and within the coming week at Chicago O'Hare International airport, followed by full deployment of the ARRA-funded technology at the remainder of the 11 airports by Summer 2010. All airports receiving ARRA-funded AIT units, except Los Angeles International, are receiving this technology for the first time.

Additional airports will be announced in the near future. Many factors are taken into consideration before AIT units are deployed including airport readiness, checkpoint infrastructure, and capacity to ensure privacy protections—including a separate, remotely located room for viewing images.

Advanced imaging technology is designed to bolster security by safely screening passengers for metallic and non-metallic threats—including weapons, explosives and other objects concealed under layers of clothing. The ARRA-funded machines will include the latest security enhancements to detect new and evolving threats.

TSA ensures passenger privacy through the anonymity of AIT images—a privacy filter is applied to blur all images; images are permanently deleted immediately once viewed and are never stored, transmitted or printed; and the officer viewing the image is stationed in a remote location so as not to come into contact with passengers being screened.

Currently, 40 AIT units purchased previously are deployed at 19 airports nationwide. TSA expects to deploy a total of

450 AIT units by the end of 2010.

Last month, in recognition of the one-year anniversary of the Recovery Act, Secretary Napolitano highlighted the ARRA investments in technology and infrastructure at airports across the country.

ARRA, signed into law by President Obama on Feb. 17, 2009, committed more than $3 billion for homeland security projects through DHS and the General Services Administration (GSA). Of the $1 billion allocated to TSA for aviation security projects, $700 million is dedicated to screening checked baggage and $300 million is allocated for checkpoint explosives detection technologies.

To learn more about the DHS Recovery Act projects, visit www.dhs.gov/recovery.

###

This page was last reviewed/modified on March 5, 2010.

I Want To

- Learn about the Travelers' Redress Process
- Find Career Opportunities
- Use the Job Finder
- Check the Threat Level
- Cross U.S. Borders
- Contact the Department
- Learn about E-Verify

Popular Searches

- Case Status, ESTA, E-Verify, Forms, Green Card, Grants, I-9, Jobs, Passport, Visa

Featured Components

- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard
- U.S. Secret Service
- Office of Inspector General

Information For

- Travelers
- First Responders
- Business
- Veterans
- Students
- Government
- Citizens

Making Connections

- Leadership Journal
- The Blog @ Homeland Security

- Homeland Security Feeds
- Homeland Security Tweets
- Homeland Security Videos

Resources

- Press Room
- Open for Business
- Science & Technology

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

TRANSPORTATION SECURITY ADMINISTRATION

Statement of

GALE D. ROSSIDES

ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Before the

COMMITTEE ON HOMELAND SECURITY & GOVERNMENT AFFAIRS

UNITED STATES SENATE

March 10, 2010

Good morning Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee. Thank you for the opportunity to appear today to discuss the steps the Transportation Security Administration (TSA) has taken in response to the attempted terrorist attack on Northwest Flight 253. I appreciate the Committee's leadership in the aftermath of the attack, and your steadfast efforts to ensure the security of the American people.

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, this Administration is determined to thwart terrorist plots and disrupt, dismantle, and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just TSA, but components

across the Department of Homeland Security and many other federal agencies as well as state, local, tribal, territorial, private sector and international partners.

Today I want to describe the role that TSA currently performs in aviation security, how TSA responded in the immediate aftermath of the attempted Christmas Day attack, and how we are moving forward to further bolster aviation security.

TSA's Role in Multiple Layers of Defense

Since 9/11, the U.S. government has employed multiple layers of defense across several departments and agencies to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities, while other countries and the private sector – especially the air carriers themselves – also have important roles to play.

Passenger Identity Verification

As one critical layer of defense, DHS conducts pre-departure passenger identity verification in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. DHS uses the Terrorist Screening Database (TSDB), managed by the FBI's Terrorist Screening Center, to determine who may board, who requires further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

Specifically, to help make these determinations, DHS uses the No-Fly List and the Selectee List, two important subsets within the TSDB. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, over, or within the United States. Individuals on the

Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

Through TSA's Secure Flight Program, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List, and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, DHS began to transfer this responsibility to TSA in 2009, and the transition is targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination.

Screening Passengers and Baggage

Another layer of defense in which TSA plays a critical role is the screening of passengers and their baggage. TSA screens passengers and baggage at airports in the United States, but not in other countries. Physical screening at foreign airports is conducted by the foreign government, air carriers, or by the respective airport authority.

Domestically, TSA employs a layered approach to security, which includes measures both seen and unseen by travelers. The 48,000 Transportation Security Officers at hundreds of airports across the United States screen 1.8 million passengers and their baggage every day using advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines, vapor trace machines that detect liquid explosives, Advanced

Imaging Technology, full-body pat-downs, explosives detection systems, Bomb Appraisal Officers, and Behavior Detection Officers – both at the checkpoint and throughout the airport. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security throughout the airport perimeter and in limited access areas of airports. The $1 billion in Recovery Act funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

In-Flight Security

To support in-flight security, Federal Air Marshals (FAM) are deployed on high-risk domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more volunteer pilots serve as armed, deputized Federal Flight Deck Officers on domestic flights. Additionally, armed law enforcement officers from federal, state, local, and tribal law enforcement agencies that have a need to fly armed provide a force multiplier on many flights.

International Screening Standards

Because TSA does not conduct screening at international airports, TSA works closely with our foreign partners to ensure international screening standards are followed- particularly for flights bound to the U.S. TSA annually conducts approximately 300 airport assessments at foreign airports using International Civil Aviation Organization (ICAO) standards and inspections of foreign and U.S. air carriers that fly to the United States using TSA standards. If an airport does not meet these standards, TSA works with the host government to rectify the

deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. If non-compliance with international standards continues long-term, TSA may recommend suspension of flight service from these airports to the United States.

In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport that is a last point of departure to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level.

Response to the Christmas Day Attack

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. TSA directed the Federal Aviation Administration to apprise 128 U.S.-bound international flights from Europe of the attempted attack and to ask them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosive detection canine teams, state and local law enforcement, expanded presence of Behavior Detection Officers, and enhanced screening. TSA conducted calls with all major airlines and the Air Transport Association, and issued Security Directives and Emergency Amendments for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

In addition to TSA's outreach, DHS was in close contact with Congress, our international partners, and state and local officials across the country. DHS and the FBI issued a joint bulletin on the attempted attack to state and local law enforcement throughout the nation and distributed

it to all Homeland Security Advisors, regional fusion center directors and Major City Homeland Security Points of Contact in the country.

On January 3, DHS/TSA issued a new Security Directive, effective on January 4 and still operational today, which includes security measures developed in consultation with law enforcement officials and our domestic and international partners. This Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism[1] or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners

Steps Forward to Improve Aviation Security

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. At President Obama and Secretary Napolitano's direction, DHS and TSA are pursuing five key objectives to enhance the protection of air travel from acts of terrorism.

Watchlists

First, DHS is working with our interagency partners to re-evaluate and modify the criteria and process used to build the TSDB, including adjusting the process by which names are added

[1] The State Department currently lists Cuba, Iran, Sudan, and Syria as state sponsors of terrorism.

to the No-Fly and Selectee Lists. The Department's ability to prevent terrorists from boarding flights to the United States depends upon these lists and the criteria used to create them. As an entity that is primarily a consumer of this intelligence and the operator of programs that rely on these lists, DHS is working closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watchlist system.

DHS/ DOE Partnership

Second, DHS has established a new partnership with the Department of Energy (DOE) and its National Laboratories in order to use their expertise to bolster security. The Deputy Secretaries of Homeland Security and Energy are leading the effort to bring the paramount capabilities and critical resources of the DOE National Laboratories to bear on developing advance technical solutions to key aviation security challenges. This partnership will focus on advancing current technology, assessing system capabilities to determine gaps, and developing emerging technologies to fill those gaps in an efficient and effective manner.

Two years ago, DHS and DOE formed the National Explosive Engineering Sciences Security (NEXESS) Center, a consortium of National Laboratories including Sandia National Laboratory, Los Alamos National Laboratory, and Lawrence Livermore National Laboratory, to provide an agile and aggressive means to anticipate and understand explosive threats and to develop countermeasures to protect the homeland. The NEXESS Center provides informed scientific analysis for short- to mid-term priority assessments as well as mid- to long-term research and technology development. The Deputy Secretaries of both DHS and DOE are working collaboratively to strengthen these efforts in light of the December 25 attempted attack.

TSA is also working closely with the DHS Transportation Security Laboratory (TSL) in technology development. The TSL, operated by DHS Science & Technology, performs extensive qualification testing for all of TSA's explosives screening equipment.

Enhanced Screening Technology

Third, TSA is aggressively pursuing the deployment of enhanced screening technology to domestic airports and encouraging our international partners to do the same. While no technology is a silver bullet in stopping a terrorist attack, a number of technologies, when employed as part of a multi-layered security strategy, can increase our ability to detect dangerous materials.

To this end, TSA will accelerate deployment of Advanced Imaging Technology to increase capabilities to identify materials such as those used in the attempted December 25 attack. These efforts are already well underway. TSA currently has 40 machines deployed at nineteen airports throughout the United States and purchased 150 additional AIT units last September under the American Recovery and Reinvestment Act of 2009. This year, TSA expects to deploy at least 450 additional units across the country. The Administration's Fiscal Year 2011 budget calls for purchasing and installing an additional 500 AIT units, which would bring the total number of AIT units to approximately 1,000. The detection capabilities of AIT units are one part of a successful technology security initiative, but it is also critical that TSOs have the necessary training to resolve an anomaly identified by the AIT operator. TSA is working to improve both the detection capability of the units and the ability of screening personnel to resolve an anomaly, while being respectful of personal privacy, dignity, and civil rights and

liberties. The Administration's Fiscal Year 2011 budget also includes additional personnel to operate these AIT machines.

DHS is also increasing assets in the area of canine teams, explosives detection equipment, and highly trained security personnel to strengthen our abilities to find dangerous materials and stop dangerous people from boarding aircraft. Nearly 950 Advanced Technology X-ray machines have been deployed to U.S. airports to enhance the screening of carry-on bags. Additional machines will follow this year and include automated detection software to improve their capability. TSA has expanded the random use of Explosive Trace Detection (ETD) machines, which can be effective against a wide scope of explosives, to screen both passengers and bags. The Administration's Fiscal Year 2011 budget request calls for $60 million to purchase approximately 800 portable ETD machines. The FY 2011 budget also requests funding for a substantial increase of explosives detection canines by adding an additional 275 teams. Further, the budget seeks funding for an additional 350 Behavior Detection Officers.

Aviation Law Enforcement

Fourth, DHS will strengthen the presence and capacity of aviation law enforcement. Beginning this month, as an interim measure, we have deployed additional law enforcement officers from across DHS- including the Secret Service, Customs and Border Protection, Immigration and Customs Enforcement, and the U.S. Coast Guard- to assist Federal Air Marshals. In January, these highly trained officers participated in an accelerated specialized training program led by the FAMS on the unique methods employed to protect and defend an aircraft. This will allow for an immediate further increase in FAMS coverage of international

flights. The President's FY 2011 budget request also increases funding to sustain long-term FAMS coverage on domestic and international flights.

International Partnerships

Fifth, as mentioned earlier, DHS will continue to work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in foreign airports and the commitment of our foreign partners to enhance security.

Last month, DHS leadership embarked upon an aggressive international outreach initiative to enhance international aviation security standards and practices- particularly for international flights bound for the United States. In early January, Deputy Secretary Lute and other senior Department officials traveled to Africa, Asia, Europe, the Middle East, Australia, and South America to meet with international leadership on aviation security. In these meetings, they reviewed security procedures and technology being used to screen passengers on U.S.-bound flights and worked on ways to bolster our collective tactics for defeating terrorists.

Later in January, Secretary Napolitano traveled to Toledo, Spain and Geneva, Switzerland to meet with her international counterparts and the private sector air carriers on aviation security. In Spain, at the invitation of the Spanish Minister of Interior, the Secretary participated in the first organizational meeting of the Spanish EU Presidency of Justice and Home Affairs ministers, a plenary of thirty-three countries. At this meeting, there was broad consensus and a clear sense of urgency to take immediate action to strengthen security measures, as the Secretary 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. There was similarly strong consensus in Geneva, where the Secretary met with the leaders of the International Air Transport Association, which represents approximately 230 airlines and more than 90 percent of the world's air traffic. They agreed that government and the private sector must work collaboratively both to develop enhanced international security standards and-most importantly-to implement them effectively.

These meetings were the first in a series to bring about international agreement on stronger aviation security standards and procedures. Over the next few months, the International Civil Aviation Organization (ICAO) will facilitate several regional aviation security meetings to build on the progress made in Toledo and Geneva. TSA, specifically, has also developed an aggressive timeline and corresponding strategy for international engagement and outreach through our Office of Global Strategies. Focusing on priority areas designed to affect the greatest change in international civil aviation security, TSA is boosting its work with foreign government counterparts and industry stakeholders to raise awareness of the threat and to encourage specific enhancements in security measures worldwide. These priorities include: developing a common view and understanding of the threat to civil aviation; enhancing international standards for civil aviation security through ICAO; conducting security audits and ensuring robust oversight; encouraging the use of technological and non-technological measures to prevent and deter terrorist activity in the civil aviation sector; developing cooperative agreements for information sharing with key foreign government partners; providing training and related technical assistance to develop and enhance sustainable security practices in partner countries; and working with appropriate foreign government counterparts to enhance their authorities in their national aviation security domain. This targeted coordination and

collaboration, through both bilateral and multilateral forums, will continue to advance our key security objectives and improve the overall level of security of international civil aviation while fostering our international partnerships and relations that are critical to this effort.

In all of these action areas to bolster aviation security, we are moving forward with a determination to safeguard the privacy and rights of travelers.

Conclusion

In closing, Mr. Chairman, TSA is taking aggressive action in the wake of the failed Christmas Day bombing. We are expanding and improving the use of technology, strengthening aviation security protocols with our foreign partners, developing long-term law enforcement capacities in aviation security, collaborating across the Administration in developing the next generation of aviation security technology, working to streamline and improve the U.S. watchlist matching process for air travelers, and strengthening a TSA workforce that is highly trained, agile and dedicated to this mission. TSA and DHS are prepared to meet the challenge.

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

3.11.2010

Advanced Imaging Technology: "Radiation Risk Tiny"

You may have read a recent article stating that Advanced Imaging Technology used at TSA checkpoints is not safe. Because of the discussion the article has created, I wanted to share this with you.

The American College of Radiology posted an article titled: ACR Statement on Airport Full-body Scanners and Radiation and then **WebMD** followed up with an article titled New Airport Scanners: Radiation Risk Tiny which quoted the ACR article.

From the ACR article: "An airline passenger flying cross-country is exposed to more radiation from the flight than from screening by one of these devices. The National Council on Radiation Protection and Measurement (NCRP) has reported that a traveler would need to experience 100 backscatter scans per year to reach what they classify as a Negligible Individual Dose. The American College of Radiology (ACR) agrees with this conclusion. By these measurements, a traveler would require more than 1,000 such scans in a year to reach the effective dose equal to one standard chest x-ray."

"The ACR is not aware of any evidence that either of the scanning technologies that the TSA is considering would present significant biological effects for passengers screened."

We also asked the **Johns Hopkins University of Applied Physics Laboratory** to perform an independent radiation safety engineering assessment of our Advanced Imaging Backscatter Technology and they determined that the radiation dose to scanned individuals from this general use system is within the requirements of ANSI N43.17 2002 and 2009.

In the coming weeks, the FDA will be posting similar information on their web page.

For your reference:

Backscatter technology projects an ionizing X-ray beam over the body

Search

Blog Home

Aviation News Of The Weird

Blog Post Archives

Comment Policy

Contact The TSA Blog Team

Follow The TSA Blog Team On Twitter

Meet Our Bloggers

Please Post Off Topic Comments Here

What To Know Before You Go

Previous Posts

- Live Aviation Security Chat with Secretary Napolit...
- Backscatter Advanced Imaging Technology on Its Way...
- What Ever Happened To The Shoe Scanner Idea?
- What Happens If My Hands Alarm During an Explosive...
- Four Year Old Boy In Philly Told To Remove Leg Bra...
- Explosive Trace Detection Usage Expanded: Give Us ...
- Bollywood Confidential
- TSA Haiti Evacuation Effort: A Federal Security Di...
- Orlando Officer Arrested
- What's Wrong With This Picture?

Blogroll

surface at high speed. The reflection, or "backscatter," of the beam is detected, digitized and displayed on a monitor. Each full body scan produces less than 10 microrem of emission, the equivalent to the exposure each person receives in about 2 minutes of airplane flight at altitude. It produces an image that resembles a chalk-etching.

Millimeter wave technology bounces harmless electromagnetic waves off of the human body to create a black and white image (not a photograph). It is safe, and the energy emitted by millimeter wave technology is the energy projected by the system is thousands of times less intense than a cell phone transmission. This technology is not new. TSA is not the first to use this technology. It's currently being used in Canadian airports and U.S. courthouses in Colorado and Texas as well as international locations.

This Standard limits the reference effective dose2 delivered to the subject to 0.25 microsieverts (25 microrem) per screening.

For your reading pleasure, here are some documents relevant to security screening of humans using ionizing radiation:

ANSI/HPS N43.17-2009 Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation

NCRP commentary 16, Screening of humans for security purposes using ionizing radiation scanning systems

NCRP Statement 10, Recent Applications of the NCRP Public Dose Limit Recommendation for Ionizing Radiation (2004)

NCRP report no. 116 Limitation of Exposure to Ionizing Radiation (1993) ISBN 0-929600-30-4 recommends annual limits on radiation dose for the general public. Report 116 also introduces the concept of a negligible individual dose.

NCRP report no. 160, Ionizing Radiation Exposure of the Population of the United States (2009)

Screening Individuals with Backscatter X-Ray Systems by Daniel Strom

HPS Position Statement Use of Ionizing Radiation for Security Screening Individuals

HPS Public Information Radiation Exposure During Commercial Airline Flights

American College of Radiology (ACR) Statement on Airport Full-body Scanners and Radiation

EPA.gov Ionizing Radiation

Information on laws and regulations applicable to manufacturers of people screening security systems that use x-rays is on FDA's X-Ray & Particulate Products other than Medical Diagnostic or Cabinet page.

ANSI/HPS N43.17 is not a mandatory standard. More information on the ANSI standards setting process is available on the ANSI website.

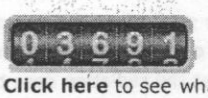
Above the Capital
Airplane Geeks Aviation Podcast
ars technica
Cranky Flier
Dipnote DOS
DOD Live
Fast Lane DOT
Flying With Fish
Greenversations
Homeland Security Watch
In Case of Emergency, Read Blog
Middle Seat Journal
Rick Seaney
Schneier on Security
Security Debrief
Security Director News
Stuck At The Airport
The Blog @ Homeland Security
The Beacon (USCIS)
Things With Wings
White House Blog

Links
TSA.gov
DHS Leadership Journal
Google TSA News

Download
Acrobat Reader

Subscribe in a reader

1696 readers
BY FEEDBURNER



Click here to see what will get your comment deleted.

The concept of justification based on a societal benefit appears in the International Commission on Radiological Protection (ICRP) report 60 (see paragraph S14).

Random Facts:

For comparison, the energy projected by millimeter wave technology is 10,000 times less than a cell phone transmission.

We, and all objects around us, generate millimeter wave energy - and we are exposed to it every single day.

Backscatter technology uses low level X-ray and a single scan is the equivalent of two minutes of flying on an airplane.

Full Body Scanners at Security Okay by Travelers - When it comes to the newest addition to airport security, 79 percent of travelers said they are comfortable with U.S. airports using full body scanners that can see through clothes.

We've written many posts on Advanced Imaging Technology and you can read them all **HERE.**

Blogger Bob
TSA Blog Team

Labels: advanced imaging technology, backscatter, Blogger Bob, Safety

Digg This! • Save to del.icio.us • Technorati Links • Share on Facebook

Posted By Blogger Bob At 2:16 PM

182 Comments:

Anonymous Said...

Sorry, Bob, but your agency has lied to the traveling public so much and for so long that we've lost trust in them to tell us the truth.

March 11, 2010 2:41 PM

RB Said...

Backscatter + flight = greater accumiltive radiation dose.

What long term studies have been completed to backup these claims?

Oh, you can keep on calling these Strip Search Machines "AIT" be we all know they are no less than "Kiddie Porn" Machines.

March 11, 2010 2:42 PM

Sandra Said...

"When it comes to the newest addition to airport security, 79 percent of travelers said they are comfortable with U.S. airports using full body scanners that can see through clothes."

That survey was done almost immediately after the underwear bomber tried to strike.

Dollars to donuts a new survey, done properly, would show a much lower acceptance rate.

Didn't the TSA try to tell us that the acceptance rate was about 95% at one time - before people learned what WBI really does. Can you explain the difference in the figures?

Bob, why was WBI renamed AIT?

What's being done by TSA to assure air travelers that perverts aren't looking at their naked scans or patting them down?

Has TSA instituted psychological assessments yet in its hiring practices?

March 11, 2010 2:49 PM

Bill Said...

Anonymous said...
Sorry, Bob, but your agency has lied to the traveling public so much and for so long that we've lost trust in them to tell us the truth.

Imperturbable Point Man Bob is undoubtedly overwhelmed by your sagacity. (sarcasm)

The post was up all of 25 minutes before you graced it with your wisdom--certainly not enough time to have read the 20+ links from scientific and medical experts. In fact, only the first paragraph (two sentences) are Bob's. The rest of the post are properly attributed quotations.

I'm not Bob.

March 11, 2010 3:05 PM

Anonymous Said...

Even the smallest bit of radiation should be avoided if there is no need for it. Radiation damage is accumulated. Should we all be hysteric? Probably not. But why sink millions of USD into a technology that doesn't provide additional security for passengers?

There are western countries that prohibited the use of these scanners for the reason that they don't detect WEI.

As a frequent flyer I'm relying on airport security. But I don't want the voodoo scurity the TSA does. It takes too long, it is not effective and it is an invasion into our privacy. So why does the TSA do it?

March 11, 2010 3:09 PM

Winstonsmith Said...

Even if I were going to stipulate to your safety data (I have no reason to believe you, but I have no evidence to counter you either), I certainly take issue with your citing an unsubstantiated 79% acceptance claim of your unconstitutional strip search technology based on a 2-line filler item on a travelers' news blog that cites nothing about who commissioned the study, when the study was done, who was asked, and how well the survey respondents understood exactly what the technology could do vis à vis their rights to be free from unreasonable search and seizure versus your permissible blanket "administrative search" are. Further that with the dimunition already cited above from your once touted 95% acceptance and you have the beginning of a public awakening of TSA's continuing and ineffective overreach.

I renew my call for the TSA budget to be slashed, for the funds to be redirected to constitutionally permissible off-airport investigation and surveillance of actual suspect persons, and to go back to the simple screening procedures we had pre-9/11 with the addition of a smarter flying public and hardened cockpit doors.

March 11, 2010 3:23 PM

Anonymous Said...

What steps is TSA taking to ensure every passenger asked to be strip-searched knows he or she can decline the strip-search?

March 11, 2010 3:38 PM

Anonymous Said...

Bill spewed:

Imperturbable Point Man Bob is undoubtedly overwhelmed by your sagacity. (sarcasm)

The post was up all of 25 minutes before you graced it with your wisdom--certainly not enough time to have read the 20+ links from scientific and medical experts. In fact, only the first paragraph (two sentences) are Bob's. The rest of the post are properly attributed quotations.

That's the problem with lying. TSA destroyed its credibility with many frequent travelers years ago and recently has done next to nothing to rebuild that same credibility. If a member of TSA management told me that the sky was blue I would check it out before believing them.

March 11, 2010 3:55 PM

Anonymous Said...

So the TSA admits that the devices are harmful but belittles the public by condescendingly telling us the flight is even worse for us.

I'm so not surprised by this behavior.

I choose to accept the risks associated with flight but choose to NOT accept the risks - health and otherwise - of these invasive machines.

March 11, 2010 4:05 PM

Anonymous Said...

How do we know that a guy like this http://www.thebostonchannel.com/mostpopular/22785620/detail.html is not going to be in the WBI viewing room?

March 11, 2010 5:46 PM

Anonymous Said...

Are you completely oblivious to the irony of the words "risk tiny" in the title of your post? How would you characterize the risk of dying in a terrorist attack targeting commercial aviation? Significant?

March 11, 2010 5:54 PM

Ayn R. Key Said...

The real question is this: When you have completely safe mmw, why do you use backscatter at all?

Seriously, no matter how tiny the risk, there is an equivalent technology that is still safer.

Is it lower cost? Does backscatter cost less than mmw?

March 11, 2010 5:58 PM

WRoberts Said...

As a qualified expert, within the meaning of 10 CFR 35, there are two sides of this issue. Side one is what is the minimum acceptable "safe" radiation dose? Our knowledge of radiobiology seems to demonstrate that a low level radiation is apparently harmless. However, the current regulatory agencies and the NCRP (National Commission on Radiation Protection) all base their regulatory activities on the assumption that risk of harm from radiation is a linear function with no lower dose limit threshold.

The FDA commissioner is probably correct in that an individual will likely not experience any direct adverse effects.

However, this must be contrasted against the BEIR VII report (Biological Effects of Ionizing Radiation 7th Committee). As did its predecessor committees, this group looked at Atomic Bomb survivors, dosimetry from the Radiation Effects Research Foundation, UNSCEAR and others.

They looked at the various models of risk of radiation injury:
Linear No safe Threshold dose model
Safe threshold of radiation;
exposure and linear increase in risk above that threshold;
Linear quadratic model;

These three models have been debated for decades.

The conclusion of the BEIR VII:

They state that their goal was not to prove or disprove any of the models, but rather develop a model that best fits the physical, biological and epidemiological data.

They looked at cellular radiobiology, genetic effects, and epidemiological effects. After studying the scientific evidence, including laboratory studies,and populations exposed (radiation workers, Chernobyl, Semipolitinsk, Urals, A-Bomb survivor data.

They conclude as follows:
For solid cancers the LNT (Risk of cancer increases in a straight line with any exposure above zero) model best fits the data. IE any radiation will increase the risk of developing a cancer, and the more exposure over a lifetime the greater that risk. They state that cancer risk is clearly greater at exposure above 100 mSv.

For genetics, the doubling dose of risk to genetic (heritable damage) is estimated at 1 Sv (1000 mSv).

The final conclusion in the summary report is the Linear No Threshold model is a best fit with the current scientific evidence, but also notes that at very low doses the risk is also very small.

The problem is this: we are using radiation increasingly in society for medical testing, non-destructive testing, treatment of disease, and now proposed and actual travel inspection.

All of this increases the population doses and individual doses. If the BEIR VII and the National Academy of Science concludes that these doses add up and increase the risk of radiation injury, eventually as we keep adding radiation exposure in our ordinary environment, then we increase the risk of having a less healthy population.

Backscatter technology per the BEIR VII report which affirms its predecessor committee reports, adds population exposures and individual exposures and thus increases risk, albeit small. But this risk is avoidable as other technology is available.

In keeping with the principle of ALARA (as low as reasonably achievable radiation exposures) we should probably not deploy these machines.

March 11, 2010 5:58 PM

Anonymous Said...

Posh! Why is everyone so hot and bothered about being stripped, exposed to radiation and treated as an inmate? It's a new world. If the government wants to inconvenance you they have that right. You gave it to them through your elected representatives.

You might show how brilliant you are on this blog, but do you really believe anyone that can change anything is parked in front of a keyboard waiting for your thoughts?

The change makers are at the $2,500/plate fundraisers getting ready for

the next campaign.bri

March 11, 2010 6:10 PM

Ayn R. Key Said...

Very funny, Bob. Many of those links are to sites that request you pay to receive the information. Some of the links don't work very well.

But here's from one of the free sites, HPS Position Statement Use of Ionizing Radiation for Security Screening Individuals.

"In radiation protection, no exposure is justified unless it produces a positive net benefit"

Since you have a valid alternative, then according to one of your supportive links, backscatter is NOT JUSTIFIED! You can claim that the benefit is increased security, but did you mention to HPS that you have a valid workable alternative? Did you? Or did you simply tell them "this is the technology we have, is it safe?"

In other words, did you lie to them by omission?

Did you tell your friendly sources that there is a safe alternative?

Bob, answer the question. Do I have to file a FOIA just to get the answer to that one question, because in this case I am quite willing to.

March 11, 2010 6:24 PM

Anonymous Said...

Thanks but I will continue to decline the AIT devices. If I don't have to expose myself to that extra radiation why should I?

Did these research studies also test to see if radiation used in these devices only exposes those being scanned? What about the poor TSOs who work around the devices all day. Will they be suing the Feds in years to come for radiation exposure related disorders?

March 11, 2010 6:58 PM

RB Said...

Ayn R. Key said...
The real question is this: When you have completely safe mmw, why do you use backscatter at all?

Seriously, no matter how tiny the risk, there is an equivalent technology that is still safer.

Is it lower cost? Does backscatter cost less than mmw?

March 11, 2010 5:58 PM

.....

TSA greasing the right pockets?

March 11, 2010 7:57 PM

Anonymous Said...

Anonymous said...

Thanks but I will continue to decline the AIT devices. If I don't have to expose myself to that extra radiation why should I?

Did these research studies also test to see if radiation used in these devices only exposes those being scanned? What about the poor TSOs who work around the devices all day. Will they be suing the Feds in years to come for radiation exposure related disorders?

Workman's comp claims here we go. FWIW, they really don't care about the front line TSOs as they are replaceable. They develope cancer/cataracts? Too bad, so sad. Fire them before they go on long term disability.

March 11, 2010 8:51 PM

Anonymous Said...

What about increased cataract risk?

What about the studies that suggest destruction of DNA in outer and middle layer skin cells for wavelengths near the MMW frequencies and for ionizing radiation like backscatter? Particularly for those of us with history of melanoma in first-degree relatives?

How often will these machines be calibrated to make sure they haven't gone out of spec and started overdosing passengers? Will the controls be as strict as those on my physician's and dentist's x-ray machine? Who at TSA will be held accountable when passengers are overdosed? Who will lose their job? Who will guarantee the passengers receive appropriate compensation?

March 11, 2010 9:42 PM

Avxo Said...

I'll ask here again, since my post on the other thread hasn't been approved yet:

Can the resolving power of the XRB and MMW machines be increased while they are deployed? If so, who can make the changes and under what conditions? Does that operation require modifications to the machine itself, or it is a software option?

More specifically, about the X-ray machines:

How often are the units tested to ensure that they remain in safe operational conditions? Who conducts these tests?

Do the machines employ fail-safe protocols and automatically shut down if they detect internals faults? Are these machines certified by any independent authority?

Do the machines employ any sort of flattening filters, collimators,

waveguides, or other devices used to attenuate the generated X-ray beam? If so, are those components fixed, or can they be removed? Will the machine operate if those components are removed?

Is the TSA personnel that operates the machines trained in the principles behind the XRB machine and general radiological safety, or will they only be trained to look at the picture and click oversized "Good" or "Bad" buttons?

March 11, 2010 10:54 PM

Avxo Said...

Ayn R. Key wrote: "*The real question is this: When you have completely safe mmw, why do you use backscatter at all?*

Seriously, no matter how tiny the risk, there is an equivalent technology that is still safer."

That's an awesome question. Given the fact that MMW has none of the nasty side-effects of XRB (no matter how insignificant those side-effects may be) why not just go with MMW, which has no such side-effects?

March 11, 2010 10:57 PM

Anonymous Said...

I definitely prefer the body scan to being "patted down" by some agent who seems to think she is the most important person in the world and claims she doesn't enjoy the process of patting down. The safety of the body scanner is a consideration but IMHO a better choice for security.

March 12, 2010 12:56 AM

Anonymous Said...

Okay. Let's just mess with some numbers here.

A TSO is on the line for 8 hrs. At 25 seconds or so a person, that is (60/25*60*8)scans occuring per shift. Considering the radiation delivered by these scans falls of at according to RMS rules (doubling the distance quarters the power exposed), that means that a TSO standing 8 feet away will recieve a 1/16th reflected scan. Let's be generous with the assumption that the scattered radiation reflected from the person in the scanner is 1/4th the original exposure. So, now that we have the problem set up... what's the answer?

A TSO standing 8 feet away from one of these will recieve, in an eight hour shift, will be exposed to 1152 scans, each of 1/64 the original power emitted. Now, this works out to works to the same as 18 passes through one of these machines a day in an 8hr shift.

Given that there won't be just one of these machines at each checkpoint, and that your average TSO is going to be standing a little bit closer, I'd say a nice round number of 20-25 scans a day equivelancy for secondary exposure is more accurate. Now, at this rate, it would take a horribly long 10 weeks for a TSO to achieve the same radiation exposure as 1

chest X-ray. Hrm.. 5 chest X-rays a year at 8 feet starts looking a little bit on the glow-in-the-dark side of radiation safety on the job, doesn't it? At six feet (roughly where the female TSO is standing) your looking at 32 scans a day equivelant exposure, 6 weeks to reach the magic chest X-ray, and 9 chest X-rays a year. I really hope she has a lead-lined corset on under that uniform, cause if she wants to have children, she's going to need it!

So, what is the safe distance for the TSO to be standing from the scanner for 8hrs a day? Does the TSA intend to comply with OSHA's placarding requirements for low level radiation in the workplace?

March 12, 2010 2:36 AM

Ayn R. Key Said...

RB wrote:
TSA greasing the right pockets?

That's a good point. I notice the change from mmw to xrb occurred about one year ago.

Did the manufacturer of mmw donate to McCain while the manufacturer of xrb donate to Obama?

March 12, 2010 12:11 PM

Gunner Said...

OK, simple question:

Will the person who is ogin gto be viewing the images have to go through to scanner to ensure they do not have any USB or hidden recoding devices planted on their body?

If not, why not?

March 12, 2010 12:33 PM

Ayn R. Key Said...

Thanks, avxo. But given that I am the one who asked it, it is certain Bobbo won't answer it.

He's waiting for a very snarky comment from me so he can respond to that instead.

March 12, 2010 12:43 PM

RB Said...

Ayn R. Key said...
RB wrote:
TSA greasing the right pockets?

That's a good point. I notice the change from mmw to xrb occurred about one year ago.

Did the manufacturer of mmw donate to McCain while the manufacturer of xrb donate to Obama?

March 12, 2010 12:11 PM

.....

Find out who Chertoff is working for and I think you will have your answer.

March 12, 2010 1:40 PM

Avxo Said...

Anonymous wrote: "*Considering the radiation delivered by these scans falls of at according to RMS rules (doubling the distance quarters the power exposed), that means that a TSO standing 8 feet away will recieve a 1/16th reflected scan.*"

RMS? You're thinking of inverse-square law, not root-mean-square. Regardless, your math is wrong there -- and fundamentally flawed. On top of that you make assumptions that may not necessarily hold true.

I'm no fan of x-ray backscatter devices, and there are plenty of legitimate points to be made about them.

March 12, 2010 2:50 PM

Anonymous Said...

Chertoff's got both of his hands up to his elbows involved with the backscatter technology. No surprise.

Leave DHS/TSA and become an influential lobbyist making big $$$$$ shilling for equipment that may or may not be useful in the WOT.

March 12, 2010 2:55 PM

Anonymous Said...

Bob, tiny does not equal nonexistent especially for cancer survivors.

March 12, 2010 3:59 PM

Ayn R. Key Said...

These are some pretty serious allegations, RB. Accusing the TSA of putting our health at risk when there is a safe alternative, because the manufacturer of the unsafe equipment has better political connections ... that's a pretty big accusation of corruption.

So do you think Bob is going to address this?

March 12, 2010 4:05 PM

Dave Nelson Said...

For WRoberts:

Thanks very much for your discussion. I would like to see exactly how the questions were put to the FDA and others and the specific ground rules and assumptions the other evaluations used as well.

The TSA has no interest in a scientific debate on the subject. As a matter of fact, they fear a public debate. I read a white paper written by someone in the TSA or DHS about their concerns about introducing strip search machines. The primary concern was that public opposition could derail the entire program and that the TSA needed to engage in an intense campaign to "sell" this to the public to win their consent and acceptance.

When I think about it for a few minutes, you can determine all of the sell-job tactics the TSA has been trying:

1. It's not really intrusive. They go to great lengths to explain the operator set up and, trust us, we don't keep images.

2. It will go a whole lot faster if you people roll over.

3. We have to stay one step ahead of the bad guys -- the good old fear-mongering approach

4. Forcing us to choose between two equally invasive and needlessly intrusive alternatives -- strip search or (call it what it really is) a police-type frisking.

5. Nobody is forcing you to fly.

6. It's safe; trust us.

7. I have no problem with my wife & kids going through it. (... still waiting for those pictures, Nico.)

8. 90% of people like it! Of course, there is no supporting data to back this statement up.

The TSA and their agents on this blog are selling this like a bunch of drug dealers. The truly sad thing is that the American people don't care.

March 12, 2010 4:31 PM

8675309 Said...

Most of the detractors have no real argument and have to resort to name calling: "Strip Search Machines" "Child Porn Viewers" "Radiation Portholes" and what have you, but why do you continue to complain over and over and over again?

IN THE USA, GOING THROUGH THESE MACHINES IS OPTIONAL.

If you don't like it, don't do it.

I don't care if the machines cost more money. I'd rather go through the machine than have some stranger run their hands all over my body.

Why don't you read the news about all the teachers that have slept with their students and then go blog about how we should stop spending

money on education?

March 12, 2010 4:54 PM

Anonymous Said...

To be honest I am afraid as a TSA employee to be exposed to these machines on a daily basis. What kind of radiation would I be getting standing next to one 40 hours a week. They can't be that safe. Same thing with our xray machines with led curtains that are constantly opening up while we run the machine, but we won't go there!

March 12, 2010 4:54 PM

Anonymous Said...

I asked this question multiple times on multiple posts and still have not gotten an answer. so here goes again:

What date or year are the TSA provided AIT sample images from? Were they taken with the newest generation machines or earlier generation ones?

March 12, 2010 8:02 PM

TSOWilliamReed Said...

I do wonder why the deployment of backscatter machines over the MMW machines. I prefer the MMW machines and the commenters statement of the TSO's exposure does worry me. Passengers will be recieving a minimal dose honestly, maybe the average passenger flys around 3-5 times a year. The TSO is going to scan hundreds of people a day. Bob, I was wondering what safety protocols will be in place for TSO's that will be exposed to hundreds of scans every day all year long? Not to mention doing test runs in their own airport and getting scanned directly.

March 13, 2010 10:55 AM

Anonymous Said...

People have the right to not go through the AIT and guess what if you dislike TSA this much people you can also drive or take a bus! please do! :)

March 13, 2010 12:40 PM

RB Said...

RB said...
Ayn R. Key said...
RB wrote:
TSA greasing the right pockets?

That's a good point. I notice the change from mmw to xrb occurred about one year ago.

Did the manufacturer of mmw donate to McCain while the manufacturer of xrb donate to Obama?

March 12, 2010 12:11 PM

.....
Find out who Chertoff is working for and I think you will have your answer.

March 12, 2010 1:40 PM

.....

Chertoff is a former homeland security secretary and the founder of the Chertoff Group, a security consulting firm whose clients include manufacturers of full-body scanners.

.....

Available information seems to say that Chertoff will not disclose who he represents but he actively presses for deployment of Strip Search Machines all while not disclosing the fact that he does represent manufacturers of these devices.

How's that for honesty?

Now you know where DHS/TSA get it from.

March 13, 2010 1:17 PM

Anonymous Said...

So, you're saying that the risk is tiny but acceptable. Is that tiny risk larger or smaller than the risk that someone's flip-flop is a disguised weapon, incendiary, or explosive? Bear in mind that there has never been a successful attack on aviation with a shoe, regardless of whether or how passengers' shoes are screened when you answer, Bob.

March 14, 2010 4:17 PM

Anonymous Said...

Now Bob,

While the radiation and images do not bother me, what happens when I am wearing a medical device? Although the TSA has not changed its rules, as of late people wearing insulin pumps and declaring them (as instructed by the TSA website) have been subject to complete carry-on bag assaults by TSA agents (although no written statements tell you that because you are diabetic, your luggage will be taken apart and not just scanned normally. I understand an extra pat-down, but this power trip must stop).

I digress, since an insulin pump must clearly be declared for use in these machines, does this now mean that every flight I take, my carefully packed bag will be emptied and inspected instead of passing through the normal belt for inspection? Or is this another made up rule by TSA agents? Is this machine even safe for those wearing insulin pumps? I can find no answers on this.

Please answer.

Allison

March 14, 2010 6:21 PM

Ayn R. Key Said...
Well, Bob, it's going public again.

And the TSA actually responds

Picked up by a news outlet

March 14, 2010 10:17 PM

Protex Said...
I'm completely okay with the use of biometric or full body scanners. As a paranoid traveler there is nothing better than to feel safe when traveling.

Why do we need to wait for another tragedy to get people to support these types of full body scanners. I will gladly volunteer to be scanned first!

March 14, 2010 11:14 PM

Eric Said...
Another blow to the 4th Amendment of the Constitution. And the reactionaries in Congress accuse Obama of wanting to turn the US into a socialist state. Next we'll be required to have internal passports like the USSR, Nazi Germany and Israel.

March 14, 2010 11:41 PM

Lynne Foster Said...
Many of us are not happy with this scanners.There is really no other way to avoid this scanning?

March 15, 2010 12:43 AM

RB Said...
Ayn R. Key said...
These are some pretty serious allegations, RB. Accusing the TSA of putting our health at risk when there is a safe alternative, because the manufacturer of the unsafe equipment has better political connections ... that's a pretty big accusation of corruption.

So do you think Bob is going to address this?

March 12, 2010 4:05 PM
.....
You explain then why TSA would install a device that may cause harm when they have perfectly usable non-radiating alternatives.

March 15, 2010 9:57 AM

Anonymous Said...
TSOWilliamReed said...

I do wonder why the deployment of backscatter machines over the MMW

machines. I prefer the MMW machines and the commenters statement of the TSO's exposure does worry me. Passengers will be recieving a minimal dose honestly, maybe the average passenger flys around 3-5 times a year. The TSO is going to scan hundreds of people a day. Bob, I was wondering what safety protocols will be in place for TSO's that will be exposed to hundreds of scans every day all year long? Not to mention doing test runs in their own airport and getting scanned directly.

Purchase a pocket dosimeter and wear it around waist level. Read and record the daily/weekly/monthly levels as this might be critical when you wind up with radiation exposure induced cancer and want to file a workman's compensation claim against the government.

March 15, 2010 10:16 AM

Anonymous Said...

Allison, you stand a better chance of getting an invitation to a White House state dinner (transportation included) than you do getting an answer from TSA.

March 15, 2010 11:08 AM

Al Ames Said...

Protex, there is a big difference betweein **FEELING** safe and **BEING** safe.

Experts have already said that there was no guarantee these machines would have detected the underwear bomber. In fact, it cited at best a 60% chance of detection.

60% chance for the invasion of privacy, no enhancement to safety, and potential health risks? No thanks.

I should have to have my privacy compromised for your paranoia, especially when the measure is just to assuage your paranoia.

I fly 100k miles per year and I'm not paranoid, despite TSA's lack of security.

As others say for those who disagree with TSA, if you're that afraid of flying, don't fly. Despite TSA's miserable performance rate, your chance of dying in plane crash over the last 10 years (including 9/11) is 20 times **LESSM** than getting struck by lightning.

Are you that paranoid about getting struck by lightning as you are about getting on a plane?

Al

March 15, 2010 11:28 AM

Blogger Bob Said...

Allison Said: Now Bob, While the radiation and images do not bother me, what happens when I am wearing a medical device? Although the TSA

has not changed its rules, as of late people wearing insulin pumps and declaring them (as instructed by the TSA website) have been subject to complete carry-on bag assaults by TSA agents (although no written statements tell you that because you are diabetic, your luggage will be taken apart and not just scanned normally. I understand an extra pat-down, but this power trip must stop). I digress, since an insulin pump must clearly be declared for use in these machines, does this now mean that every flight I take, my carefully packed bag will be emptied and inspected instead of passing through the normal belt for inspection? Or is this another made up rule by TSA agents? Is this machine even safe for those wearing insulin pumps? I can find no answers on this. Please answer. Allison March 14, 2010 6:21 PM

Hi Allison. Per the TSA web page, you do not have to tell us you have an insulin pump. It's an option if you're not comfortable going through the metal detector with it. If you are concerned or uncomfortable about going through the walk-through metal detector (WTMD) with your insulin pump, notify the Security Officer that you are wearing an insulin pump and would like a full-body pat-down and a visual inspection of your pump instead. As far as your bags being searched, this could be triggered by a number of things. Without being there, it's hard for me to speculate. As far as the safety of your device going through the WTMD, I would contact the manufacturer of your pump, but I have heard of no safety issues regarding pumps and WTMDs. I just checked a web page from a manufacturer and it said there are no safety concerns. But I'll let you research that on your own.

Thanks,

Blogger Bob
TSA Blog Team
March 15, 2010 12:13 PM

Anonymous Said...
I wonder if a unionized TSA would refuse to work near the backscatter machines because of safety concerns?
March 15, 2010 12:20 PM

Ayn R. Key Said...
RB wrote:
You explain then why TSA would install a device that may cause harm when they have perfectly usable non-radiating alternatives.

I'd rather Bob explain it.
March 15, 2010 12:22 PM

Blogger Bob Said...
Anonymous said... Okay. Let's just mess with some numbers here. A TSO is on the line for 8 hrs. At 25 seconds or so a person, that is

(60/25*60*8)scans occuring per shift. Considering the radiation delivered by these scans falls of at according to RMS rules (doubling the distance quarters the power exposed), that means that a TSO standing 8 feet away will recieve a 1/16th reflected scan. Let's be generous with the assumption that the scattered radiation reflected from the person in the scanner is 1/4th the original exposure. So, now that we have the problem set up... what's the answer? A TSO standing 8 feet away from one of these will recieve, in an eight hour shift, will be exposed to 1152 scans, each of 1/64 the original power emitted. Now, this works out to works to the same as 18 passes through one of these machines a day in an 8hr shift. Given that there won't be just one of these machines at each checkpoint, and that your average TSO is going to be standing a little bit closer, I'd say a nice round number of 20-25 scans a day equivelancy for secondary exposure is more accurate. Now, at this rate, it would take a horribly long 10 weeks for a TSO to achieve the same radiation exposure as 1 chest X-ray. Hrm.. 5 chest X-rays a year at 8 feet starts looking a little bit on the glow-in-the-dark side of radiation safety on the job, doesn't it? At six feet (roughly where the female TSO is standing) your looking at 32 scans a day equivelant exposure, 6 weeks to reach the magic chest X-ray, and 9 chest X-rays a year. I really hope she has a lead-lined corset on under that uniform, cause if she wants to have children, she's going to need it! So, what is the safe distance for the TSO to be standing from the scanner for 8hrs a day? Does the TSA intend to comply with OSHA's placarding requirements for low level radiation in the workplace? March 12, 2010 2:36 AM

While I'd like to sit back and rub my goatee while smoking my Mahogany Calabash pipe, I can't take credit for this response.

(This response has been confirmed by Certified Health Physicists)

In general, the scenario above is well thought out. However, there is one incorrect assumption in the calculation -- the scatter faction for x-rays is not 1/4.

For the energy these system operate at, the scatter faction is roughly 1/1000th.

Here's the calculation:

1 scan every 25 seconds results in 60/25*60*8 = 1152 scans per 8 hours shift.

8 feet away (roughly 4 times the distance) reduces the intensity to 1/16 the original value.

Scatter faction of 1/1000.

Then using the maximum allowable dose per screening of 0.025 millirem gives a yearly dose of:

1152 screenings/shift * 0.025 rem/screening * 1/16 * 1/1000 * 5

days/week * 50 work-weeks/year = 0.45 mrem

For comparison purposes, this is about the amount of radiation a person receives from 12 hours of natural background radiation or 1 hour of flight at 39,000 feet. Differences in background radiation levels in various parts of the U.S. are easily 50 mrem/year or more.

Also, the above calculation assumes the individual is 8 feet from the system 100% of the time. In general people move around during the day and take breaks. Most of the time is spent further from the system which will reduce the actual radiation dose even further.

Some other things to consider to put situation into perspective are:

1. In the U.S. the occupational exposure limit is 5,000 mrem/year.

2. The recommended occupational dose limit for pregnant women is 500 mrem during the pregnancy.

3. The U.S. and international recommended dose limit for the public is 100 mrem/year.

4. Radiation warning signs are required in areas where a person can receive 5 mrem or more in 1 hour.

Blogger Bob
TSA Blog Team

March 15, 2010 12:25 PM

Anonymous Said...

Bob, you're making the assumption that the equipment is working correctly, that there are no radiation leaks from poor maintenance, etc.

People asked questions about how the equipment is maintained and those questions went unanswered. On another blog a TSO commented on the lead lined flaps for the carry on luggage being worn and sticking open. If that is the case, then at least at that airport TSA is exposing both workers and passengers to unnecessary radiation exposure. Also it reflects poorly on your agency's commitment to keeping the travelers safe.

March 15, 2010 12:38 PM

RB Said...

Some other things to consider to put situation into perspective are:

1. In the U.S. the occupational exposure limit is 5,000 mrem/year.

2. The recommended occupational dose limit for pregnant women is 500 mrem during the pregnancy.

3. The U.S. and international recommended dose limit for the public is 100 mrem/year.

4. Radiation warning signs are required in areas where a person can receive 5 mrem or more in 1 hour.

Blogger Bob
TSA Blog Team
.....

FDA say "no threshold of exposure below which x-radiation may not adversely effect human healths" yet TSA didn't use this information while trying to con the public on "AIT Child Porn Viewers".

Wonder why?

http://www.fda.gov/Radiation-EmittingProducts/ ResourcesforYouRadiationEmittingProducts/Consumers/ucm142625.htm

Is the TV Radiation a Hazard?

Scientists have not identified specific health effects resulting from exposure to extremely low doses of low-level radiation over prolonged periods of time. **However, the current assumption is that there is no threshold of exposure below which x-radiation may not adversely effect human health.**

March 15, 2010 12:49 PM

Anonymous Said...
RB, wait for a comment that x-rays coming from a television are not the same as x-rays coming from the AIT/WBI.

March 15, 2010 1:21 PM

Mr. Gel-Pack Said...
At 2,000,000 passengers per day, 1/1000 of a chest x-ray is worth 2,000 x-rays per day. Sure, you aren't doing them to the same person, but if it causes just one more person to die of cancer, is it really worth it?

Is the point of the whole-body-imagers to replace the objective metal-detecting test in favor of yet another ill-defined, subjective visual inspection?

Will the XRB (or the objectively safer MMW) detect a blasting cap hidden inside the body better than the plain-old walk-through metal detector?

How much safer is TSA making us? and is the microscopic benefit worth the added risk?

March 15, 2010 3:28 PM

Anonymous Said...
How can people not trust the government? Have they ever used

information for purposes other than intended, then lied? Have they physically harmed innocent people?

Oh, stay away from the French bread.

March 15, 2010 5:26 PM

Anonymous Said...

Bob

care to explain this?

http://www.chicagobreakingnews.com/2010/03/body-scanners-ohare-airport.html

Mandatory if thats the case bob your a liar and have bold face lied to everyone on this.

Ill let you explain, but this will be in my next letter to my congress critters, as well as to the committee members that have over-site of TSA as well.

Hey Nico where are the pictures of your family since you say these things are safe? were still waiting years later

March 15, 2010 6:03 PM

Avxo Said...

Blogger Bob wrote: "The U.S. and international recommended dose limit for the public is 100 mrem/year."

As far as I know that's the limit established by the DOE for amount of radiation that a member of the general public can be exposed to from DOE facilities and their operations.

Now, this may seem like nitpicking, but don't call it recommended please. We have recommended doses for things like vitamins, sodium, cholesterol and whatnot. But we don't have a "recommended radiation quota."

The term "recommended" suggests that one must receive that dose to remain healthy, just as one must receive certain nutrients etc to remain healthy.

March 15, 2010 8:48 PM

RB Said...

The truth is starting to leak out.

http://www.chicagobreakingnews.com/2010/03/body-scanners-ohare-airport.html

Official: Body scanners the future for all passengers

"Kathleen Petrowsky, the TSA director at O'Hare, said she anticipates that the body scans--now optional for passengers--will become mandatory in the future to guard against improvised explosive devices being smuggled onto airliners."

March 15, 2010 9:26 PM

Jared Said...

What does Jason Chaffetz have to say about this?

March 16, 2010 9:00 AM

TSOWilliamReed Said...

While I'd like to sit back and rub my goatee while smoking my Mahogany Calabash pipe, I can't take credit for this response.

(This response has been confirmed by Certified Health Physicists)

In general, the scenario above is well thought out. However, there is one incorrect assumption in the calculation -- the scatter faction for x-rays is not 1/4.

For the energy these system operate at, the scatter faction is roughly 1/1000th.

Here's the calculation:

1 scan every 25 seconds results in 60/25*60*8 = 1152 scans per 8 hours shift.

8 feet away (roughly 4 times the distance) reduces the intensity to 1/16 the original value.

Scatter faction of 1/1000.

Then using the maximum allowable dose per screening of 0.025 millirem gives a yearly dose of:

1152 screenings/shift * 0.025 rem/screening * 1/16 * 1/1000 * 5 days/week * 50 work-weeks/year = 0.45 mrem

For comparison purposes, this is about the amount of radiation a person receives from 12 hours of natural background radiation or 1 hour of flight at 39,000 feet. Differences in background radiation levels in various parts of the U.S. are easily 50 mrem/year or more.

Also, the above calculation assumes the individual is 8 feet from the system 100% of the time. In general people move around during the day and take breaks. Most of the time is spent further from the system which will reduce the actual radiation dose even further.

Some other things to consider to put situation into perspective are:

1. In the U.S. the occupational exposure limit is 5,000 mrem/year.

2. The recommended occupational dose limit for pregnant women is 500 mrem during the pregnancy.

3. The U.S. and international recommended dose limit for the public is 100 mrem/year.

4. Radiation warning signs are required in areas where a person can receive 5 mrem or more in 1 hour.

Blogger Bob
TSA Blog Team

March 15, 2010 12:25 PM

Thats good to know bob thanks for the peace of mind.

March 16, 2010 10:57 AM

TSOWilliamReed Said...

RB said...
Some other things to consider to put situation into perspective are:

1. In the U.S. the occupational exposure limit is 5,000 mrem/year.

2. The recommended occupational dose limit for pregnant women is 500 mrem during the pregnancy.

3. The U.S. and international recommended dose limit for the public is 100 mrem/year.

4. Radiation warning signs are required in areas where a person can receive 5 mrem or more in 1 hour.

Blogger Bob
TSA Blog Team
.....

FDA say "no threshold of exposure below which x-radiation may not adversely effect human healths" yet TSA didn't use this information while trying to con the public on "AIT Child Porn Viewers".

Wonder why?

http://www.fda.gov/Radiation-EmittingProducts/ ResourcesforYouRadiationEmittingProducts/Consumers/ucm142625.htm

Is the TV Radiation a Hazard?

Scientists have not identified specific health effects resulting from exposure to extremely low doses of low-level radiation over prolonged

periods of time. However, the current assumption is that there is no threshold of exposure below which x-radiation may not adversely effect human health.

March 15, 2010 12:49 PM

Yet we are exposed to hundreds of different low level radiation sources a day. The sun itself radiates the heck out of us every day. Electrical devices, power lines, radio signals, wireless router feeds surround us, cell phones, television sets, all sorts of things. The FDA isn't limiting or banning the use of any of these radiation sources and the scanner generates less radiation.

March 16, 2010 10:57 AM

Anonymous Said...

Hi, I tried looking around this blog and couldn't find the answer to this. There's a post on camping gear and allowed vs. banned items for carry-on, but inexplicably it didn't mention one of the main things people take on camping trips...tents.

Are tents allowed in carry-on bags, assuming they meet the size requirements? They come with poles at least (not all need stakes in some weather), and if fishing poles are allowed in certain circumstances, I wonder if tent poles would be allowed.

Can a person carry a small packed tent on a plane?

March 16, 2010 12:32 PM

Anonymous Said...

TSO WilliamReed:

Yet we are exposed to hundreds of different low level radiation sources a day. The sun itself radiates the heck out of us every day. Electrical devices, power lines, radio signals, wireless router feeds surround us, cell phones, television sets, all sorts of things. The FDA isn't limiting or banning the use of any of these radiation sources and the scanner generates less radiation.

There is a difference between ionizing (bad) radiation and non ionizing (good) radiation. Look it up.

March 16, 2010 1:01 PM

Anonymous Said...

Still wondering when the TSA is going to post full size and full resolution images produced by the newest generation WBI scanners.....

After all the TSA says they are not that detailed or explicit.....then what is the hold up??? Are you guys having trouble putting the scanner into "test mode" to allow for storage of the images?

March 16, 2010 1:51 PM

Anonymous Said...

Does the TSA have any comment responding to the multiple complaints by passengers last year regarding not being informed of the images the AIT scanners produce (no signage or verbal description) or the that they had a pat-down option before they were directed thru the machines?

http://epic.org/2010/03/epic-v-dhs-epic-obtains-compla.html

March 16, 2010 2:00 PM

Denny (Germany) Said...

Thus the general standard chest radiography may for example not too often be accomplished, since the dose comes otherwise into an health-endangering range.

Same probably for the scanners to be valid, ensure there particularly make themselves I around much flier, those can naturally too many jets not well stand, if you are for example each day everywhere in the world on the way.

With us in Germany 82% the citizen would not like to see naked scanners on German airports. These will however nevertheless come probably.

March 16, 2010 3:01 PM

Anonymous Said...

I do love the masterful use of the Hegelian dialectic in this discussion; first, the argument was about the machines themselves, now the argument is about one machine over another - which implies that a machine in general is acceptable.

Perhaps that is the point of this blog and the encouragement of posting counter arguements; to direct the social mood in favor of TSA.

March 16, 2010 3:18 PM

Anonymous Said...

I really hope that the project manager who fielded all of these finds out that he' bought a pig in a poke.

March 16, 2010 3:57 PM

Anonymous Said...

Fair Use extract From Defense Technology Intl interview with Rafi Sela (Israeli airport security expert):

... where are they (airports) going wrong in their procedure?
They have one place where they perform their security and the rest of the airport is wide open. There is no sense in enforcing one place and leaving the rest open. Security at Pearson International Airport in Toronto is more hassle than sense. This goes back to basics. They are so

busy finding water bottles and baby formula that they do not check the people or any other threats that can easily go through the scanners. I do not want to give specific details so as not to give terrorists ideas, but here is just one example: I traveled with an almost empty tube of toothpaste, which was larger that the size allowed. There was hardly any paste left inside, yet they would not let me fly with it because it was a larger almost-empty container than was allowed. You can figure out for yourself how effective a procedure this is.

Do you believe that if airports used basic training methods they could cut down on security technology?
No. The right technology with the right training can do the job. I know one can drastically reduce the number of people and the cost of technology and have a much safer airport than [with] the current practice.

What kind of technology do you think is of no use?
Body scanners, for sure, and metal detectors and X-ray machines in their current form.

How much savings would replacing those with the techniques you advocate result in for a mid-sized airport?
I estimate 20-30% savings with over 300% more security

Rafi Sela
Managing Partner, AR Challenges Ltd., Kfar Vradim, Israel, and AR Challenges Inc., North Bethesda, Md.
Age: 63
Education: B.S. in mechanical engineering from Technion-Israel Institute of Technology in Haifa; MBA from the University of Washington in Seattle.
Background: Served 18 years in the Israel Defense Forces (IDF), led training and ordnance divisions for special operations technologies... Sela's work with AR includes strategic design of operations and security at Israel's Ben Gurion Airport.

March 16, 2010 4:35 PM

Avxo Said...

TSOWilliamReed wrote "*Yet we are exposed to hundreds of different low level radiation sources a day. The sun itself radiates the heck out of us every day. Electrical devices, power lines, radio signals, wireless router feeds surround us, cell phones, television sets, all sorts of things. The FDA isn't limiting or banning the use of any of these radiation sources and the scanner generates less radiation.*"

There's radiation and then there's radiation. You might want to educate yourself on the difference between ionizing and non-ionizing radiation.

March 16, 2010 5:04 PM

Blogger Bob Said...

Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.

http://ow.ly/1n0Vc

Thanks,

Blogger Bob
TSA Blog Team

March 17, 2010 7:19 AM

Anonymous Said...
Hi Bob,

Allison on the insulin pump again. Several acquaintances of mine and I have been told by the TSA at Miami, Washington Regan, SFO, and Atlanta that this is the new protocol they are following- that you must declare any attached medical device, and upon doing so they are required to hand search (I mean they will be pulling everything out of) your carryon. It has been told to me while in Atlanta- I typically do not declare it, but obviously would on the scanner, as I am fairly certain that is they can see me, they can see my pump, no? In Atlanta they saw my tubing poking out, which made me have to declare it.

My question is this- although that is not a posted rule on the TSA website, it is being told to TSA agents that this is, in fact, new protocol. By utilizing the (now) optional body scanner, I must declare the pump so they don't freak out, no? Upon doing so, I am allowing them to hand search my bag with no cause, correct?

I would like a direct answer- obviously I have read the TSA website on what is required for attached medical devices, however TSA agents are NOT following those rules.

Allison

March 17, 2010 7:58 AM

Blogger Bob Said...
Alison,

I just e-mailed the procedures department and I'll let you know when I hear something.

Thanks,

Blogger Bob
TSA Blog Team

March 17, 2010 8:18 AM

Jim Huggins Said...
Bob, you write:

Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.

If so ... then what's the point of having AIT at all? If I can always opt-out of an AIT scan, doesn't that make it easier for me to smuggle contraband through a checkpoint?

March 17, 2010 8:44 AM

Anonymous Said...

Blogger Bob said...

Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.

Your own agency seems to be fielding it as the primary, not secondary means of screening. Might be more than a little communication problem there Bob.

March 17, 2010 9:12 AM

RB Said...

Blogger Bob said...
Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.
http://ow.ly/1n0Vc

Thanks,

Blogger Bob
TSA Blog Team

March 17, 2010 7:19 AM

.....

And TSA is selling ocean front property in Kansas.

March 17, 2010 10:02 AM

Anonymous Said...

Blogger Bob said...
Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.
http://ow.ly/1n0Vc

Thanks,

Blogger Bob
TSA Blog Team

Yeah, until the next "game changer" gets onto a plane with a bomb. If these ever became mandatory the airlines would suffer the most. Since the economy is currently hanging on by a thread, I don't think the Fed would give any passengers a reason not to fly.....until the economy rebounds that is.

FYI: Hundreds of passengers filed complaints about the use of these scanners last year.

http://www.straitstimes.com/BreakingNews/World/Story/STIStory_503018.html

March 17, 2010 10:38 AM

RB Said...

http://www.reuters.com/article/idUSTRE62F4W020100316

U.S. air travelers complain about body scans

(Reuters) - "Hundreds of U.S. air travelers have lodged complaints over use of full-body security scanners in the past year, charging they violate personal privacy and may be harmful to their health, documents released on Tuesday showed."

The complaints ranged from concern about genitals being seen and the use of the devices on children, to anger over passengers not being told they could request a pat-down search instead and potential health worries from the scans.

""I was not given an option to use the whole body screening device. Neither was anyone else. **It appeared that everyone was being required to go through the devices, *even children*,"** said one complaint from an unidentified traveler who flew through the Tulsa airport in May 2009.""

March 17, 2010 11:29 AM

Ayn R. Key Said...

Bob,

Why backscatter instead of mmw?

March 17, 2010 1:13 PM

James Polk Said...

I do not believe these scanners pose any substantial risk to people flying. The chances of getting killed in a crash or by terrorist is probably greater than risk from the minute amounts of radiation emitted from these devices. I think the safety factor overrides the minute danger factor in this case.

March 17, 2010 2:22 PM

Anonymous Said...

Ayn, one word, Chertoff.

March 17, 2010 2:31 PM

Anonymous Said...

Bob you better speak to the FSD and spokeperson at ORD was quoted in the paper saying otherwise and get them to post a correction.

Do you mean optional like shoes and other items that are now mandatory? Due to past behavior and pattern of evidence im very skeptical

March 17, 2010 3:24 PM

RB Said...

Ayn R. Key said...
Bob,

Why backscatter instead of mmw?

March 17, 2010 1:13 PM

.....

Super Major Pregnant Pause.

March 17, 2010 4:30 PM

Anonymous Said...

I"m told that envelopes are available for mailing small items that cannot be carried onto the aircraft. However, these envelopes are not placed at the point where the items are refused, but at the entry to the airport, a considerable distance away. At the Sarasota Airport, I had to give up a small Red Cross pocket knife that I had been awarded for public service because, at age 81, I could not manage the trip back and forth while lugging my carry-on bag. Why victimize travelers in this way when it would be a simple matter to have the envelopes available where the item is refused.

March 17, 2010 5:45 PM

Anonymous Said...

Bob,

If TSA insists upon having the ability to leer at passengers' private parts to clear them through security while sitting in dark private booths (which sounds very much like a peep show to me), I'd like to know what it's doing about ensuring the safety and dignity of the flying public. Given recent revelations about some of the more nefarious TSOs out there-- ones who bring weapons to work, others who get arrested for sexual assaults-- I'd like to know what the TSA is doing to ensure that the public isn't victimized every time they fly.

Can you please comment on when TSA will start using psychological evaluations as a screening tool for its TSOs, and require periodic reinvestigations of this nature for all TSOs in their workforce? This is an honest and sincere question about a genuine issue of legitimate concern. The American public ought to have assurances that their government agent screeners aren't doing obscene things while fondling their naked images.

Thanks.

March 17, 2010 6:50 PM

LTSO With Answers Said...

Blogger Bob said...
Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.
http://ow.ly/1n0Vc

Thanks,

Blogger Bob
TSA Blog Team

March 17, 2010 7:19 AM
.....
RB said...
And TSA is selling ocean front property in Kansas.

Is the property under or over the rainbow RB?

March 17, 2010 9:46 PM

Franz Pichler Said...

As someone before asked i also want to know:
What steps is TSA taking to ensure every passenger asked to be strip-searched knows he or she can decline the strip-search?

March 18, 2010 8:21 AM

Anonymous Said...

According to a GAO report, by 2014 the WBI are to be the ***PRIMARY*** means of WEI detection at airports.

Bob, someone's feeding you incorrect information.

http://homeland.house.gov/Hearings/index.asp?ID=242

March 18, 2010 10:11 AM

Anonymous Said...

If there are no moral or ethical issues with WBI equipment why won't TSA come clean on the images these devices make and post full size, full resolution images as seen by the operators?

It's been over a year, TSA has not posted such images.

March 18, 2010 11:05 AM

Shelby Said...

I disagree with some of the previous comments, I think the TSA has our best interests in mind. There's a fine line that has to be walked between "personal security" and "personal space". The two go hand in hand, and when you are in a situation such as mass transit at 30,000 feet, you've

got to bend a little and realize that you are not going to have as much privacy as you would on your couch at home.

I would much rather subject myself to high levels of security screening, so long as it means I have the peace of mind knowing that everyone else around me has also gone through those high levels of security screenings.

And the fact that the TSA is investing money to make these technologies less invasive is another great sign.

March 18, 2010 12:17 PM

Becka Said...

i think that no matter what the TSA does to help protect us there will be people who complain. these scans & other security precautions are necessary to protect us & if you are not guilt then you have no reason to worry. if you are worried about the radiation then feel free to take a bus or use your own vehicle. i for one am grateful the TSA is continuing to advance their technology because i can promise you that the terrorists are doing the same & we need to protect ourselves.

March 18, 2010 12:25 PM

Blogger Bob Said...

Anonymous said... According to a GAO report, by 2014 the WBI are to be the PRIMARY means of WEI detection at airports. Bob, someone's feeding you incorrect information.
http://homeland.house.gov/Hearings/index.asp?ID=242 March 18, 2010 10:11 AM

I can see how the word "primary" would lead you to that assumption, but it doesn't mean what you think it means.

Primary means it will be used as the primary means of screening, rather than just being used to resolve metal alarms. (secondary)

Even though it will be the primary means of screening, passengers will still be able to opt out and receive a pat down instead.

Thanks,

Blogger Bob
TSA Blog Team

March 19, 2010 10:25 AM

Anonymous Said...

becka spewed

i think that no matter what the TSA does to help protect us there will be people who complain. these scans & other security precautions are necessary to protect us & if you are not guilt then you have no reason to

worry. if you are worried about the radiation then feel free to take a bus or use your own vehicle. i for one am grateful the TSA is continuing to advance their technology because i can promise you that the terrorists are doing the same & we need to protect ourselves.

Oh, but Becka, you do need to worry even if you are innocent because if you violate TSA's secret rules and regulations you will be held accountable even if you make an honest mistake.

As to the WBI/AIT the GAO has questions to if it would have detected the panty bomber's bomb.

As to radiation exposure, well, hope you never get cancer due to frequent low level radiation exposure.

March 19, 2010 10:27 AM

Anonymous Said...

Bob, please stop playing word games. Primary, in this case, means that the WBI/AIT will be used as the first means of screening. By default the WTMD will either get yanked out and quietly replaced by the WBI/AIT (sold to TSA by a firm Chertoff represents) or left to sit idle.

When you play word games, your credibility and that of your agency further deteriorates. Your agency, for a short while, had the trust of the American public, and by abusing that trust, TSA has lost much of the support it once had due to bad publicity, thefts, abuse of passengers, rogue TSOs, rogue TSIs, etc.

March 19, 2010 10:34 AM

Anonymous Said...

"Even though it will be the primary means of screening, passengers will still be able to opt out and receive a pat down instead. "

And what steps is TSA taking to ensure that every passenger knows they can opt out of being strip-searched, Bob? For, it looks like, at least the third time on this thread?

March 19, 2010 10:49 AM

RB Said...

Blogger Bob said...
Anonymous said... According to a GAO report, by 2014 the WBI are to be the PRIMARY means of WEI detection at airports. Bob, someone's feeding you incorrect information.
http://homeland.house.gov/Hearings/index.asp?ID=242 March 18, 2010 10:11 AM

I can see how the word "primary" would lead you to that assumption, but it doesn't mean what you think it means.

Primary means it will be used as the primary means of screening, rather

than just being used to resolve metal alarms. (secondary)

Even though it will be the primary means of screening, passengers will still be able to opt out and receive a pat down instead.

Thanks,

Blogger Bob
TSA Blog Team

March 19, 2010 10:25 AM

.....
Bob, are you more in the loop on future policy than a FSD?

Are you speaking for TSA when you say WBI will not be required in the future?

March 19, 2010 10:52 AM

Jim Huggins Said...
Bob writes:

Primary means it will be used as the primary means of screening, rather than just being used to resolve metal alarms. (secondary)

Even though it will be the primary means of screening, passengers will still be able to opt out and receive a pat down instead.

So, in fact, many of us have been correct all along. TSA is planning on a massive expansion of screening procedures.

Today, I can walk through a checkpoint with my privacy relatively intact. In five years, I'll either have to let a stranger view my naked body on a screen, or "request" that another stranger pat me down. (And, if present reports are any indication, any such "request" will be met with plenty of opposition and questioning at the checkpoint as well.)

March 19, 2010 10:52 AM

RB Said...
Blogger Bob said...
Anonymous said... According to a GAO report, by 2014 the WBI are to be the PRIMARY means of WEI detection at airports. Bob, someone's feeding you incorrect information.
http://homeland.house.gov/Hearings/index.asp?ID=242 March 18, 2010 10:11 AM

I can see how the word "primary" would lead you to that assumption, but it doesn't mean what you think it means.

Primary means it will be used as the primary means of screening, rather than just being used to resolve metal alarms. (secondary)

Even though it will be the primary means of screening, passengers will still be able to opt out and receive a pat down instead.

Thanks,

Blogger Bob
TSA Blog Team

March 19, 2010 10:25 AM

.....
So what did they say>

March 19, 2010 10:56 AM

Blogger Bob Said...

RB said... Bob, are you more in the loop on future policy than a FSD? Are you speaking for TSA when you say WBI will not be required in the future? March 19, 2010 10:52AM

RB, I'll repeat what I wrote earlier:

Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.
http://ow.ly/1n0Vc

Thanks,

Blogger Bob
TSA Blog Team

March 19, 2010 11:02 AM

Ayn R. Key Said...

So, Bob, I've been asking why the TSA favors unsafe Backscatter instead of safe MMW. Is the reason because Chertoff represents the firm that manufactures unsafe Backscatter?

March 19, 2010 11:02 AM

Sandra Said...

Do any of those of you who unequivocally support WBI to make you feel safe **EVER** stop to think about the much higher risk of death you face while driving to the airport than you face from terrorism-related death when getting on an airplane?

If you **STOPPED TO THINK** and put things in perspective, you'd probably never leave your house because you'd be so frightened about dying in your car.

We have become a nation of absolute cowards.

March 19, 2010 12:05 PM

Avxo Said...

becka said: *"these scans & other security precautions are necessary to protect us & if you are not guilt then you have no reason to worry"*

Wow... is this what passes for an American these days?

March 19, 2010 12:34 PM

RB Said...

RB, I'll repeat what I wrote earlier:

Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.
http://ow.ly/1n0Vc

Thanks,

Blogger Bob
TSA Blog Team

March 19, 2010 11:02 AM

.....

So what is it, TSA's Federal Security Directors are being misinformed or they are acting on their on to mis-inform the public?

Seems like a sloppy way to run an organization but since TSA can't even get a simple Shoes in the Bins/Shoes on the Belts policy implemented correctly I am not surprised.

Which bring up the very valid reason why travelers require detailed guidelines of what requirements they must comply with to transit a TSA Drag Net Checkpoint.

Also, where is the policy available for public viewing that allows ice through the checkpoint for everyone, not just one Hollywood Semi-Celeb or people with medical/health concerns?

March 19, 2010 12:45 PM

Anonymous Said...

Ayn R. Key said...

Bob,

Why backscatter instead of mmw?

My guess is that with backscatter they will eventually modify the scanners to increase the level of radiation emitted to actually penetrate

through the body and essentially perform a cavity search.

Or it could be plain old misdirection. By getting everyone to focus on the "tiny" but cumulative radiation risks with backscatter they can then pull the switcheroo and plug in the MMW scanners. Thus by trying to lower American passengers "reasonable expectaion of privacy" with the initial implementation of the backscatter scanners the TSA can then say "see we replaced the harmful X-ray scanners with harmless MMW scanners. We do care about your safety".

March 19, 2010 1:27 PM

Robert Johnson Said...

Bob, if you're saying there are no plans to make WBI mandatory, that leaves the door wide open to change in the future.

Becka, please read Daniel Solove's 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. Please click on one-click download to get to the PDF.

I may not have anything to hide and may not be guilty of anything, but it also does not mean it's any of their business.

If a policeman came to your house and asked to do a search of your house for illegal drugs, weapons, and other contraband, would you let them in? Under the constitution, you don't have to even if you have nothing to hide.

Do share intimate details, your financials, and other sensitive and personal information with others when they ask? If you have nothing to hide and aren't guilty, then you have no grounds to object by your logic.

Robert

March 19, 2010 2:55 PM

Anonymous Said...

Ok, I will ask one more time but this time I will be a little more direct. This is Danny, a BDO with TSA. I have put out this challenge at least twice on different blog posts here. AVXO, RB, Ayn R. Key, Jim Huggins, and all of the others who belittle every TSA Officer, yes that is part of our title; and call us names and tell me what I am, at least according to you. Where do you work? What company do you work for?? What do you do for a living? Are you in a profession that is not in trouble? Are you a school teacher, cop, banker, mortgage business, etc, tell me what you do. Lets see what kind of work you do. I will be more then happy to answer your questions, if I can. You may not belief me, or like the answers but I will do my best. But tell me what you do, I did. See if you live in a glass house. Go ahead through a stone my way, but I may throw stones back at you.

March 19, 2010 4:22 PM

HappyToHelp Said...

RB said...
"Also, where is the policy available for public viewing that allows ice through the checkpoint for everyone, not just one Hollywood Semi-Celeb or people with medical/health concerns?"

311 for carry-ons
"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Tim
TSA Blog Team

March 19, 2010 4:23 PM

Anonymous Said...
I like the word games in the MMW description at the top of the blog:
...TSA is not the first to use this technology. It's currently being used in Canadian airports.....

The only reason the scanners are being used in Canadian airports is because the TSA asked the airports to install them after the underwear bomber. Yet another misleading blurb to try and side track the uninformed masses.

Until I am permitted to view my own image produced by these machines I will never even consider submitting to one.

March 19, 2010 6:14 PM

Anonymous Said...
If you STOPPED TO THINK and put things in perspective, you'd probably never leave your house because you'd be so frightened about dying in your car.

Theres a difference though in actually driving a car and flying on a plane with 180 other people. In a car, I am in control of defensive maneuvering in avoiding collisions. That is of course if I'm paying very close attention the the road and the drivers around me, which i do. In an airplane, I have no control whatsoever. Theres nothing i can do to avoid a crash/explosion on a plane.

What are you going to do if someone with a bomb gets on a plane? Because if there was no TSA this would become a reality. I guess you're willing to take the chance of someone blowing up a plane because it would only happen once. I'm not willing to take that chance. Brand me a coward then, but i will not die onboard of a plane as part of a terrorist attack tyvm.

March 19, 2010 9:38 PM

Anonymous Said...
I get so sick and tired of hearing people complain about this and that.

This stuff is here for our safety people!!! If it wasnt here, and it was YOUR plane that exploded in the sky, some of you would be complaining that they didnt have the machines. Did all of you forget 9/11? How about Richard Reid? Abdulmuttalab? The terrorists are still trying to get to us. They are changing their tactics daily so the TSA has to do the same. Get over it! I'd take any security precaution the government comes up with if it means that no more of my fellow innocent Americans have to die. By all means though, if any of you feel they need to die so you can get through security quicker...continue writing your blogs

March 20, 2010 10:23 AM

Anonymous Said...

Robert Johnson said

If a policeman came to your house and asked to do a search of your house for illegal drugs, weapons, and other contraband, would you let them in? Under the constitution, you don't have to even if you have nothing to hide.

Robert, that's a poor example. There is a difference between implied consent and the 4th amendment. When you enter certain parts of the airport you are giving your consent to search of your person and property. In your own home there is no implied consent. So you just simply tell the police officer to get a warrant.

4th amendment Implied consent two different things.

March 20, 2010 6:43 PM

Isaac Newton Said...

Blogger Bob said:

Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate. http://ow.ly/1n0Vc

Sure Bob.

After all, you said (April 15 2008) that the images were suitable for the cover of Reader's Digest, yet you haven't released full-resolution images.

And you said that the machine couldn't store the images at all, until you had to admit that it COULD but it WOULDN'T because, well, we're still waiting to hear how you ensure that.

And your former boss Kip said authoritatively that the liquid restrictions would be relaxed (no size limit, liquids in bin) by Fall 2009 and gone completely by the end of 2010.

And your agency keeps weaseling out of the deadline to screen 100% cargo.

So when you say these machines are completely safe and that they

won't become mandatory, why should we believe you again??

March 22, 2010 2:19 AM

Anonymous Said...

"Bob, how did Bill's abusive and threatening (post) get posted?"

Probably the same way the post on Feb 16th insulting the Amish got posted.

The moderator approved it.

March 22, 2010 11:13 AM

Robert Johnson Said...

Anonymous:

Just because implied consent may exist doesn't mean that implied consent exists for everything at a checkpoint.

Implied consent was based in court cases based on a very narrow and limited administrative search, NOT the ever expanding searches TSA employs.

Robert

March 22, 2010 1:56 PM

Robert Johnson Said...

Quote from Anonymous: "I get so sick and tired of hearing people complain about this and that. This stuff is here for our safety people!!! If it wasnt here, and it was YOUR plane that exploded in the sky, some of you would be complaining that they didnt have the machines. Did all of you forget 9/11? How about Richard Reid? Abdulmuttalab? The terrorists are still trying to get to us. They are changing their tactics daily so the TSA has to do the same. Get over it! I'd take any security precaution the government comes up with if it means that no more of my fellow innocent Americans have to die. By all means though, if any of you feel they need to die so you can get through security quicker...continue writing your blogs"

So you'd be willing to give up what it means to be an American and the freedoms that it comes with simply to be safe? Wow. Move to North Korea. There's little crime and terrorism there.

Terrorism is a threat, but not enough to be afraid of. You are 20 TIMES more likely to be struck by lighting over the last 10 years (1 in 500,000) vs. dying in a terrorist incident on a plane (1 in over 10,000,000 - yes, that's MILLION). Are you scared of getting struck by lightning? No? Then why are you more afraid of terrorism and willing to give up your freedoms for something 20 times less likely?

Terrorism is a tactic. Blowing up planes is a tactic. The real aim is to create fear and to get people to change how they live because of that

fear. Congratulations, you are giving the terrorists what they want and letting them win.

Robert

March 22, 2010 2:02 PM

Anonymous Said...

To Allison with the insulin pump:
Don't hold your breath waiting for an answer. This exact issue was posted about last April under the "Traveling 101 for Diabetics" thread and was never responded to. I think you only got a response because you posted on a very active, current thread. I hope you get an answer. I'd like to know why wearing an insulin pump gets such extra scrutiny!

March 22, 2010 2:10 PM

Robert Johnson Said...

Quote from Anonymous: "Theres a difference though in actually driving a car and flying on a plane with 180 other people. In a car, I am in control of defensive maneuvering in avoiding collisions. That is of course if I'm paying very close attention the the road and the drivers around me, which i do. In an airplane, I have no control whatsoever. Theres nothing i can do to avoid a crash/explosion on a plane."

Guess what? You might be able to control your car, but you can't control the other idiots out there driving. You can't always avoid see what's happening around you.

An example. This past Saturday night, I was in an SUV with my family on a freeway. Some idiot decided to change lanes without looking and slammed into us. My mother happened to be driving, has been a good driver for years and hasn't even been involved in an accident for over 10 years. We had no control over the idiot slamming into us. We were very fortunate that we didn't have a bigger accident and roll over on the freeway.

We had no control over that other guy.

"What are you going to do if some one with a bomb gets on a plane? Because if there was no TSA this would become a reality. I guess you're willing to take the chance of someone blowing up a plane because it would only happen once. I'm not willing to take that chance. Brand me a coward then, but i will not die onboard of a plane as part of a terrorist attack tyvm.

Funny, before TSA came about bombs weren't getting on planes with any regularity. So it appears that that statement is false.

Another funny thing is in the underwear bomber incident, AMS security was the same security that TSA implements and requires to be implemented for a plane bound to the US. Guess what? It FAILED. And even with the latest nude-o-scopes, there was only a 60% chance that it

would have detected the underwear bomb. And TSA's detection rate has been abysmal for years - we're quite fortunate that a bomb hasn't gone off. Maybe it's because the threat is way overstated?

Don't buy into the fear that TSA propagates.

Robert

March 22, 2010 2:10 PM

Avxo Said...

Danny, the BDA TSO, wrote: *"AVXO [...] who belittle every TSA Officer, yes that is part of our title; and call us names and tell me what I am, at least according to you."*

If you're going to call someone out by name, at least get your facts straight and don't accuse people for no reason. It is possible to have disagreements or differences of opinion and remain respectful, and if you bothered to actually read my posts you would see that I have belittled nobody, and have been nothing but respectful to everyone on here.

Danny then continued: *"Where do you work? What company do you work for?? What do you do for a living?"*

Perhaps that would be relevant if I maintained a blog, such as this one, soliciting public input on my job and my performance at it.

Danny then continued: *"Lets see what kind of work you do. I will be more then happy to answer your questions, if I can. You may not belief me, or like the answers but I will do my best. But tell me what you do, I did."*

What I do is irrelevant. This blog solicits input from the public, without regard for what those members of the public do for a living.

Danny droned on some more: *"See if you live in a glass house. Go ahead through a stone my way, but I may throw stones back at you."*

Ah, I see. So your problem is that you don't like criticism...

March 22, 2010 3:29 PM

AngryMiller Said...

Ok, I will ask one more time but this time I will be a little more direct. This is Danny, a BDO with TSA. I have put out this challenge at least twice on different blog posts here. AVXO, RB, Ayn R. Key, Jim Huggins, and all of the others who belittle every TSA Officer, yes that is part of our title; and call us names and tell me what I am, at least according to you. Where do you work? What company do you work for?? What do you do for a living? Are you in a profession that is not in trouble? Are you a school teacher, cop, banker, mortgage business, etc, tell me what you

do. Lets see what kind of work you do. I will be more then happy to answer your questions, if I can. You may not belief me, or like the answers but I will do my best. But tell me what you do, I did. See if you live in a glass house. Go ahead through a stone my way, but I may throw stones back at you.

Field service here Danny boy. I deal with some of your cow-orkers on an at least twice a week and found the majority of them okay. When passing through a checkpoint, at least here in the US, I am more surprised by the rarity of professionalism on the part of TSOs than I am of the rude, incompetent TSOs which sadly is the rule rather than exception. Please explain why that is.

I demand professionalism on the part of all TSOs. I demand that they know their SOP better than I do (from just having been on the receiving end of it so many times). Often that isn't the case. I demand that if a TSO doesn't know something that he/she will either go look it up (I'll wait) or get someone who does know the SOP instead of making up something on the spot and expect me to believe a word of it. Honesty is the only policy. Never lie to anyone as they may actually know what it is they are discussing with you better than you do.

You want respect. Respect is earned. While passengers would like to be shown some respect on the part of those who would make air travel safer for us, we would be willing to just have some common courtesy and not be regarded as an unidicted terrorist. Treat us like an unindicted terrorist and we WILL treat you shabbily in return. It works both ways.

March 22, 2010 3:59 PM

Ryan62 Said...

Robert,
Can I get a source, preferably a peer reviewed study, indicating that with the use of AIT there would only be a 60% chance of finding the device the Christmas Day bomber had.
Further, if Amsterdam used the same screening and TSA and it failed, that is a reason to add things like the AIT, rather than shove your head back under the sand.
As for bombs getting onto planes with any regularity prior to TSA, well at least one a year from 1964-1989 with the exception of 1977, and 11 more from 1990-2009. You can quible about what "fairly regularly" means all you want.

March 22, 2010 4:01 PM

Jim Huggins Said...

Danny the BDO writes:

AVXO, RB, Ayn R. Key, Jim Huggins, and all of the others who belittle every TSA Officer, yes that is part of our title; and call us names and tell me what I am, at least according to you. Where do you work?

First of all, I have not belittled "every TSA Officer". I have never called anyone names here. I criticize policies and procedures, not people. And,

over the course of this blog, I've defended TSA as much as I've criticized them.

Second, I don't know why I should tell you where I work, when you didn't tell me where you work. Let's play fair. Where do you work?

Third ... that little link up there by my name will lead you (eventually) to all the information you'd want to know about me. And, by the way, my job does subject me to public scrutiny, and there are plenty of websites out there that discuss my job performance --- good, bad, and ugly. I'm not hiding.

March 22, 2010 4:04 PM

Ryan62 Said...

Robert,
Just because someone advocates for security doesn't mean they are "scared". It means they see something as a reasonable precaution. Wearing your seatbelt in a car can be annoying and uncomfortable. I don't wear it because I am afraid of crashing. I wear it because I see it as a reasonable precaution.
Locking the doors in my house can be inconvienent, and the odds of my home actually being broken into are small, yet I still lock them. Not because I am "buying into the fear" that someone propogates, but rather because I think it is a reasonable precaution.
Now, you are certainly welcome to disagree and we can discuss what are reasonable and unreasonable precautions. But you have no right to assume that everyone who supports more stringent security than you do only does so out of some misguided fear.

March 22, 2010 4:10 PM

Anonymous Said...

When will the TSA be posting unaltered full size, full resolution sample images produced by the latest generation scanners?

March 22, 2010 4:43 PM

Anonymous Said...

If the scanners are such a benefit to security, why were they not installed in any NY airports? I thought NYC was still a prime target for terrorists? Is the TSA stalling the introduction of them in NY with hopes that there will be another attack, and then it will be easier to sell the concept of a strip search to the many liberal new yorkers who won't submit to this invasion of privacy? After all if the screener can't see you...you must not be naked....that is some sound logic.

Keep up the fear mongering guys.... there are still lots of parents who won't let you guys ogle their naked children yet. But you almost have them!!!!

March 22, 2010 4:59 PM

Anonymous Said...

Who in the airport has the clearance to disable the backscatter body algorithm or any of the other privacy settings?

When does the TSA plan to start telling us they need to start saving naked images of passengers with no privacy settings applied just until their plane lands safely, of course? Or does the saving of images fall under a national security exemption in which they don't need to inform us?

March 22, 2010 5:10 PM

Anonymous Said...

"if it was YOUR plane that exploded in the sky, some of you would be complaining that..."

You know, I think if their plane exploded in the sky you would not hear them complain. Not this side of the grave.

March 22, 2010 6:52 PM

Jim Huggins Said...

RB asked:

"Also, where is the policy available for public viewing that allows ice through the checkpoint for everyone, not just one Hollywood Semi-Celeb or people with medical/health concerns?"

HappyToHelp quoted the 311 for carry-ons page:

"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

HappyToHelp: the only problem with the quote above is that it comes in the middle of a section describing exceptions **for medical needs only**. The paragraph immediately above the one you quoted says (emphasis added by me):

***To ensure the health and welfare of certain air travelers**, in the absence of suspicious activity or items, greater than 3.4 ounce (100ml) of the following liquids, gels and aerosols are permitted through the security checkpoint in reasonable quantities for the duration of your itinerary (all exceptions must be presented to the security officer in front of the checkpoint):*

A reasonable reading of the web page would seem to suggest that ice isn't permitted for ordinary travelers who don't have a medical need for it. This would seem to contradict the Britney Spears rule, since she didn't have a medical need.

Numerous requests for clarification on this point have gone unanswered. Would you -- or anyone else at TSA -- like to comment on this discrepancy?

March 22, 2010 9:39 PM

Anonymous Said...

Looks like the TSA is lying about the scanners remaining optional. Did Obama pass health care to cover the tens of thousands new cases of cancer that the rampant use of these scanners will result in? Given the choice i would rather be blown up in the air quickly than suffer an agonizing battle with cancer stretched out over many years. But thank God my job does not require me to fly. TSA already destroyed domestic tourism, now they have there eye on the aviation industry. On the bright side at least they are thinning out the heard of mindless sheep in this country, so eventually logical thinkers will be able to reclaim it.

http://www.computerworld.com/s/article/9173881/TSA_plans_to_double_its_use_of_whole_body_scanners

March 22, 2010 10:46 PM

Anonymous Said...

America has absolutely no chance. Watch the video from the link.

http://www.nbclosangeles.com/news/local-beat/TSA__How_Safe_Is_It_to_Fly__Los_Angeles.html

March 22, 2010 10:57 PM

Paxton Said...

I have a question: Will these machines ever come down? It seems like we are in an war with terrorism that will never end. We have to live in a perpetual police state where we each feel like suspects rather than citizens.

I would be SHOCKED if this "war on terror" ends and we can lessen security. I pray there will be a day.

March 23, 2010 7:03 AM

Ryan62 Said...

Anon -
Care to explain how TSA "destroyed the domestic tourism industry"? I think the recession did that, and it wasn't caused by TSA?
I invite you to look at the actual statistics
http://www.airlines.org/economics/traffic/Annual+US+Traffic.htm
rather than be a mindless sheep that repeats nonsense about how "no one flies because of TSA". Every year since TSA was created air travel has increased up until the start of the current recession. After the "War on Liquids" after "the shoe carnival" and all the rest air travel kept going up.
So it would seem a self proclaimed "logical thinker" wouldn't be able to make much of a case that TSA has destroyed tourism or aviation.

March 23, 2010 11:32 AM

Ayn R. Key Said...

Danny the BDO,

Either you missed when I answered your question the last time or you ignored it. Either way it's rather unprofessional of you to call me out and then fail to notice when I respond.

I am an electrical engineer. I got my start working on communications equipment. Everything I've written about x-rays versus millimeter is written as a professional.

As much as I think the TSA should not exist, the issue of x-rays versus millimeter waves goes far, FAR beyond that. It goes down to basic public health and safety issues that they drilled into our heads the first year of college. It goes to my semi-annual safety refresher briefings. It goes to my viewing myself as a scientist and thus wanting to see scientific accuracy in this blog.

Since you are a BDO instead of an engineer, and since you are so in love with titles and credentials instead of with actual competence since seeing a title enables you to forgo independent analysis of the capability of the individual, then I have the credentials you lack when discussing this issue. However if by some chance you decide to go by competence while reading this comment then I also have that over you.

When it comes to mmw versus xrb I have both credentials and competence over just about everyone in the TSA, and I'm far from being the very best of electrical engineers. I'm probably average, but still that puts me far ahead of any mere BDO.

March 23, 2010 12:30 PM

Robert Johnson Said...

And Ryan62, just because I don't support the current security measures and even more, doesn't mean I don't advocate security at all. That's also patently false. Did you not just do what you accused me of?

But hey, the guy said he was afraid. Am I not to take him at his word?

Robert

March 23, 2010 1:46 PM

Robert Johnson Said...

Ryan62,

Here's a link to my source.

http://news.bbc.co.uk/2/hi/8441205.stm

"Mr Johnson also told the Commons there was only a 50 to 60% chance that a body scanner would have detected bomb materials allegedly carried by Mr Abdulmutallab.

He said such machines were not a "magic bullet"."

Believe, don't believe it, it's up to you.

Of course, he's right that these aren't a magic bullet. But that's exactly what these are being touted as.

The The GAO also stated:

"Second, as we reported in October 2009, TSA does not know whether its explosives detection technologies, such as the AITs, are susceptible to terrorist tactics. Although TSA has obtained information on vulnerabilities at the screening checkpoint, the agency has not assessed vulnerabilities—that is, weaknesses in the system that terrorists could exploit in order to carry out an attack—related to passenger screening technologies, such as AITs, that are currently deployed. 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, where he concealed an explosive in his underwear. However, TSA has not assessed whether these and other tactics that terrorists could use to evade detection by screening technologies, such as AIT, increase the likelihood that the screening equipment would not detect the hidden weapons or explosives. Thus, without an assessment of the vulnerabilities of checkpoint technologies, it is unclear whether the AIT or other technologies would have been able to detect the weapon Mr. Abdulmutallab used in his attempted attack."

Tests by Qinetiq, a manufacturer of these devices in the UK, have shown that "Tests by scientists in the team at Qinetiq, showed the millimetre-wave scanners picked up shrapnel and heavy wax and metal, but plastic, chemicals and liquids were missed."

There's also the fact that if, by TSA's admission, that these devices are designed NOT to penetrate the skin, devices hidden in body cavities, in fat folds, and under large breasts would not be detected.

Something invasive and not effective isn't a way to detect the bombs.

Funny thing is, we've had the puffers for how long? But instead of going back and fixing them to work in an airport environment, which should be doable, let's do something that hasn't been proven to be effective.

Also, A UN human rights expert says that the use of full body scanners at airports following the Christmas day terrorist attempt was more of a political response than a carefully designed security measure .

But hey, Chertoff said we need these things. And of course, he has nothing to gain considering he represents RapiScan.

And also, btw, the fear thing was in another thread - I confused the two but it's hard to know if the 2 anons are the same.

Robert

March 23, 2010 2:43 PM

Anonymous Said...

UK screener uses AIT to ogle a female co-worker. Thank god this could never happen in the U.S. LOL

http://www.dailymail.co.uk/news/article-1260222/Heathrow-security-worker-quizzed-naked-body-scan-colleague.html?ITO=1490

March 24, 2010 9:09 AM

Anonymous Said...

Granted, this isn't the TSA, but does **anyone** doubt similar scenarios would play out here?

BAA is investigating an incident in which a Heathrow security operative "ogled" a female colleague who'd wandered into a body scanner, the Sun reports.

John Laker, 25, allegedly copped an eyeful of Jo Margetson, 29, when the latter "entered the X-ray machine by mistake". She was "horrified" as Laker "pressed a button to take a revealing photo" and remarked: "I love those gigantic tits."

March 24, 2010 1:45 PM

Anonymous Said...

Terrorism is a tactic. Blowing up planes is a tactic. The real aim is to create fear and to get people to change how they live because of that fear.

Nope. Incorrect. Terrorists want to KILL the infidels (you and me), not scare them. Maybe thats why you dont understand what were up against rob. But hey, when you make your next trip to candyland, since you seem to live there, can i get some of the giant red licorice? its my favorite.

March 24, 2010 2:53 PM

Anonymous Said...

Can anybody confirm if you can refuse to pass by the backscatter scanner if you're pregnant?
Can you "chose" the pat-down instead?

Thank you very much for your time.
Sebastian.

March 25, 2010 12:33 AM

Anonymous Said...

I have sent multiple emails to TSA-ContactCenter@dhs.gov and they keep responding with the same "AIT is incapable of storage" rhetoric. My question is not about AIT machine storage it is regarding external USB media storage such as USB

flash drives. So i will ask you bloggers:

Is it at all possible in any mode to store a passengers scanned image to a USB flash drive or external hard drive connected via a USB port? Also are the TSA screeners allowed to bring USB drives or external storage devices into the viewing room with them?

Please don't respond with the same AIT storage rhetoric. If anything say you cannot comment about this. thanks.

March 25, 2010 7:28 PM

Anonymous Said...

More privacy invasions by TSA via your phones bluetooth:

TSA considers Bluetooth to track security checkpoint wait times

http://www.geek.com/articles/mobile/tsa-considers-bluetooth-to-track-security-checkpoint-wait-times-20100324/

March 25, 2010 7:37 PM

TSM/West Said...

ANON Said

Can anybody confirm if you can refuse to pass by the backscatter scanner if you're pregnant?
Can you "chose" the pat-down instead?

Thank you very much for your time.
Sebastian.

March 25, 2010 12:33 AM

Yes you can.

March 25, 2010 9:49 PM

Robert Johnson Said...

Quote from an Anon: *"Nope. Incorrect. Terrorists want to KILL the infidels (you and me), not scare them. Maybe thats why you dont understand what were up against rob. But hey, when you make your next trip to candyland, since you seem to live there, can i get some of the giant red licorice? its my favorite."*

Ah, so you really have nothing to say, so you try to insult me by comparing my philosophy to candyland? Classy, Anon.

At any rate, there's more than just killing infidels, anon. Otherwise, we'd have jihad going on worldwide. Funny how you don't see Al Qaida targeting places like say India, China, etc. You know, places that aren't Muslim and has MANY, MANY more infidels than the US.

No, they want to take the US down. They'd be quite content to see us

not be free and live under sharia law. They despise what we stand for, and who we associate with (in particular, Israel). Even last year during the German elections, Al Qaida was threatening Germany if Angela Merckel was re-elected? Why? She had fairly close ties with the US and was a partner to the US in many ways.

Osama knows that he can never kill all of us infidels, even if he'd love to. So how do you take the "great Satan down?" Fear. Crash a few planes into some buildings. Send some idiots in like Reid and the underwear bomber. Osama learned with the liquid bomb plot that he didn't have to succeed to succeed - he can send in some clowns that will fail and still send the US into a panic.

Planes aren't the only things that can be targeted. Shopping malls, schools, stadiums, etc - any of them can be targeted to cause mass havoc. He doesn't need aviation to do that.

He knows his best chance to take down the "great Satan" is to get us to implode. Get us to give up freedom because of fear. Get us to do stupid things because we're afraid. Change us over years.

If anything, we know from his attacks that Osama is very patient. Getting America to implode isn't an overnight job, but he's accomplishing it piece by piece.

As Abraham Lincoln said "America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves." And that's exactly what he's getting us to do, Anon, is to destroy ourselves. Threatening planes is just one of many tactics to do that.

You don't understand that Anon. I'd seriously think about it.

Robert

March 25, 2010 10:37 PM

RB Said...

HappyToHelp said...
RB said...
"Also, where is the policy available for public viewing that allows ice through the checkpoint for everyone, not just one Hollywood Semi-Celeb or people with medical/health concerns?"

311 for carry-ons
"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Tim
TSA Blog Team

March 19, 2010 4:23 PM

.....
As has already been pointed out that section deals with people with medical issues or people with special needs, not the general public.

Want to try again Tim?

March 26, 2010 10:18 AM

RB Said...

Blogger Bob said...
RB said... Bob, are you more in the loop on future policy than a FSD? Are you speaking for TSA when you say WBI will not be required in the future? March 19, 2010 10:52AM

RB, I'll repeat what I wrote earlier:

Imaging technology is always optional and there are no plans to make it mandatory. Anything else you hear or read is inaccurate.
http://ow.ly/1n0Vc

Thanks,

Blogger Bob
TSA Blog Team

March 19, 2010 11:02 AM
.....
And I will repeat the question since you seem to not have responded directly; Are you more in the loop that a FSD at a major airport?

Your basically calling the FSD a liar Bob.

March 26, 2010 10:22 AM

RB Said...

Anonymous said...
Ok, I will ask one more time but this time I will be a little more direct. This is Danny, a BDO with TSA. I have put out this challenge at least twice on different blog posts here. AVXO, RB, Ayn R. Key, Jim Huggins, and all of the others who belittle every TSA Officer, yes that is part of our title; and call us names and tell me what I am, at least according to you. Where do you work? What company do you work for?? What do you do for a living? Are you in a profession that is not in trouble? Are you a school teacher, cop, banker, mortgage business, etc, tell me what you do. Lets see what kind of work you do. I will be more then happy to answer your questions, if I can. You may not belief me, or like the answers but I will do my best. But tell me what you do, I did. See if you live in a glass house. Go ahead through a stone my way, but I may throw stones back at you.

March 19, 2010 4:22 PM
.....

Danny, I am a United States citizen. I have every right to expect my government to act within the bounds of the United States Constitution. I believe that TSA has not done so. As a citizen I have a responsibility to question my government when they step out of bounds which your agency does on a regular basis.

My name is Ron. I am retired military. I currently work in the banking industry and my company is very strong. I live in the DFW area.

Happy now?

March 26, 2010 10:31 AM

Ranger11 Said...

This argument just goes back and forth. I have spent my whole adult life fighting the war on terror. I am retired military and now work with DHS/TSA. If I thought for one second that the idea behind terrorism was just to scare, I would be dead.

Being scared is the result of the damage inflicted by the terrorists. It is a side affect of the terrorist activity. People die in a horrific, unforeseen event that shocks and surprises the victims and all those who come in contact with the events aftermath. That is what scares people.

The purpose of the attack is to cause devastation and make us aware that we are vulnerable to the attack itself. If that scares us, then so be it. The intent is to destroy and kill, not to scare. Terrorism is the act of violence with the intent to do harm, especially bombing, kidnapping, and assassination, carried out for political purposes (in most cases).

Again, the fact that it scares us, is a side affect. If they only meant to scare us, we would have many more people walking this earth today.

March 26, 2010 11:06 AM

LTSO With Answers Said...

AngryMiller said... *When passing through a checkpoint, at least here in the US, I am more surprised by the rarity of professionalism on the part of TSOs than I am of the rude, incompetent TSOs which sadly is the rule rather than exception. Please explain why that is.*

AngryMiller I must say that from airport to airport I see the same thing when I travel. I believe it is because of the leadership at that airport or checkpoint. They still get the job done though just not in the friendly aspect that the public demands.

March 26, 2010 1:34 PM

Anonymous Said...

From Danny BDO

I retired as a telephony design engineer. I asked the questions that I did, mainly because of the fact, btw you did not say were you worked and what company, but that is beside the point. You took one thing and made it about me, and even had to say that I was unprofessional

because I mentioned you by name, along with everyone else that takes shots at TSA. I have a degree, in fact I am working on a Masters Degree. I made a point of asking what I asked because of everyone taking shots at a TSA employee, and painting everyone based on a few examples, that for most of the TSA work force believe that they do not paint all of us in the same way. We deal with some passengers that are horrible, they are rude, but we do not paint every passenger the same. The behavior that some of the people, and no I am not saying you, but for the most part everyone who paints everyone the same way based on the actions of only a few, would or could we call them a racist if we were talking about a race? You would not say that and most people would not, but yet when you and the others take shots at TSA as a whole against the Officers, well that is wrong on your part, and wrong on anyone elses part period. We are here to job that is presented for us to do. We do not make the rules, but we are asked to obey the rules and help others to try and follow the rules as well. Some do it better then others, the same as in any job. I am sure that you are great in your job, but do everyone at work act and behave the same way as you do? No, it simply is not possible. Last thing, you are the only one that I saw post anything, and yes I missed your response in the thread, sorry, I will go back and read it. Danny BDO

March 26, 2010 3:28 PM

GSOLTSO Said...

Sebastian, according to all the info and Bobs previous posts, passengers will be able to opt out of the AIT. If someone you know is pregnant and wishes to recieve alternative screening, they are welcome to do so, all they have to do is request it when they get to the checkpoint.

West
TSA Blog Team

March 26, 2010 5:47 PM

Ryan Thompson Said...

I think it's unnecessary to have these crazy scanners. It's just costing us money, time, and health issues we don't need.

If someone's going to bomb us, they're going to find a way.

March 29, 2010 1:09 AM

Blogger Bob Said...

RB said...Your basically calling the FSD a liar Bob. March 26, 2010 10:22 AM

Twist my words as you will, but I have said nothing of the sort. I believe I said "Anything else you hear or read is inaccurate."

Blogger Bob
TSA Blog Team

March 29, 2010 9:52 AM

Blogger Bob Said...

RB said... As has already been pointed out that section deals with people with medical issues or people with special needs, not the general public. March 26, 2010 10:18 AM

This is listed under both the main 3-1-1 page as an exception. It is also listed in the special needs page.

"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Main 3-1-1 Page

Special Needs Page

March 29, 2010 9:59 AM

Blogger Bob Said...

Anonymous said... Is it at all possible in any mode to store a passengers scanned image to a USB flash drive or external hard drive connected via a USB port? Also are the TSA screeners allowed to bring USB drives or external storage devices into the viewing room with them? March 25, 2010 7:28 PM

Images can only be saved in test mode. The machines are not placed in test mode while at the airport. Test mode is used in testing situations at laboratories and testing facilities.

Thanks,

Blogger Bob
TSA Blog Team

March 29, 2010 10:05 AM

Blogger Bob Said...

Anonymous said... Can anybody confirm if you can refuse to pass by the backscatter scanner if you're pregnant? Can you "chose" the pat-down instead? Thank you very much for your time.
Sebastian. March 25, 2010 12:33 AM

TSM West is correct. Additionally, anybody (pregnant or otherwise) can choose the pat-down as an alternative to the AIT machines.

Thanks,

Blogger Bob

TSA Blog Team

March 29, 2010 10:07 AM

RB Said...

Blogger Bob said...
RB said... As has already been pointed out that section deals with people with medical issues or people with special needs, not the general public.
March 26, 2010 10:18 AM

This is listed under both the main 3-1-1 page as an exception. It is also listed in the special needs page.

"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Main 3-1-1 Page

Special Needs Page

March 29, 2010 9:59 AM

.....
Your 3.4-1-1 link is broken.

March 29, 2010 10:29 AM

RB Said...

Blogger Bob said...
RB said... As has already been pointed out that section deals with people with medical issues or people with special needs, not the general public.
March 26, 2010 10:18 AM

This is listed under both the main 3-1-1 page as an exception. It is also listed in the special needs page.

"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Main 3-1-1 Page

Special Needs Page

March 29, 2010 9:59 AM

.....

OK, I twisted your words.

The FSD at Chicago indicated that WBI would become mandatory.

You say they are wrong, misspoke, not correctly informed or any other term you wish to chose to indicate disagreement.

I asked before and you dodged the question, are you more in the loop than a FSD at a major airport?

March 29, 2010 10:35 AM

Anonymous Said...

Bob, is the tiny risk strip-search machines present larger or smaller than the risk that someone's flip-flop is a disguised weapon, incendiary, or explosive?

Will these machines be used to screen TSOs?

March 29, 2010 11:47 AM

Jim Huggins Said...

Bob writes, regarding the question of frozen liquids:

This is listed under both the main 3-1-1 page as an exception. It is also listed in the special needs page.

"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Bob ... on the 3-1-1 page, look at the paragraph **immediately preceding the exception list**. The paragraph says that the exceptions are granted only **"to ensure the health and welfare of certain air travelers"**.

There's nothing that indicates that I, as a healthy person with no special medical needs, can take solid ice through a checkpoint.

So, which is it? Is the web page wrong in saying ice is permitted only for passengers with special needs? Or is the web page right, and your statement of the policy is wrong?

(And how can a common passenger know the difference?)

March 29, 2010 12:13 PM

RB Said...

Blogger Bob said...
RB said... As has already been pointed out that section deals with people with medical issues or people with special needs, not the general public.
March 26, 2010 10:18 AM

This is listed under both the main 3-1-1 page as an exception. It is also listed in the special needs page.

"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Main 3-1-1 Page

Special Needs Page

March 29, 2010 9:59 AM

.....

Bob, it seems your 3-1-1 link only allows ice for those with special needs. The section dealing with ice is discussing accommodations for those with special needs. Not everyone.

Either fix it or retract your statement!

.....

http://www.tsa.gov/311/311-carry-ons.shtm

To ensure the health and welfare of **certain air travelers**, in the absence of suspicious activity or items, greater than 3.4 ounce (100ml) of the following liquids, gels and aerosols are permitted through the security checkpoint in reasonable quantities for the duration of your itinerary (all exceptions must be presented to the security officer in front of the checkpoint):

Baby formula, breast milk, and juice if a baby or small child is traveling;

All prescription and over-the-counter medications (liquids, gels, and aerosols) including petroleum jelly, eye drops, and saline solution for medical purposes;

Liquids including water, juice, or liquid nutrition or gels for passengers with a disability or medical condition;

Life-support and life-sustaining liquids such as bone marrow, blood products, and transplant organs;
Items used to augment the body for medical or cosmetic reasons such as mastectomy products, prosthetic breasts, bras or shells containing gels, saline solution, or other liquids; and,

Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements.

March 29, 2010 1:24 PM

Ayn R. Key Said...

Ayn R. Key wrote:
Either way it's rather unprofessional of you to call me out ***and then fail to notice when I respond.***

Danny the BDO wrote:
You took one thing and made it about me, and even had to say that I was unprofessional because I mentioned you by name, along with everyone else that takes shots at TSA.

There is a problem with what you wrote Danny. This time I put it in bold for your benefit.

Danny the BDO wrote:
The behavior that some of the people, and no I am not saying you, but for the most part everyone who paints everyone the same way based on the actions of only a few, would or could we call them a racist if we were talking about a race?

Race, gender, and other similar considerations are factors that people do not, and cannot, choose but are intead born with. Being a TSO is not the same. To put your comment in proper perspective, you are saying we should not judge all muggers the same because if we did it would be similar to being a racist.

Now the topic of this thread is backscatter. The sub-topic I've been focusing on in this thread is mmw versus backscatter. As a retired engineer, what is **your** take on mmw versus backscatter? Be very careful though, because if you state the scientifically accurate answer I'm sure that your superiors at the TSA will take a very dim look on what you write. You may even get in actual trouble for writing the scientifically accurate answer, as a TSO employee, on this blog.

By the way, have you ever heard of Oath Keepers?

March 29, 2010 1:53 PM

AngryMiller Said...

LTSO with Answers said...

AngryMiller said... When passing through a checkpoint, at least here in the US, I am more surprised by the rarity of professionalism on the part of TSOs than I am of the rude, incompetent TSOs which sadly is the rule rather than exception. Please explain why that is.

AngryMiller I must say that from airport to airport I see the same thing when I travel. I believe it is because of the leadership at that airport or checkpoint. They still get the job done though just not in the friendly aspect that the public demands.

I'm not talking about being friendly. I am talking about having a professional demeanor. If this is a management problem then why isn't

TSA upper level management working on getting this resolved? Your agency is a representative of the US government to many foreigners traveling through the US. It behooves you to operate in a professional manner. Other countries manage to do this while getting the job done. Why can't we do this.

March 30, 2010 9:16 AM

Anonymous Said...

When will the TSA post unaltered, full size, full resolution sample images taken from the newest generation AIT machines MMW & x-ray?

March 30, 2010 1:08 PM

Anonymous Said...

If an anomaly or weapon is detected on a passenger's image is the screener viewing the image able to remove the algorithm applied to the image or disable any other privacy settings? Who in the airport has the clearance level to do so?

March 30, 2010 1:14 PM

RB Said...

Blogger Bob said...
RB said... As has already been pointed out that section deals with people with medical issues or people with special needs, not the general public.
March 26, 2010 10:18 AM

This is listed under both the main 3-1-1 page as an exception. It is also listed in the special needs page.

"Frozen items are allowed as long as they are frozen solid when presented for screening. If frozen items are partially melted, slushy, or have any liquid at the bottom of the container, they must meet 3-1-1 requirements."

Main 3-1-1 Page

Special Needs Page

March 29, 2010 9:59 AM
.....
Your link to 3-1-1 is still broken.

The information you tried to point to does not allow ice for all, just those with special needs.

Either fix the informaiton or retract your statement Bob.

April 1, 2010 10:46 AM

Anonymous Said...

My greatest concern is the DAILY Quality Control and DAILY Maintenance Standards that need to be imposed
and released for public purview with the recommendations required by the radiology professionals so we do not have another CT Scan debacle with large numbers of people fatally dosed by these machines!

April 2, 2010 5:17 PM

LTSO With Answers Said...

AngryMiller said...

I'm not talking about being friendly. I am talking about having a professional demeanor. If this is a management problem then why isn't TSA upper level management working on getting this resolved? Your agency is a representative of the US government to many foreigners traveling through the US. It behooves you to operate in a professional manner. Other countries manage to do this while getting the job done. Why can't we do this.

Yes I see what you mean and still agree and stand by what I think is the problem. To me, us as leads and supervisors need to be setting the example and enforcing SOP and policy all day everyday. We need to encourage and be a critic of our officers. That is how you shape officers to be professional. It is hard and professionalism can be seen as an opinion. It varies from one person to the next so it makes it difficult to set and control an image of being professional.

April 3, 2010 12:50 PM

Ryan62 Said...

Robert Johnson -
We don't see Al Qaeda attacking India and China? Correct, we don't see that particular branch of radical Islam, but there are certainly terrorist groups trying to kill infidels there. Did you miss the Mumbai attacks? How about the Muslim Uighurs in China? Or even moving to a majority Muslim country, the Bali Night Club bombings in Indonesia.
To argue this is all about the US is laughable in its ignorance of what is going on in the world. Is the United States a large symbolic target? Absolutely, but we are certainly not the only target and it is certainly not all about the US.

Linking to one guy saying "60%" certainly doesn't stand up to the level of scientific accuracy you all seem to expect from TSA. If its good enough for the goose it is certainly good enough for the gander.
Further, yes it won't detect something in a body cavity. It isn't supposed to. My car doesn't fly either, that doesn't mean it doesn't work. Yes, puffers are a great technology, but if TSA were fielding puffers again I am sure we would be hearing all the self proclmaimed experts go on and on about why puffers don't work and how that isn't "the real threat".

April 4, 2010 12:23 PM

Anonymous Said...

Blogger Bob said:
"Images can only be saved in test mode. The machines are not placed in test mode while at the airport. Test mode is used in testing situations at laboratories and testing facilities."

So when these devices fail or need servicing at the airport they will be transported back to the laboratories or testing facilities?

I can bet you that the technician will place the device into test mode at the airport if it needs servicing. It is possible, and probable that screeners will soon learn how to do just that. If screeners think it is all a joke to toss packets of a white powder into people's carry on, then explain why they won't think saving some images won't be as funny. Your agency does not have a good track record when it comes to professionalism.

April 5, 2010 4:17 PM

Blogger Bob Said...
Anonymous said: If screeners think it is all a joke to toss packets of a white powder into people's carry on, then explain why they won't think saving some images won't be as funny. April 5, 2010 4:17 PM

I don't want to speculate, so I sent an e-mail asking if there is a maintenance mode in addition to a test mode. I'm pretty sure there is, but I don't want to shoot from the hip and speculate.

As far as your comment about the powder, it was one person (not multiple) and that person was disciplined and they later resigned.

Thanks,

Blogger Bob
TSA Blog Team

April 6, 2010 8:39 AM

AngryMiller Said...
LTSO said:

Yes I see what you mean and still agree and stand by what I think is the problem. To me, us as leads and supervisors need to be setting the example and enforcing SOP and policy all day everyday. We need to encourage and be a critic of our officers. That is how you shape officers to be professional. It is hard and professionalism can be seen as an opinion. It varies from one person to the next so it makes it difficult to set and control an image of being professional.

Wearing an ill fitting, wrinkled uniform is unprofessional. Snapping at the travelers when they don't know the procedures is unprofessional. Being

rude to the travelers is unprofessional. Mistreating their belongings is unprofessional. Not knowing the SOP and making up something on the spot is unprofessional.

None of those things I mentioned are incredibly onerous/expensive to fix. Other countries manage to do it so why can't we?

TSOs are an ambassador of the US to foreign travelers. TSOs represent our government. Would you want some of your coworkers representing you to the world?

April 6, 2010 9:16 AM

Anonymous Said...

" Is the United States a large symbolic target? Yes."

Far more than that.

The United States is a target because our foreign policy has overthrown lawfully elected governments, backed monstrous dictators and has had a murderous impact on the people of the region.

I know this is a very unpopular truth. I hope the moderator will allow it to be said. This time.

April 6, 2010 10:17 AM

Blogger Bob Said...

Anonymous said... So when these devices fail or need servicing at the airport they will be transported back to the laboratories or testing facilities? I can bet you that the technician will place the device into test mode at the airport if it needs servicing. It is possible, and probable that screeners will soon learn how to do just that. April 5, 2010 4:17 PM

Test mode is not utilized by technicians for maintenance. It is only used in lab environments for testing.

Thanks,

Blogger Bob
TSA Blog Team

April 7, 2010 7:56 AM

RB Said...

Blogger Bob said...
Anonymous said... So when these devices fail or need servicing at the airport they will be transported back to the laboratories or testing facilities? I can bet you that the technician will place the device into test mode at the airport if it needs servicing. It is possible, and probable that screeners will soon learn how to do just that. April 5, 2010 4:17 PM

Test mode is not utilized by technicians for maintenance. It is only used in lab environments for testing.

Thanks,

Blogger Bob
TSA Blog Team

April 7, 2010 7:56 AM

.....

Is it your claim that a WBI machine cannot in any way, shape, or form, be placed in TEST MODE if the machine is in an airport?

April 7, 2010 12:52 PM

Anonymous Said...

Hi Bob,
You still did not answer the question "Can the machine be put into test mode at the airport ?"

Your answer was: " Test mode is not utilized by technicians for maintenance. It is only used in lab environments for testing."

"not utilized" does not say that test mode can't be used at the airport.

Now try again, this time with no spin. Yes or no, can the machine be put into test mode at the airport ?

April 7, 2010 2:49 PM

RB Said...

Why has TSA resumed purchases of Backscatter WBI that produce possibly dangerous radiation rather than more MMW WBIers that do not produce radiation?

Are MMW machines not performing well or is it some other reason?

April 8, 2010 4:53 PM

Robert Johnson Said...

Quote from Ryan62: *"We don't see Al Qaeda attacking India and China? Correct, we don't see that particular branch of radical Islam, but there are certainly terrorist groups trying to kill infidels there. Did you miss the Mumbai attacks? How about the Muslim Uighurs in China? Or even moving to a majority Muslim country, the Bali Night Club bombings in Indonesia.*
To argue this is all about the US is laughable in its ignorance of what is going on in the world. Is the United States a large symbolic target? Absolutely, but we are certainly not the only target and it is certainly not all about the US."

So let's take a look at how other countries react. London's subway was bombed. Did they go crazy and panic like we did? Nope. Back to normal. What about in Madrid? Did they go crazy? What about in Mumbai?

The Chinese take a particularly hardline against dissidents like the Uighurs, Falun Gong, and so forth. Doesn't seem to be working out too well for them.

Travel outside of the US, Ryan. There is a big difference between traveling inside and to/from the US than traveling elsewhere. Does that mean that the threat magically disappears?

"Linking to one guy saying "60%" certainly doesn't stand up to the level of scientific accuracy you all seem to expect from TSA. If its good enough for the goose it is certainly good enough for the gander."

It's more than TSA has put up. Do you have any evidence to back up their claim of it pretty much being the be-all-end-all that they make it out to be? Do you have any evidence that it's MORE effective than 60%?

"Further, yes it won't detect something in a body cavity. It isn't supposed to. My car doesn't fly either, that doesn't mean it doesn't work."

Your car also isn't being touted as a magic bullet that will solve all your transporation woes like these machines are being touted for curing our security woes either.

I guess once we have a rectum bomber, THEN we'll get to that. It's already been tried against a Saudi prince.

These things are being touted as a panacea to "keep us safe." Problem is that's a way of getting around the system, and does nothing to address that

"Yes, puffers are a great technology, but if TSA were fielding puffers again I am sure we would be hearing all the self proclmaimed experts go on and on about why puffers don't work and how that isn't "the real threat".

Actually, I haven't heard anyone complain about the puffers. Any gripe I've heard about them has come from TSA complaining about maintenance issues.

Even the most vehement haters I've known thought the puffers were a good thing.

Tell me, how the puffers aren't addressing a "real" threat when they're supposed to be detecting explosives? They did it well and weren't invasive. TSA screwed up on the implementation by not testing them in a real world situation. However, instead of going back and fixing something they had already invested in, they decided to go with a new toy, that's much more invasive and can be more "fun" for certain types of people.

And in all likelihood, a puffer would have had a much higher chance of detecting the explosive than the scanner. However, once again, we see TSA tilting at windmills.

Robert

April 15, 2010 10:38 PM

Anonymous Said...

Franz Pichler said...
As someone before asked i also want to know:
What steps is TSA taking to ensure every passenger asked to be strip-searched knows he or she can decline the strip-search?
****

theres a sign right next to the machine ((usally on the right for sum reason))saying u can request a pat down instead...

a big problem in airports that i see ((and i travel airport to airport every week so i pretty much know my way around)) is the people around me just dont seem to be very aware of their surroundings. from the time i check my bags and get my ticket to the time i get thru security i can usually count about 6 different signs that CLEARLY state the liquid rules with size restriction and all yet the first 3 or 4 people in front of me have drinks in their bags. i even heard another passanger telling a TSO that she had no idea how her water got in her bag but she thought "the maid must of have stuck it in my bag before we left the hotel" which was a lie cuz it was half frozen and i saw her drinking it in line and as she was walking off tell the man with her "i knew i just figured they wouldnt see it in the xray" .... seriously...airports are FULL of signs just cuz their small dosnt mean they arent important.....so basically people just be more aware of your surroundings it would save u alotof questions

April 19, 2010 2:30 PM

Kacey Jone Said...

What steps is TSA taking to ensure every passenger asked to be strip-searched knows he or she can decline the strip-search?

April 20, 2010 7:31 AM

Lana Said...

The real question is this: When you have completely safe mmw, why do you use backscatter at all?

Seriously, no matter how tiny the risk, there is an equivalent technology that is still safer.

Is it lower cost? Does backscatter cost less than mmw?

July 1, 2010 6:24 AM

Anonymous Said...

At the Gulfport airport, I was told to step into this box and hold my hands up. I said "What is this?" and was ignored. After I came out, I asked again, and was told it was an x-ray. I assume that this was the body scanner and I felt COMPLETELY VIOLATED. Not only was I not told that I had the right to deny this, but I wasn't even told what it was.

July 1, 2010 1:18 PM

Post a Comment

Subscribe to Post Comments [Atom]

Links To This Post:

Create a Link

<< Home

U.S. Department of Homeland Security

Freedom of Information Act Office
601 South 12th Street
Arlington, VA 20598-6020

Transportation
Security
Administration

MAR 15 2010

FOIA Case Number: TSA09-0510 and TSA10-0260

Mr. John Verdi
EPIC Open Government Project
1 1718 Connecticut Ave NW, Ste #200
Washington, D.C. 20009

Dear Mr. Verdi:

This letter is in response to your Freedom of Information Act (FOIA) requests to the Transportation Security Administration (TSA) dated April 14, 2009 and July 2, 2009, respectively, on behalf of the Electronic Privacy Information Center ("EPIC") in which you are seeking records dealing with TSA's advanced imaging technology (AIT) program. The security measures that TSA employs are critical to our mission to protect transportation and national security. Preventing undue disclosure of these measures is necessary to counter the increased sophistication of those who pose a threat to civil aviation and their ability to develop techniques to subvert current security measures. Also, TSA is committed to ensuring the privacy of the traveling public to the greatest extent possible. AIT is part of our multi-layered security strategy to stay ahead of evolving threats.

This response pertains to those documents over which TSA exercises control, including the following documents identified in your July 2, 2009 request set forth below:

TSA10-0260:

1. All unfiltered or unobscured images captured using Whole Body Imaging Technology (WBI),
2. All contracts entered into by DHS pertaining to WBI systems, including contracts for hardware, software or training.
3. All documents detailing the technical specifications of WBI hardware, including any limitations on image capture, storage or copy.
4. All documents, including but not limited to presentations, images and videos used for training persons to use WBI systems.
5. All complaints related to the use of WBI and all documents relating to the resolution of those complaints.
6. All documents concerning data breaches of images generated by WBI technology."

Your request has been processed under the FOIA, 5 U.S.C. § 552.

As an preliminary matter, in our interim response to you dated December 1, 2009, for your April 14, 2009 request, we provided you responsive records for Item 2. We stated that after a search of files for records that would be responsive to your request, we had located (286) pages responsive to Item 2 of your request; however, the correct page count of responsive records located is (238) pages.

With respect to Items 1-3 of your April 14, 2009 request, we are continuing our review of additional documents. In response to Items 1-4, and 6, of your July 2, 2009 request, we are continuing our search for and review of responsive documents.

With respect to Item 5, of TSA10-0260, a search within the TSA was conducted and documents (451 pages) responsive to your request were located. The documents located consist of complaints regarding AIT received by TSA. Of the 4,000,000+ individuals screened using AIT, the 600+ total complaints received by TSA constitute approximately .00015 % of the total number of those individuals, an infinitesimally small percentage of the traveling public.

Portions of all 451 pages are being withheld under Exemptions "High" and "Low" (b)(2) and (b)(6) of the FOIA. We have inserted notations in the attached documents to identify the portions deleted and the reasons therefore. A more complete explanation of these exemptions is provided below.

Exemption (b)(2)

Exemption 2 of the FOIA exempts from mandatory disclosure records that are "related solely to the internal personnel rules and practices of an agency." The courts have interpreted the exemption to encompass two distinct categories of information: (1) internal matters of a relatively trivial nature -- often referred to as "Low" 2 information; and (2) more substantial internal matters, the disclosure of which would risk circumvention of a legal requirement -- often referred to as "High" 2 information.

Exemption "low" 2 of the FOIA protects from disclosure internal matters of a relatively trivial nature. The Supreme Court has held that the very task of processing and releasing some requested records would place an administrative burden on the agency that would not be justified by any genuine public benefit. Low 2 serves to relieve the agency from the administrative burden of processing FOIA requests when internal matters are not likely to be the subject of public interest. For example, routine internal personnel matters, such as information relating to performance standards and leave practices, are included within the scope of the exemption. Exemption 2 has also been construed to permit the nondisclosure of mundane, yet far more pervasive administrative data -- such as file numbers, mail routing stamps, initials, data processing notations, brief references to previous communications, and other similar administrative markings.

I have determined that certain portions of the requested records are properly withheld from disclosure as "High" 2 information, in that they contain internal administrative and/or personnel matters to the extent that disclosure would risk circumvention of a regulation or statute or impede the effectiveness of law enforcement activities. A more detailed explanation follows.

Sensitive materials are exempt from disclosure under "High" 2 when the requested document is predominantly internal, and disclosure significantly risks circumvention of a regulation or statute, including civil enforcement and regulatory matters. Whether there is any public interest in disclosure is legally irrelevant. Rather, the concern under "High" 2 is that a FOIA disclosure should not benefit those attempting to violate the law and avoid detection.

Exemption (b)(6)

Exemption 6 of the FOIA permits the government to withhold all identifying information that applies to a particular individual when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." This requires a balancing of the public's right to disclosure against the individual's right to privacy. After performing this analysis, I have determined that the privacy interest in the identities of individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Please note that any private interest you may have in that information does not factor into the aforementioned balancing test.

Fees

TSA is waiving any applicable fees associated with the processing of your request.

In addition, as TSA's s response to this request is currently the subject of litigation, the administrative appeal rights that normally accompany a FOIA response are not being provided.

If you have any questions regarding this release, please contact Department of Justice Attorney Jesse Grauman. He can be reached directly at 202-514-2849.

Sincerely,

for

Kevin J. Janet
FOIA Officer
Freedom of Information Act Office

Enclosure

GAO

United States Government Accountability Office

Testimony

Before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, March 17, 2010

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

Statement of Steve Lord, Director
Homeland Security and Justice Issues

GAO

Accountability * Integrity * Reliability

March 17, 2010

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

GAO Accountability · Integrity · Reliability

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 ongoing work on air cargo security. For the ongoing 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.

View GAO-10-484T or key components. For more information, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

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 twofold 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 billion 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 ongoing 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.

AR 001353

Madame 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 both 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

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

addressed all three elements of the system.[2] Similarly, securing the flying public involves tradeoffs between security, privacy, and the efficient flow of commerce. Striking the right balance between these three goals is an ongoing 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 technology 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 ongoing 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

---

[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, D.C.: 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, D.C.: Oct. 7, 2009); *Homeland Security: DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity*, GAO-10-106 (Washington, D.C.: 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, D.C.: 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, D.C.: Mar. 18, 2009); *Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process*, GAO-08-48T (Washington, D.C.: 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, D.C.: Oct. 11, 2007).

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

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 governing 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.

[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.

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

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. 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

[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.

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.

[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.

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 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

[8]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.

[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 GAO-10-128 and GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition*, GAO-04-386SP (Washington, D.C.: Jan. 2004).

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

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

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

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 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.

[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.

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.

[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 inbound 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.

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 with operational testing.[19] As we previously reported, based on preliminary observations from ongoing 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 ongoing 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

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

[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]GAO-09-422T.

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 ongoing 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 inbound 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 ongoing review of TSA's air cargo security efforts, to be issued later this year.

[21]For additional information on TSA's staffing study, see GAO, *Aviation Security: Status of Transportation Security Inspector Workforce*, GAO-09-123R (Washington D.C.: 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.

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)—nationwide 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 milestones 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

[23]GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: 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]GAO-09-399.

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

---

[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, D.C., 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)).

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 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

[30] GAO-10-128.

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.

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

Contacts and Acknowledgements

For additional information about this statement, please contact Stephen M. Lord at (202) 512-4379 or lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

In addition to the contact named above, staff who made key contributions to this statement were E. Anne Laffoon and Steve D. Morris, Assistant Directors; Nabajyoti Barkakati, Carissa Bryant, Frances Cook, Joseph E. Dewechter, Amy Frazier, Barbara Guffy, David K. Hooper, Richard B. Hung, Lori Kmetz, Linda S. Miller, Timothy M. Persons, Yanina Golburt Samuels, Emily Suarez-Harris, and Rebecca Kuhlmann Taylor.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.